
Venafi Platform: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-000357-001
Revision	F
Release Date	10 March 2021

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Certified Platforms.....	4
Certified Platforms for Luna HSM	4
Certified Platforms for Cloud Luna HSM.....	4
Prerequisites	5
Configure Luna HSM	5
Configure Luna Cloud HSM Service.....	6
Install Microsoft Visual C++	8
Install Venafi Platform	9
Integrating Venafi Platform with Luna HSM.....	9
Create an HSM (Cryptoki) Connector.....	9
Enable Venafi Advanced Key Protect.....	10
Use Luna HSM in Venafi Platform	11
Contacting Customer Support.....	30
Customer Support Portal	30
Telephone Support	30
Email Support	30

Overview

Thales Luna HSMs are available as on premise hardware HSMs, also known as Luna HSMs and as a cloud offering, namely DPOD Luna Cloud HSM. The benefits of integrating these HSMs with Venafi Platform include:

- > Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of the keys.
- > HSM audit trail*.
- > Significant performance improvements by off-loading cryptographic operations from application servers.

*Luna Cloud HSM service does not have access to the secure audit trail

Certified Platforms

[Certified Platforms for Luna HSM](#)

[Certified Platforms for Cloud Luna HSM](#)

Certified Platforms for Luna HSM

The following platforms are certified for integrating Venafi Trust Protection Platform with Luna HSM:

HSM Type	Platforms Certified
Luna HSM	Windows 2016 Server Datacenter Windows 2012R2 Server

NOTE: This integration is tested in both HA and FIPS mode.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Certified Platforms for Cloud Luna HSM

The following platforms are certified for integrating Venafi Trust Protection Platform with Luna Cloud HSM:

HSM Type	Platforms Certified
Luna Cloud HSM	Windows 2016 Server Datacenter Windows 2012R2 Server

Luna Cloud HSM: Luna Cloud HSM platform provides on-demand, cloud-based HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and

easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

[Configure Luna HSM](#)

[Configure Luna Cloud HSM Service](#)

[Install Microsoft Visual C++](#)

[Install Venafi Platform](#)

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the *Luna HSM Product Documentation* for more information.
2. Create a partition that will be later used by Venafi TPP.
3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe

lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights
reserved.

Available HSMs:

Slot Id ->                0
Label ->                  Venafi
Serial Number ->          1213475834492
Model ->                  LunaSA 7.3.0
Firmware Version ->       7.3.0
Configuration ->          Luna User Partition With SO (PW) Signing With Cloning
Mode
Slot Description ->        Net Token Slot
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

NOTE: Refer to the [Luna HSM documentation](#) for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

Set up Luna HSM High-Availability

Refer to the [Luna HSM documentation](#) for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

NOTE: The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

- > [Standalone Cloud HSM service using minimum client package](#)
- > [Standalone Cloud HSM service using full Luna client package](#)
- > [Luna HSM and Luna Cloud HSM service in hybrid mode](#)

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using [pscp](#), scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

```
[Windows]
cvclient-min.zip
```

4. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.

```
[Windows]
Right-click setenv.cmd and select Run as Administrator.
```

5. Run the **LunaCM** utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using [pscp](#), scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

[Windows]

cvclient-min.zip

4. Run the **setenv** script to create a new configuration file containing information required by the Luna Cloud HSM service.

[Windows]

Right-click **setenv.cmd** and select **Run as Administrator**.

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

NOTE: Skip this step for Luna Client v10.2 or higher.

Cloud HSM Certificates:

server-certificate.pem

partition-ca-certificate.pem

partition-certificate.pem

LunaClient Certificate Directory:

[Windows default location for Luna Client]

C:\Program Files\Safenet\Lunaclient\cert\

6. Open the configuration file from the Cloud HSM service client directory and copy the **XTC** and **REST** section.

[Windows]

crystoki.ini

7. Edit the Luna Client configuration file and add the **XTC** and **REST** sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in **XTC** and **REST** sections. Do not change any other entries provided in these sections.

NOTE: Skip this step for Luna Client v10.2 or higher.

[XTC]

```
. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .
```

[REST]

```
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .
```

9. Edit the following entry from the **Misc** section and update the correct path for the **plugins** directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>
```

```
[Windows Default]
```

```
C:\Program Files\Safenet\Lunaclient\plugins\
```

Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the **ChrystokiConfigurationPath** environment variable and point back to the location of the Luna Client configuration file.

[Windows]

In the Control Panel, search for "environment" and select **Edit the system environment variables**. Click **Environment Variables**. In both list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** and point to the **crystoki.ini** file in the Luna client install directory.

11. Run the **LunaCM** utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

NOTE: Refer to the [Luna Cloud HSM documentation](#) for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the [Standalone Cloud HSM service using full Luna client package](#) section above.

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Luna Cloud HSM Service in FIPS mode

Luna Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Install Microsoft Visual C++

Install Microsoft Visual C++ on the Venafi Platform server. Microsoft Visual C++ is required to access some HSM on Demand applications and utilities. Refer to [Microsoft Visual C++ Download Portal](#) for more information on installing Microsoft Visual C++.

Install Venafi Platform

Install Venafi Trust Protection Platform on the target machine. For Venafi Code Signing, the installable components are:

- > Venafi Platform with Venafi Code Signing components
- > CSP for code signing workstations

Refer to [Venafi Documentation](#) for detailed instructions.

Integrating Venafi Platform with Luna HSM

This section contains the following topics:

- > [Create an HSM \(Cryptoki\) Connector](#)
- > [Enable Venafi Advanced Key Protect](#)
- > [Use Luna HSM in Venafi Platform](#)

Create an HSM (Cryptoki) Connector

To create an HSM connector, you need to:

1. Open the **Venafi Configuration Console** and from the **Venafi Configuration** pane on the right, click **Connectors**.



2. Click **Create HSM Connector** from the **Actions** pane on the right.
3. Enter the Venafi Trust Protection Platform administration credentials if needed, and then click **OK**.
4. In the **Create new HSM (Cryptoki) Connector** window that appears, fill out the **Name**, **Cryptoki DII Path**, **Slot**, **User Type** and **Pin** fields, and then click the **Verify** button.

The dialog box contains the following fields and controls:

- Name:** Text box containing 'HSM'.
- Cryptoki DII Path:** Text box containing 'C:\Program Files\SafeNet\LunaClient\c' with a 'Browse...' button.
- Slot:** Spin box set to '0'.
- User Type:** Dropdown menu set to 'Crypto Officer (User)'.
- Pin:** Password field with masked characters and a 'Verify' button.

- Click the **Create** button that appears under the **Permitted Keys** field.

Create new HSM (Cryptoki) Connector

Please fill out all fields to create a new HSM connector.

Name:

Cryptoki DLL Path:

Slot:

User Type:

Pin:

Permitted Keys:

(Ctrl-Click to multi-select)

☐ Allow Key Storage (Private Keys are non-exportable)

- Verify that the HSM connector appears under the **Platform Connectors** pane.

Component	Detail	Description
Software	Key Generation & Data Encryption	Connector providing software-based encryption
Null	Data Encryption	Pass-through encryption driver. For data that does not need to be encrypted.
HSM	Key Generation & Data Encryption	HSM

Enable Venafi Advanced Key Protect

Venafi Advanced Key Protect enables you to orchestrate HSM-based generation and storage of cryptographically strong keys. To enable Venafi Advanced Key Protect:

- Open the **Venafi Configuration Console** and click the **Connectors** node from the left pane.
- In the Actions panel, click **Enable Advanced Key Protect**.
- Review the information in the dialog boxes and confirm the action.
- Restart the IIS service by going to the **Product** node, selecting **Website** service, and then clicking **Restart**.
- Restart the Venafi Platform service by selecting **Venafi Platform** service, and then clicking **Restart**.
- Restart the Logging service by selecting **Logging** service, and then clicking **Restart**.

For more information on Venafi Advanced Key Protect module, refer to <https://www.venafi.com/platform/advanced-key-protect>.

Use Luna HSM in Venafi Platform

Venafi Platform leverages Luna HSMs in the following use cases:

[Use Case I – Database Protection with HSM encryption](#)

[Use Case II - Central HSM Key Generation](#)

[Use Case III - Remote HSM Key Generation](#)

[Use Case IV – Next-Gen Code Signing](#)

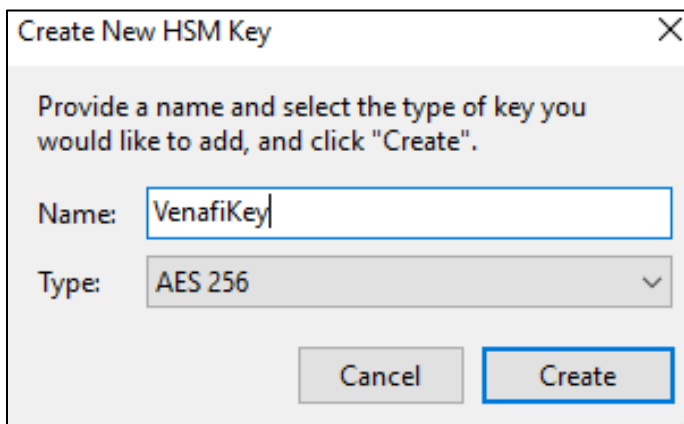
Use Case I – Database Protection with HSM encryption

Venafi Platform maintains all system information (configuration settings, managed server and certificate information, credentials, archived certificates, and private keys) in a database. The platform uses Luna HSMs to encrypt the information used to connect to the database, as well as to secure the encryption assets within the database, including certificate private keys, credential objects, and SSH keys.

NOTE: Ensure that the HSM client is configured on the system and HSM partition is accessible from the HSM client. If you are using HSM in HA mode, ensure that HAOnly is enabled from the HSM client.

Create the encryption key

1. In **Venafi Configuration Console**, select **HSM connector** and click **Properties**.
2. In **Permitted Keys** field, click the **New Key** button to create a new encryption key on the HSM partition or service.
3. In the **Create New HSM Key** window, specify the name of the encryption key in the **Name** field, select **AES 256** from the **Type** drop down menu, and then click **Create**.



Create New HSM Key

Provide a name and select the type of key you would like to add, and click "Create".

Name:

Type:

4. Select the new key in the **Permitted Keys** field and click **Create**.

Create new HSM (Cryptoki) Connector

Please fill out all fields to create a new HSM connector.

Name:

Cryptoki DLL Path:

Slot:

User Type:

Pin:

Permitted Keys:

(Ctrl-Click to multi-select)

5. The encryption key is generated on the partition. You can verify the encryption key exists by executing the `partition contents` command in `lunacm`.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->          0
Label ->            Venafi
Serial Number ->    1254270083886
Model ->            LunaSA 7.3.0
Firmware Version -> 7.3.0
Configuration ->    Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> role login -n co

enter password: *****

Command Result : No Error

lunacm:> partition contents

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:              VenafiKey
Handle:              972
Object Type:         Symmetric Key
Object UID:          7a0400002c00000351380800

Number of objects: 1
```

Use Case II - Central HSM Key Generation

Luna HSM enables you to centrally generate the private keys for certificates and SSH keys. Centrally generated private keys are exported from the HSM and stored as cipher text in the Venafi database. The private keys and certificates are installed on the target machines that will use them.

NOTE: Central HSM Key Generation is supported by HSM on Demand with Key Export service in Non-FIPS mode and Luna HSM with Key Export in Non-FIPS mode. Ensure that the HSM client is configured on the system and the HSM partition is accessible from the client. If you are using HSM in HA mode, ensure that HAOnly is enabled and HASync is disabled from HSM client. Ensure that the application is configured on the target machine and can be reached by Venafi Platform server.

To complete Central HSM Key Generation in Venafi Platform, you need to perform the following procedures:

- > [Create HSM connector](#)
- > [Enable Venafi Advanced Key Protect](#)
- > [Create the Certificate Authority \(CA\) template](#)
- > [Configure Certificate Object for Central HSM Key Generation](#)

Create HSM Connector

Refer the [Creating the HSM Connector](#) section for detailed steps.

Enable Venafi Advanced Key Protect

Refer the [Enabling Venafi Advanced Key Protect](#) section for detailed steps.

Create the Certificate Authority (CA) template

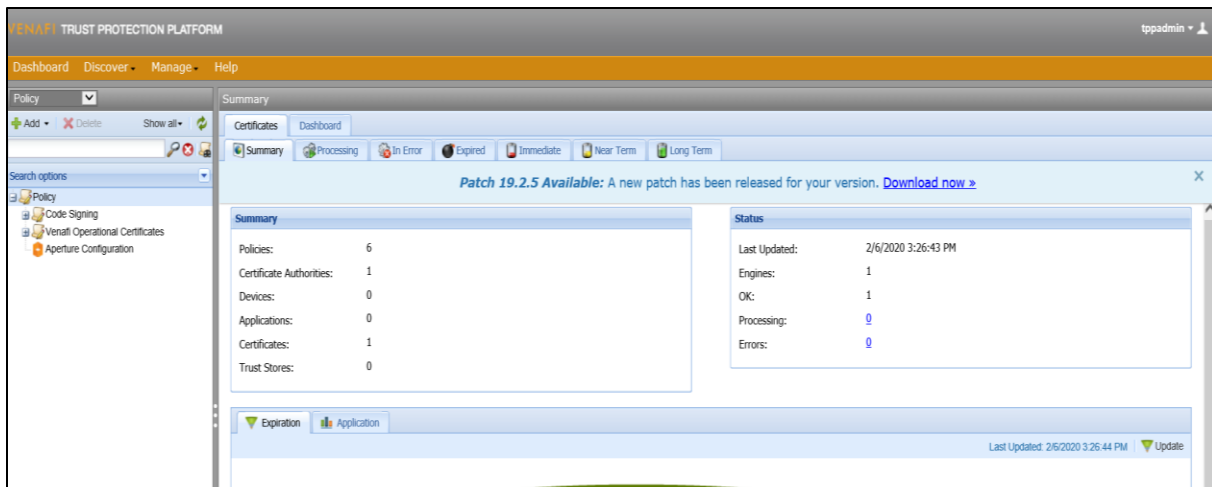
During the certificate enrollment and provisioning procedures, every certificate object must reference a CA template object. The CA template objects provide the information that Trust Protection Platform needs to submit the certificate signing request (CSR) to the CA and retrieve the signed certificate. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

Configure Certificate Object for Central HSM Key Generation

Configure and update the Venafi platform policies to allow and use the Luna HSM for central HSM key generation. To configure test certificate for Central HSM Key Generation:

1. Log in to admin console from `https://[IP_address_of_Venafi_TPP]/vedadmin`.

2. Select policy from the **Policy** tree in Venafi Platform.



3. Select Policy > Settings > Certificate tab.
4. Specify the **HSM** in the **Key Generation** drop-down menu.

Other Information

CA Template:

Key Generation:

Encryption Key:

Disable Automatic Renewal:

Allow Simple Passwords for Private Key Downloads:

Private Key PBE Algorithm:

Renewal Window: days

Each algorithm type has a corresponding security/compatibility value. Generally, they are inversely related due to their adoption by software applications.

5. Click **Save**.
6. Right click on the selected policy.
 - a. Click **Add > Certificates > Certificate**.
 - b. Specify the details of the certificate in **General Information** tab.
 - c. Open the **Management Type** drop-down menu and select **Provisioning** or **Enrollment**.

General Information

* Certificate Name:

Description:

Contact(s):

Approver(s):

Processing Disabled: ☐

Management Type:

Managed By:

- d. Enable the **Service Generated CSR** radio button in the **CSR Generation** field.

- e. Set Generate Key/CSR on Application to **NO**.
- f. Fill out the details in the **Subject DN** tab.
- g. Specify the key type in the **Private Key** tab.

Private Key	
Private Key Stored:	No
Key Algorithm:	RSA
Key Strength (bits):	2048
Elliptic Curve:	P256

- h. Choose the configured **CA template** in **Other Information** tab.

Other Information	
CA Template:	\\VED\Policy\SafeNetHSM\SafeNetCA
Disable Automatic Renewal:	No
Renewal Window:	30 days

- i. Click **Save**. The certificate gets generated with **Certificate Status** as **OK**.

ClientCertificate : Summary	
Certificate	Monitoring Validation General Support
Summary	Settings Associations Compliance History
Restart Retry Reset Renew Now Check Revocation Validate Now Revoke Change Certificate Type Print	
<div> <div> <div>Certificate Status</div> <div> <div>OK</div> <div> <div>Expiration Date</div> <div>Lifecycle Stage</div> <div>none</div> </div> </div> </div> <div> <div>Revocation</div> <div> <div>Last Check:</div> <div>Result:</div> </div> </div> <div> <div>Validation</div> <div> <div>Last Check: never</div> <div>State:</div> <div>SSL/TLS Result:</div> <div>File Result:</div> </div> </div> </div>	

- j. Click the **Renew Now** button. The **Certificate Status** changes from **OK** to **Queued for Renewal**.

- k. Wait for some time and then click refresh in top rightmost corner. Scroll down to see the details of the certificate. If the certificate is of type **Provisioning**, associate the certificate to the application object and verify that the certificate is installed on the application server.

Miscellaneous	
Valid From:	2/21/2019 5:02:41 PM
Valid To:	2/21/2020 5:02:41 PM
Serial Number:	2BC68DC0DA67284493F0AB187202EFA0
Version:	3
Signature Algorithm:	sha256RSA (1.2.840.113549.1.1.11)
SHA1 Thumbprint:	76F68A1CF3296DBD871CCA2DFFAF071C0161CCA0
Subject Key Identifier	7b 96 50 9b 3d 9e 99 5f 47 93 1b 3b 97 b0 bc 7e 6d 96 b9 77
Basic Constraints	Subject Type=End Entity, Path Length Constraint=None
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Encipher Only (f9)
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Public Key	
Public Key Size:	2048
Public Key Exchange Algorithm:	RSA
Public Key Signature Algorithm:	RSA

Use Case III - Remote HSM Key Generation

To complete Remote HSM Key Generation in Venafi Platform, you need to perform the following tasks:

- > [Configure remote machine](#)
- > [Enable Venafi Advanced Key Protect on Venafi Platform](#)
- > [Create the Certification Authority \(CA\) template](#)
- > [Configure Certificate Object for Remote HSM Key Generation](#)

Configure remote machine

Perform the following steps on remote machine where you want to install the certificate:

1. Install Luna HSM client on the target machine and configure the partition.
2. Configure the application on the remote machine to use Luna HSM.

Refer to [Venafi Documentation](#) for the list of supported applications.

Enable Venafi Advanced Key Protect on Venafi Platform

To enable Venafi Advanced Key Protect, refer to the [Enabling Venafi Advanced Key Protect](#) section.

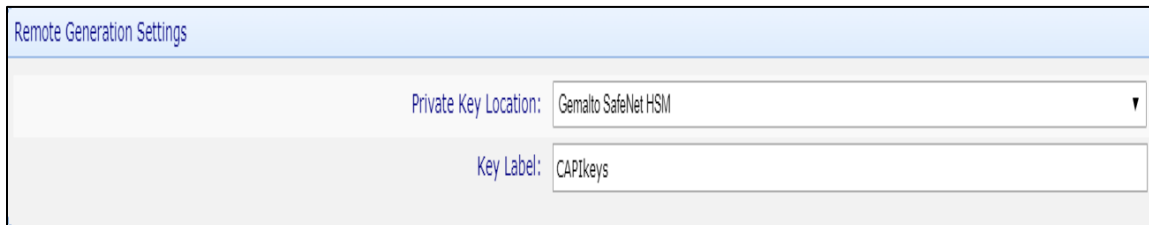
Create the Certification Authority (CA) template

During certificate enrollment and provisioning procedures, every certificate object must reference a CA template object. CA template objects provide the information Trust Protection Platform needs to submit the certificate signing request (CSR) to the CA and retrieve the signed certificate. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

Configure Certificate Object for Remote HSM Key Generation

To configure the Certificate object for remote HSM key generation:

1. Log in to the admin console: `https://[IP_address_of_Venafi_TPP]/vedadmin`
2. Select the policy from the **Policy** tree in Venafi Platform.
3. Choose the application that you have configured on the target machine.
4. In the **Remote Generation Settings** window, choose **Gemalto SafeNet HSM** under the **Private Key Location** drop down and specify the key label in **Key Label** field.

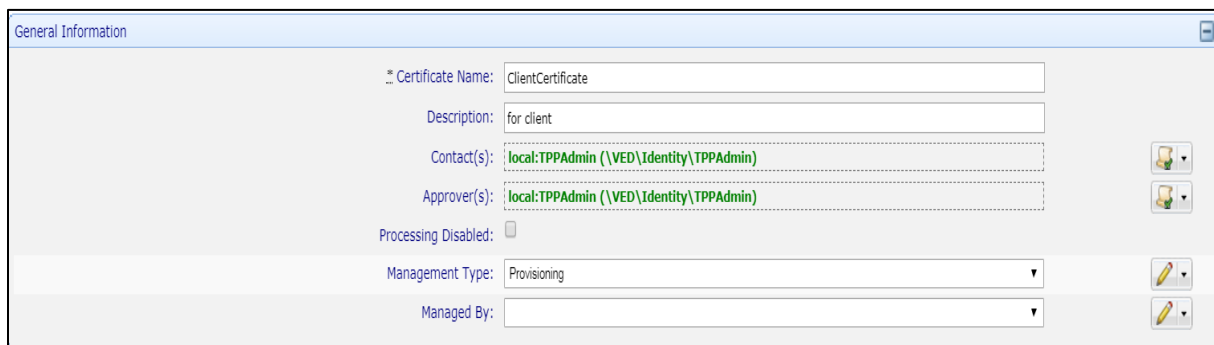


Remote Generation Settings

Private Key Location: Gemalto SafeNet HSM

Key Label: CAPIkeys

5. Click **Save** to save the application object.
6. Right click on policy.
 - a. Click on **Add > Certificates > Certificate**.
 - b. Specify the details of the certificate in **General Information** tab.
 - c. Open the **Management Type** drop-down menu and select **Provisioning**.



General Information

Certificate Name: ClientCertificate

Description: for client

Contact(s): local:TPPAdmin (\VED\Identity\TPPAdmin)

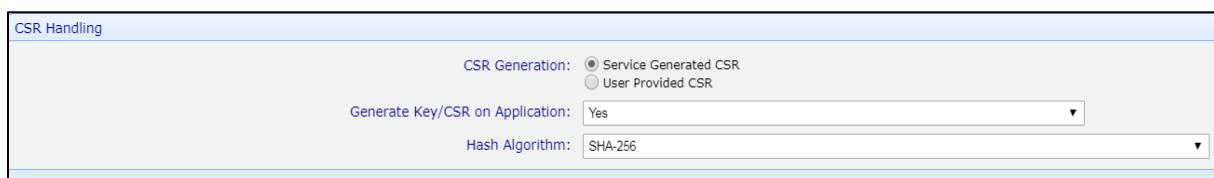
Approver(s): local:TPPAdmin (\VED\Identity\TPPAdmin)

Processing Disabled: ☐

Management Type: Provisioning

Managed By:

- d. Enable the **Service Generated CSR** radio button in the **CSR Generation** field.
- e. Set **Generate Key/CSR on Application** to **Yes**.



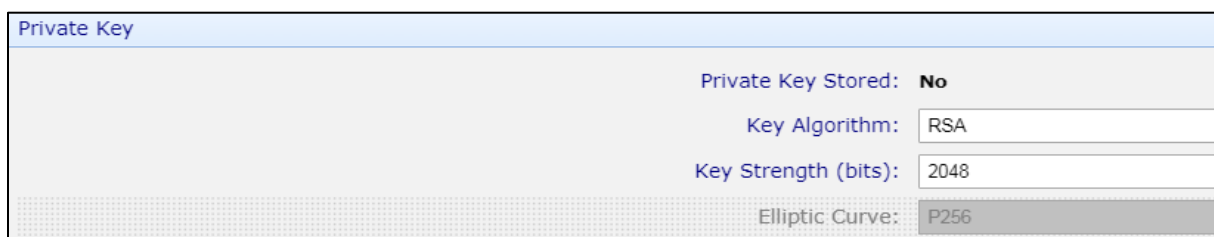
CSR Handling

CSR Generation: ☒ Service Generated CSR ☐ User Provided CSR

Generate Key/CSR on Application: Yes

Hash Algorithm: SHA-256

- f. Fill out the details in the **Subject DN** tab.
- g. Specify the key type in the **Private Key** tab.



Private Key

Private Key Stored: No

Key Algorithm: RSA

Key Strength (bits): 2048

Elliptic Curve: P256

- h. Choose the **CA template** in **Other Information** tab.

NOTE: Remote HSM key generation will not work with self-signed CA template.

7. Click **Save**. Certificate generates with the **Status OK**.

The screenshot shows the 'ClientCertificate : Summary' window with the 'Certificate' tab selected. The 'Certificate Status' section displays 'OK' with a green checkmark icon. Below this, there are four fields: 'Expiration Date', 'Lifecycle Stage' (set to 'none'), 'Revocation' (with 'Last Check:' and 'Result:' labels), and 'Validation' (with 'Last Check:' set to 'never', 'State:' label, 'SSL/TLS Result:', and 'File Result:'). The top navigation bar includes tabs for Certificate, Monitoring, Validation, General, and Support, and a secondary bar with icons for Summary, Settings, Associations, Compliance, and History. A toolbar at the bottom contains buttons for Restart, Retry, Reset, Renew Now, Check Revocation, Validate Now, Revoke, Change Certificate Type, and Print.

8. Go to the application object where you want to associate the certificate. Under Certificate section, choose the renewed certificate in the **Associated Certificate** field. Click **Save**.
9. Go back to the certificate object and click **Renew Now**. The certificate moves from **OK** to **Queued for Renewal** Stage.
10. Wait for some time and then click refresh icon in top rightmost corner. Scroll down to see the details of the renewed certificate.

The screenshot shows the details of a renewed certificate, divided into two sections: 'Miscellaneous' and 'Public Key'. The 'Miscellaneous' section lists the following information: Valid From (2/21/2019 5:02:41 PM), Valid To (2/21/2020 5:02:41 PM), Serial Number (2BC68DC0DA67284493F0AB187202EFA0), Version (3), Signature Algorithm (sha256RSA (1.2.840.113549.1.1.11)), SHA1 Thumbprint (76F6BA1CF3296DBD871CCA2DFFAF071C0161CCA0), Subject Key Identifier (7b 96 50 9b 3d 9e 99 5f 47 93 1b 3b 97 b0 bc 7e 6d 96 b9 77), Basic Constraints (Subject Type=End Entity, Path Length Constraint=None), Key Usage (Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Encipher Only (f9)), and Enhanced Key Usage (Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)). The 'Public Key' section lists: Public Key Size (2048), Public Key Exchange Algorithm (RSA), and Public Key Signature Algorithm (RSA).

11. After the installation process gets completed on the target machine, the status returns to **OK**.
12. Verify that the certificate is installed on the application on the target machine and the keys are created on the HSM.

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

    Available HSMs:

    Slot Id ->          0
    Label ->            Venafi
    Serial Number ->    1254270083886
    Model ->            LunaSA 7.3.0
    Firmware Version -> 7.3.0
    Configuration ->    Luna User Partition With SO (PW) Key Export With Cloning Mode
    Slot Description -> Net Token Slot

    Current Slot Id: 0

lunacm:> role login -n co

    enter password: *****

Command Result : No Error

lunacm:> partition contents

    The 'Crypto Officer' is currently logged in. Looking for objects
    accessible to the 'Crypto Officer'.

    Object list:

    Label:      CAPIkeys
    Handle:     2217
    Object Type: Private Key
    Object UID: a60e00002e00000351380800

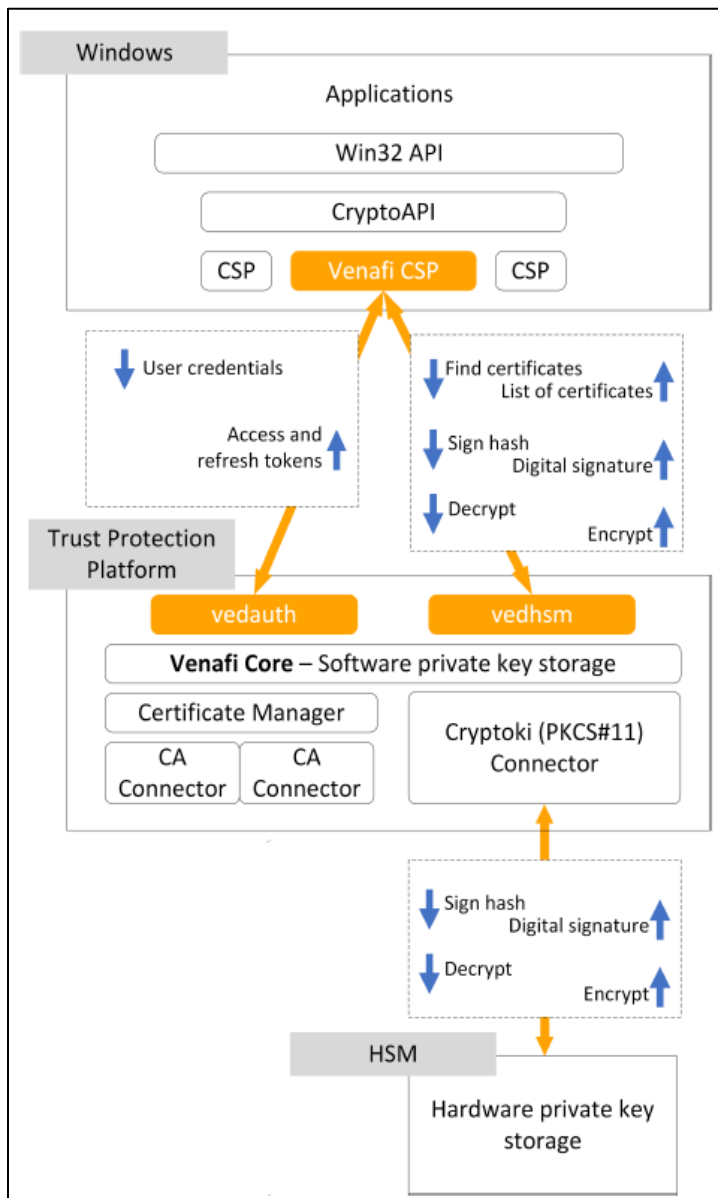
    Label:      CAPIkeys
    Handle:     2219
    Object Type: Public Key
    Object UID: a50e00002e00000351380800
```

Use Case IV – Next-Gen Code Signing

Venafi Next-Gen Code Signing secures all private keys, automates code-signing workflows, and maintains a record of all code signing activities. To use Luna HSMs for code signing key storage, the HSMs must be connected to the Venafi Platform. After being connected, the HSMs become available as a key storage option when setting up code signing projects.

NOTE: Verify that the Venafi Next-Gen Code Signing software license is enabled before proceeding with the Integration.

Trust Protection Platform uses the vedauth and vedhsm endpoints to facilitate authentication and HSM functions, as shown in the figure below.



To complete code signing in Venafi Platform, you need to perform the following procedures:

1. [Enable Key Storage in the HSM Connector](#)
2. [Enable Venafi Advanced Key Protect](#)
3. [Assign the Code Signing Administrator](#)
4. [Create the Certificate Authority \(CA\) template](#)
5. [Create the Signing Flow](#)
6. [Create the Environment Template](#)
7. [Create the Code Signing Project](#)
8. [Edit an existing environment](#)
9. [Approve the Code Signing Project](#)
10. [Install and Configure the Venafi Crypto Service Provider \(CSP\)](#)
11. [Sign code using Venafi Code Signing](#)

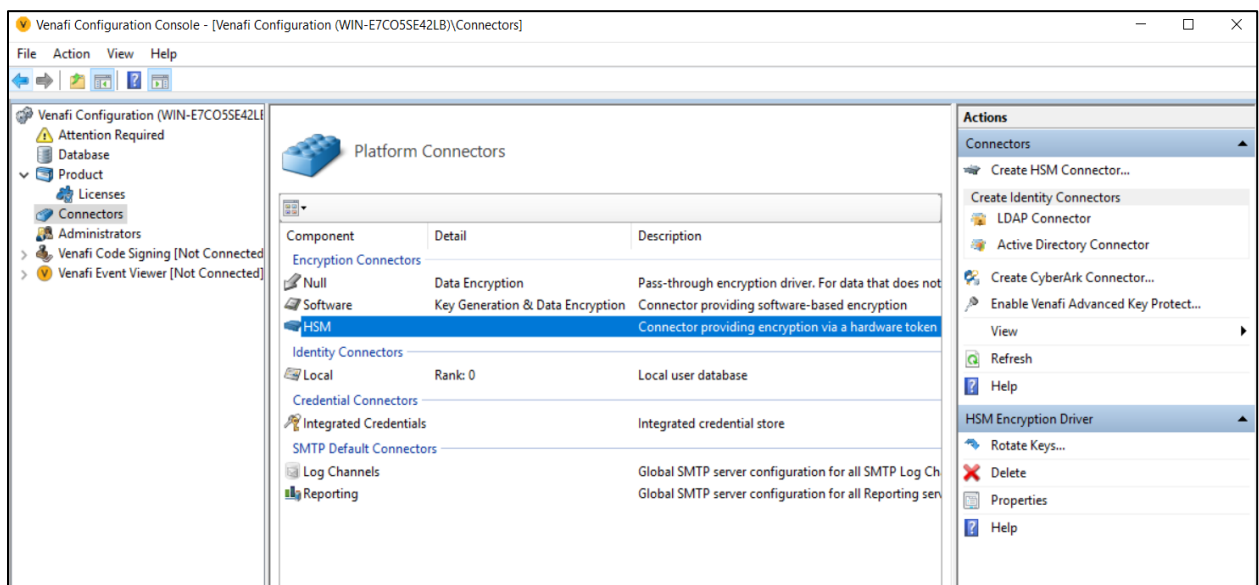
1. Enable Key Storage in HSM Connector

NOTE: Ensure that the HSM service client is configured on the host system and that the HSM partition or DPoD Luna Cloud HSM service is accessible over **lunacm**.

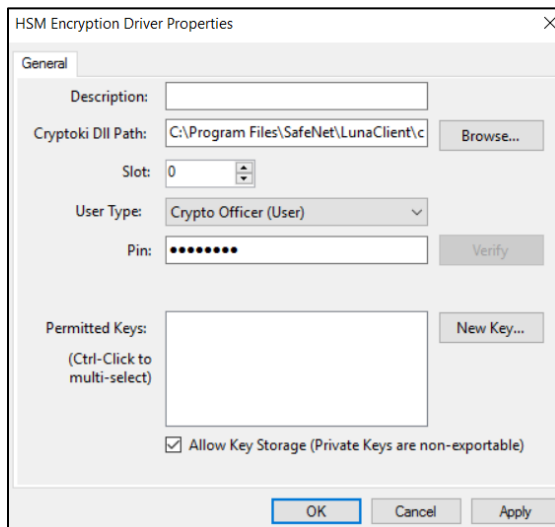
The HSM connector provides the HSM credential information to Venafi, allowing Venafi to access signing keys stored on the HSM. You create the HSM connector using the **Venafi Configuration Console**. To create the HSM Connector, refer to [Creating a HSM \(Cryptoki\) connector](#).

To enable Key Storage in HSM connector:

- a. Open the Venafi Configuration Console, and click the **Connectors** node from the **Venafi Configuration** pane.



- b. Select HSM connector under Encryption Connectors and click **Properties** in Actions pane. **HSM Encryption Connector Properties** screen will appear.
- c. Select the **Allow Key Storage** check box and click **Apply > OK**.



- d. Restart the Venafi services.

2. Enable Venafi Advanced Key Protect on Venafi Platform

To enable Venafi Advanced Key Protect, refer to [Enabling Venafi Advanced Key Protect](#) section.

3. Assign the Code Signing Administrator

The **Administrators** node allows you to view, assign, and delete Code Signing Administrator users. Add the Code Signing Administrator capability to an existing Venafi user. To assign the Code Signing Administrator:

- a. Click the **Administrators** node in Venafi Configuration Console.
- b. In the Actions panel, click **Add Code Signing Administrator**.
- c. Search for the user you want to assign, and click **Select**.

4. Create the Certificate Authority (CA) template

Each environment in a code-signing project requires a CA template. You can create a self-signed CA template, a DigiCert CA template, or a Microsoft CA template. Refer to [Venafi Documentation](#) for details.

5. Create the Signing Flow

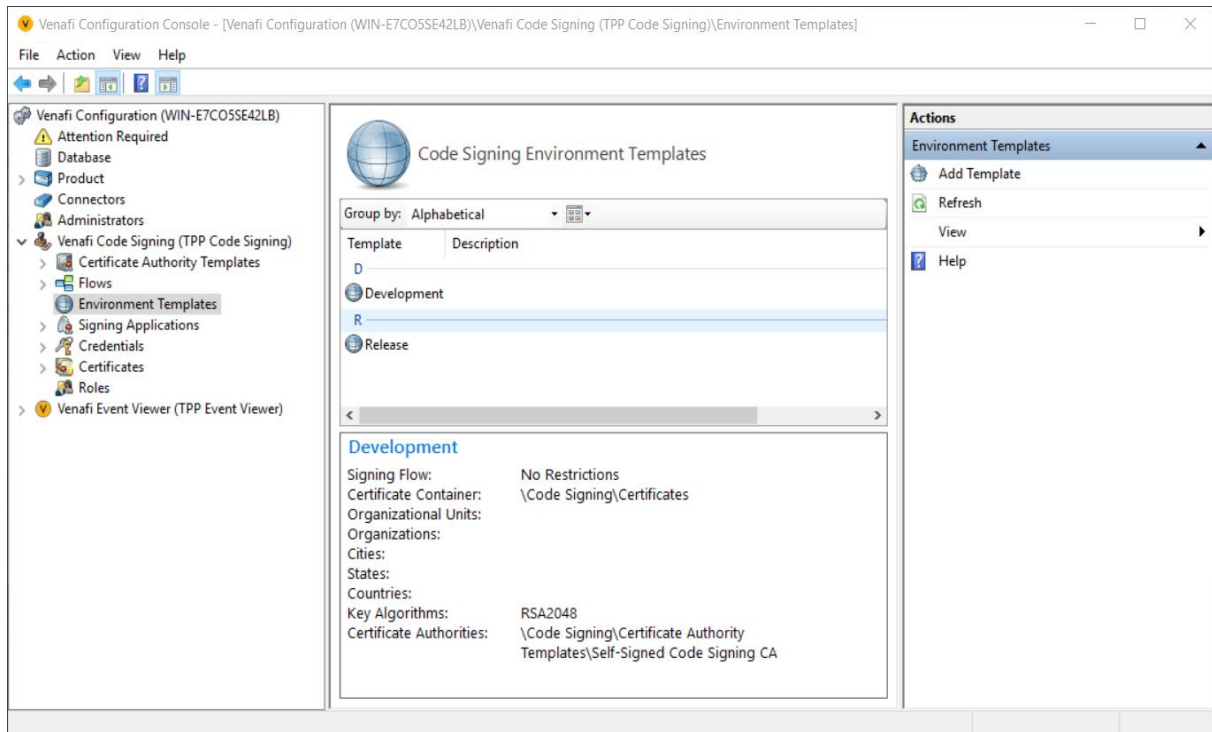
Flows in Venafi Code Signing define the approvals that must be granted before a signing can take place using a given private key. Create the Venafi approval flow to define the required approvals for code signing. To create the Signing Flow:

- a. In the Flows node, click Add a new Code Signing Flow in the Actions Panel.
- b. Specify the name of the flow and click **Create**.
- c. Record the Signing Flow name; it is required for an upcoming procedure.
- d. Configure the flow by adding Approvers. Refer to [Venafi Documentation](#) for details.

6. Create the Environment Template

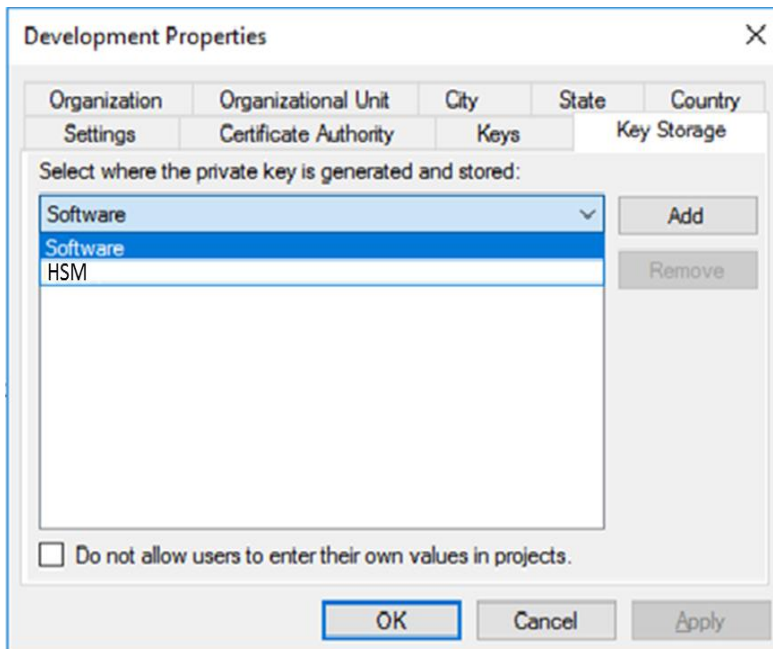
Code Signing Environment Templates allow the Code Signing Administrator to suggest or require specific values to be used in code signing Projects. Each project requires at least one environment. To create the Environment Template:

- a. In the **Venafi Code Signing** node of the Venafi Configuration Console, select **Environment Templates**.



- b. Click **Add Template** from the Actions panel.
- c. Specify the name of the template. The **Development Properties** wizard displays.
- d. Under **Settings**, specify **Description**, **Certificate Container** and the **Signing Flow** created in the previous procedure.
- e. Under the **Certificate Authority** tab, specify the CA template created in the earlier procedure.
- f. Under the **Keys** tab, select the RSA key length values you want to allow. This algorithm and key length appears as part of the certificate.

- g. Under the **Key Storage** tab, click on the drop-down menu and select the **HSM Connector** created in a previous procedure. Click **Add**.



- h. You can specify additional details, such as the **Subject Domain Name** of the certificate, in the remaining tabs, but they are not required to complete the integration.

7. Create the Code Signing Project

Code signing projects govern the use of private code signing keys. Code signing projects rely on settings defined in the Environment Template. To create the Code Signing Project:

- a. Log into Aperture by going to [https://\[IP_address_of_Venafi_TPP\]/Aperture/codesigning](https://[IP_address_of_Venafi_TPP]/Aperture/codesigning).
- b. Click on **Add Project** on the project list screen to open the project configuration wizard.
- c. Enter a **Project Name** and **Description**. Click **Next**. The option to select **Environment** to support with the Project appears.

NOTE: If you want to use an existing key and certificate, skip step d.

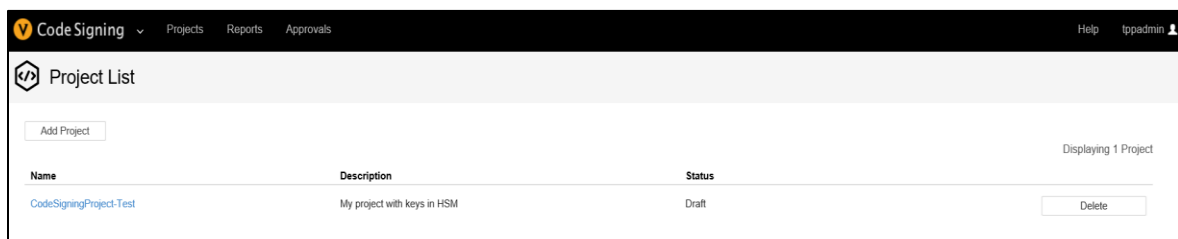
- d. If you want to create an environment that generates a new certificate and private key, click the **Add Environment** card.
 - i. From the **Environment Type** drop-down, select the type of environment.
 - ii. Click the **Certificate Provider** drop-down list, and select the certificate provider you want to associate with this environment. If only one certificate provider is assigned to this environment, that provider is automatically selected and the drop-down is not editable.
 - iii. In the **Environment Name** box, enter a name for this environment.
 - iv. Ensure that **Key Storage** location points to HSM connector.
 - v. Complete the remaining fields as per part of Subject DN of the certificate.
 - vi. Click **Add**.

- e. Click **Next**.
- f. Assign Users and Approvers to the project.
- g. Click **Next**.
- h. Optionally, if you want to restrict what signing applications are allowed to use this project, enter them in the **Permitted Applications** field.
- i. If you want to create new certificate and private key on approval, Click **Submit for Approval**. Skip the [Edit an existing environment](#) section and jump to the [Approving the Code Signing Project](#) section to proceed further.
- j. If you want to use existing key or certificate instead, click on **Save as Draft**.

8. Edit an existing environment

If you want to use existing key or certificate as a code signing key, follow these steps:

- a. From the project list, select the Draft project created in previous section.



- b. Click **Environments**.
- c. Select **Use Existing Key in HSM**.
- d. Select **Environment Template** from drop down and specify **Environment Name**.

- e. Click **OK**. **Import Key from Existing HSM** will appear.
- f. Select **HSM connector** name in **Key Storage Location** drop down.
- g. Select existing key pair on HSM in **Private Key** and **Public key** drop downs.

- h. Specify **Certificate Provider** and Certificate DN details in respective fields.

- i. Click **Save**.
- j. Click **Submit for Approval**.
- k. The project will be submitted for approval by the Code Signing Administrator.

9. Approve the Code Signing Project

After the code-signing project is submitted for approval, the Code Signing Administrators receive an email informing them that a project is ready for review. The Code Signing Administrators need to follow these steps for reviewing and approving the code-signing project:

- Sign into Aperture at [https://\[IP address of Venafi TPP\]/Aperture/codesigning](https://[IP address of Venafi TPP]/Aperture/codesigning).
- In the Code Signing menu, click **Approvals > Pending Approvals**.
- Click **Approve** for the Code Signing Project created in the previous procedure. At this point, if you have selected to generate new key pair on HSM, the keys are created.

```
lunacm:> partition contents

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:      RSA 2048 26956599
Handle:     618
Object Type: Private Key
Object UID: 5e0d00002e00000554380800

Label:      RSA 2048 26956599
Handle:     140
Object Type: Public Key
Object UID: 5d0d00002e00000554380800
```

This completes the configuration for Venafi Code Signing Project.

10. Install and Configure the Venafi Cryptographic Service Provider (CSP)

The Venafi Cryptographic Service Provider (CSP) is the bridge between the workstation on which code signing operations take place and the Venafi Platform server, which stores and manages use of private code signing keys.

Install the Venafi CSP on every workstation where code will be signed using private keys managed by Venafi Platform. The Venafi CSP communicates with the Venafi Platform server over a TLS-encrypted REST API.

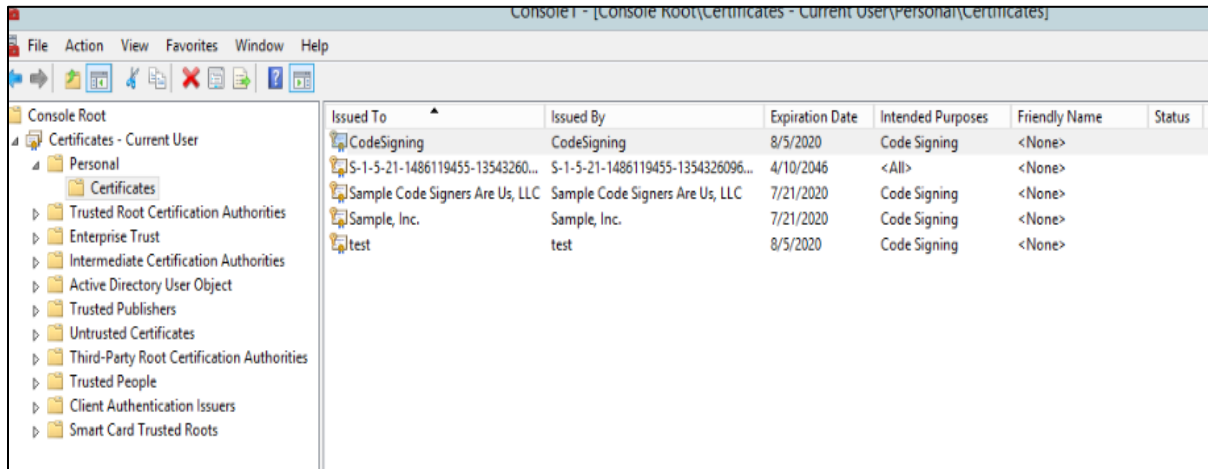
The Venafi CSP supports both CSP and KSP. The Venafi CSP only supports RSA certificates.

To install and configure the Venafi CSP:

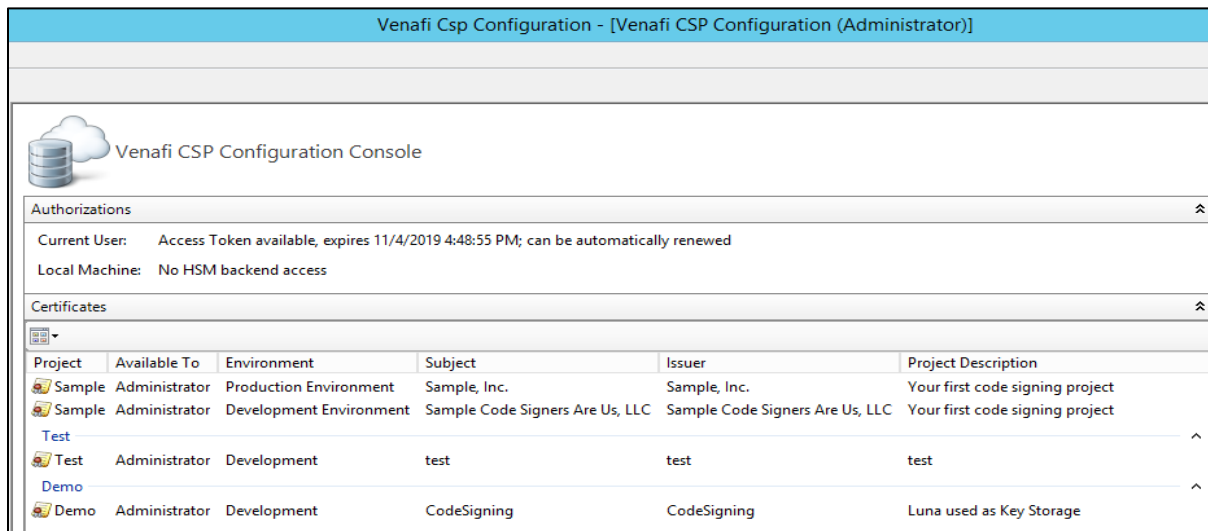
- a. Obtain **VenafiCSP-x64.msi** (64-bit Windows) or **VenafiCSP-x86.msi** (for 32-bit Windows).
- b. Run the CSP installation file as the administrator on client machine. The CSP installation wizard opens.
- c. Accept the license agreement, and click **Next**.
- d. Select the location where you want the CSP to be installed, and then click **Next**.
- e. Click **Install**. On the **Welcome** screen, select whether you want to use an answer file for this installation. Click **Next**.
- f. On the **Before You Begin** screen, verify that you have all the information you need to complete installation.
- g. On the **Host URLs** screen, enter the URL addresses for the **Authentication Server** and the **HSM Server**.
Authentication Server URL: `https://<IP_address_of_Venafi_TPP>/vedauth`
HSM Server URL: `https://<IP_address_of_Venafi_TPP>/vedhsm`
- h. Click **Next**.
- i. On the **Access Authorization** screen, enter your Trust Protection Platform user name and password. Check whether you want to enable access for the **Current User** only, **Local Machine** only, or both.
- j. On the **Configure CSP** screen, determine the location where the configuration progress and errors will be logged.
- k. Click **Finish**.

11. Sign code using Venafi Code Signing

When a Key User or a Local Machine is issued a grant, the associated certificates permitted to be used by that user or machine are installed in the CAPI store. These certificates can be used by the signing applications as code signing certificates.



The certificate and Project Details are visible in Venafi CSP Configuration Console and on the client machine.



This integration guide provides example material to sign applications:

Example 1: Using jarsigner

Example 2: Using signtool

Example 1: Using jarsigner

Execute **jarsigner** to sign .jar files on the target machine using the installed Code Signing Certificate.

```
C:\Program Files\Java\jdk1.8.0_101\bin>jarsigner.exe -storetype Windows-My -keystore NONE sample.jar -signedjar signedsample.jar CodeSigning
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after the signature
evocation date.

C:\Program Files\Java\jdk1.8.0_101\bin>jarsigner -verify signedsample.jar
jar verified.
```

Example 2: Using signtool

Execute **signtool** to sign .exe or .dll files on target machine using the installed Code Signing Certificate.

```
C:\Users\Administrator\Desktop>signtool sign /n "codesigning" sample.dll
Done Adding Additional Store
Successfully signed: sample.dll

C:\Users\Administrator\Desktop>signtool sign /n "codesigning" sample.exe
Done Adding Additional Store
Successfully signed: sample.exe
```

This completes the Venafi Code Signing integration with the Luna HSM or DPoD Luna Cloud HSM service.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.