This document provides a step by step guide for integrating SafeNet’s Luna SA 4 Hardware Security Module (HSM) with Venafi Encryption Director™ 6.

**Overview**

Venafi Encryption Director™ stores sensitive information such as logon credentials and private key material within it’s own database. This data is automatically encrypted by default using a symmetric key that is managed by the Microsoft Data Protection Application Program Interface (MS DPAPI). For customers that require additional security, Venafi Encryption Director provides a PKCS#11 driver that can be used to integrate with third party Hardware Security Module’s (HSM’s) such as the Luna SA 4 from Safenet. This provides the ability to configure Venafi Encryption Director to use keys stored on and managed by the HSM, thus truly separating the stored data from the encryption keys.

**About Venafi**

If you have any questions, feedback or suggestions regarding this product be sure to read the Help, Support & Feedback section. Thank you for purchasing this product and I hope you find it useful for your projects.

**About SafeNet**

If you have any questions, feedback or suggestions regarding this product be sure to read the Help, Support & Feedback section. Thank you for purchasing this product and I hope you find it useful for your projects.
1. Overview 2

2. Background 2

3. Pre-requisites 1

4. Components 2
   4.1 Installing the Windows Client 2
       4.1.1 Installation Steps 2
   4.2 Creating the NTLS Connection 6
       4.2.1 Configuration Steps 6
   4.3 Generating Test Keys 10
       4.3.1 Open a session with the HSM 10
       4.3.2 Logon to the HSM 12
       4.3.3 Generate test keys 13
   4.4 Configuring Venafi Encryption Director™ 14
1. Overview

This document provides details for integrating Venafi Encryption Director™ (VED) and the Luna SA 4 and 5 range of networked Hardware Security Modules (HSM's) from SafeNet.

2. Background

Venafi Encryption Director stores various credentials within its configuration database. By default, this data is encrypted using Microsoft’s Data Protection API (DPAPI) before it is stored. For organisations that require additional security, Venafi Encryption Director can be configured to encrypt this data to symmetric keys stored on an HSM. Thus, the data and the key used to encrypt the data are completely separate.

3. Pre-requisites

The following pre-requisites are assumed:

- Venafi Encryption Director has been installed and configured
- A SafeNet Luna SA 4 or 5 HSM has been installed and configured
- A suitable partition has been created on the HSM and the partition activated

**Luna HSM Partition List:**

<table>
<thead>
<tr>
<th>Partition SN:</th>
<th>150775008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Name:</td>
<td>ved</td>
</tr>
<tr>
<td>Activated:</td>
<td>yes</td>
</tr>
<tr>
<td>Auto Activation:</td>
<td>yes</td>
</tr>
<tr>
<td>Partition Owner Locked Out:</td>
<td>no</td>
</tr>
<tr>
<td>Partition Owner PIN To Be Changed:</td>
<td>no</td>
</tr>
<tr>
<td>Partition Owner Login Attempts Left:</td>
<td>10 before Owner is Locked Out</td>
</tr>
<tr>
<td>Crypto-User Locked Out:</td>
<td>no</td>
</tr>
<tr>
<td>Crypto-User Challenge To Be Changed:</td>
<td>no</td>
</tr>
<tr>
<td>Crypto-User Login Attempts Left:</td>
<td>10 before Crypto User is Locked Out!</td>
</tr>
<tr>
<td>Legacy Domain Has Been Set:</td>
<td>no</td>
</tr>
<tr>
<td>Partition Storage Information (Bytes):</td>
<td>Total=102701, Used=0, Free=102701</td>
</tr>
<tr>
<td>Partition Object Count:</td>
<td>0</td>
</tr>
</tbody>
</table>
4. Components

gfdgdf

4.1 Installing the Windows Client

This section provides a quick guide for installing the SafeNet LunaSA 4 Windows client.

4.1.1 Installation Steps

Step 1. Locate the Luna SA Client software and launch the installation program file.

Step 2. The wizard will present a list of installable components.

You only need the basic client components so leave all of the checkboxes unselected.

Step 3. The installation wizard will verify that only the client components will be installed.

This will start the installation wizard. Click the “Next” button.
Click the "Yes" button.

Step 4. The client installation wizard will start.

Click the "Next" button.

Step 5. You will be prompted to accept the license agreement. Click the "Yes" button.

Step 6. You will be prompted to choose the installation path for the client software. Click the "Next" button.
Step 7. You will be prompted to select the name of the client for the program files.

Click the “Next” button to select the default location.

Step 8. The installation wizard will continue to install the client into the selected location.

Click “Next” to select the default value.
You will be prompted once the setup is complete. Click the “Next” button.

Step 9. The installer will then ask if you wish to install any more components.

Click the “No” button.

Step 10. The installation will complete.

Click the “Finish” button.
4.2 Creating the NTLS Connection

This section provides a step by step guide for configuring the Network Transport Layer Security (NTLS) between the Windows client and the HSM.

This will consist of the following:-

- Download NTLS server certificate
- scp admin@192.168.1.249:server.pem 192.168.1.249.pem
- Trust NTLS server certificate
- vtl addServer –n 192.168.1.249 –c 192.168.1.249.pem
- Create NTLS client certificate
- vtl createCert –n 192.168.1.79
- Upload NTLS client certificate
- scp cert\192.168.1.79.pem admin@192.168.1.249:
- Register client certificate
- client register -client 192.168.1.79 -ip 192.168.1.79
- Assign client to partition
- client assignPartition –client 192.168.1.79 –partition mypartitionone
- Verify connectivity to partition from client
- vtl verify

4.2.1 Configuration Steps

Step 1. Download NTLS Certificate — Open a Windows command prompt and change directory to the where the Luna SA 4 client is installed.

Step 2. Trust NTLS Certificate — To trust the newly downloaded server certificate,

Download the NTLS server certificate using the following command:

ctp admin@10.1.2.110:server.pem 10.1.2.110

When prompted type the admin password for the HSM.

The server certificate will be downloaded to the local Windows machine.

Replace the 10.1.2.110 with the correct IP address for your SafeNet Luna 4 HSM.

Step 2. Trust NTLS Certificate — To trust the newly downloaded server certificate,
type the following command: -

vtl addServer -n 10.1.2.110 -c 10.1.2.110.pem

The HSM will then be trusted by the Windows client.

Replace the 10.1.2.110 with the correct IP address for your SafeNet Luna 4 HSM.

Step 3. Create NTLS client certificate — To create a new NTLS client certificate,

type the following command: -

vtl createCert -n 10.1.2.200

A new client private key and certificate will created in the “cert\client” directory.

Replace the 10.1.2.200 with the correct IP address for your Windows machine.

Step 4. Upload NTLS client certificate — To upload the newly generated certificate to the HSM,
Type the following command:

```
cert client\10.1.2.200.pem
```

When prompted type the admin password for the HSM.

The Windows client certificate will be uploaded to the HSM.

Replace the 10.1.2.200 with the correct IP address for your Windows machine. Replace the 10.1.2.110 with the correct IP address for your HSM.

Step 5. Register client certificate — To register the client certificate on the HSM open an SSH connection to the server using the “putty” utility and logon using the admin account.

Type the following command:

```
client register -client 10.1.2.200 -ip 10.1.2.200
```

The Windows client will be registered on the HSM.

Replace the 10.1.2.200 with the correct IP address for your Windows machine.
Step 6. Assign client to partition — To assign the Windows client to the HSM partition,

```
G:\Program Files\Luna\vtl verify
The following Luna SM Slots/Partitions were found:
Slot  Serial #   Label
---  --------  -----
   1  319300001  ved

G:\Program Files\Luna>
```

Type the following command:

```
client assignPartition -client 10.1.2.200 -partition ved
```

The Windows client will be assigned to the HSM partition.

Step 7. Verify connectivity to partition from client — To verify connectivity from the Windows client to the HSM,

```
vtl verify
```

The command should then return the Slot, Serial # and Label for the HSM.
4.3 Generating Test Keys

4.3.1 Open a session with the HSM

Step 1. Run the “ckdem” utility — Open a command prompt and navigate to the “c:\program files\LunaSA” directory.

Type the following command to start the utility:

`ckdemo`

The utility will then display a list of numbered options as shown below.
Step 2. **Start a new session** — Open a new session with the HSM.

Type the following command:

```
1 <enter>
```

The utility will then display a list of available slots on the HSM.

Step 3. **Choose the HSM slot number** — Slot 1 was used for the purposes of this integration testing.

Type the following command:

```
1 <enter>
```

You will then be prompted to select a user type.

Step 4. **Select a user** — “Normal User” was used for the purposes of this integration testing.
The utility will then return a list of available options.

### 4.3.2 Logon to the HSM

#### Step 1. Login to the HSM — Select option 3 (Login) to login to the HSM.

Type the following command:

3 <enter>

You will then be prompted to select a user type.

#### Step 2. Select the user — Select option 1 (Crypto-Officer).

Type the following command:

1 <enter>

You will be prompted to enter a PIN which is the partition challenge.

#### Step 3. Enter the partition PIN — Enter the PIN for the partition challenge.

Type the following command:

SafeNet123 <enter>

Replace “SafeNet123” with the correct pin number.

The utility should now return a “CKR_OK” message.

### 4.3.3 Generate test keys

#### Step 1. Generate key — Use the “Simple Generate Key” option 45 to create a new symmetric key on the HSM.

Type the following command:

45 <enter>

You will be prompted to enter the type of key.

#### Step 2. Select key type — Select a suitable key type. An AES key was used for the purposes of this integration testing.
The utility should now return a “CKR_OK” message.

Step 1. Login to the HSM — Login to the HSM via SSH and verify that the “Partition Object Count” has increased.

Type the following command:

16 <enter>

You will be prompted to enter a number of other key attributes.

Type the following commands:

32 <enter>
1 <enter>
1 <enter>
1 <enter>
1 <enter>
1 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>
0 <enter>

Type the following command:

par show <enter>

The “Partition Object Count” should reflect the number of keys that have been generated.
4.4 Configuring Venafi Encryption Director™

This section provides information for configuring Venafi Encryption Director™ to use Symmetric encryption keys stored on the HSM. It assumes that the SafeNet Luna SA client has been installed and the connectivity verified using the “vtl verify” command.

**Step 1. Verify communications to the HSM —** Open a windows command prompt and navigate to the directory where the LunaSA Windows client is installed. e.g. C:\Program Files\LunaSA.

Type the following command:

```
vtl verify
```

If the communications between the Windows server and the HSM is configured correctly, the command should then return the Slot, Serial # and Label for the HSM.
Click add, then select the “PKCS11 HSM” option.

Step 3. Navigate to Director’s “Encryption” tree —

Click add, then select the “PKCS11 HSM” option.

Step 4.