

Luna HSM

1. Extract Setup Files

1.1 Unzip setup-CodeSign-Luna.zip

- This archive contains the main Luna client and configuration files.
- Right-click the zip file and choose Extract All.

1.2 Unzip cvclient-min.zip inside the same folder

- It includes additional client-side components required for Luna connectivity.
- Extract its contents directly inside setup-CodeSign-Luna (not in a subfolder).

2. Set Up Environment

2.1 Open an Administrator Command Prompt

- Required for executing environment scripts with elevated privileges.

2.2 Navigate to the folder and run:

`setenv.cmd`

- Sets up environment variables necessary for Luna client operations.

2.3 Verify Luna Client HSM Connection

`lunacm`

- It opens the Luna command-line tool to check HSM availability and status.
- Use the 'partitions' command to see available partitions and labels.

3. Set up Cygwin and SSL Directory

3.1 Unzip the Cygwin folder to the C: Drive

- Provides a Linux-like environment for OpenSSL operations.

3.2 Create an SSL directory in C: Drive

```
mkdir C:\\ssl
```

- A placeholder for storing any custom SSL configurations or scripts.

3.3 Update Windows System Environment Variables

- Ensures OpenSSL commands recognize the Cygwin SSL binaries.
- Add the following to the Path: C:\\cygwin\\usr\\local\\ssl\\bin

4. Modify the cryptoki.ini Configuration File

4.1 Open the cryptoki.ini file

- Main configuration file for the Luna client cryptographic engine.

4.2 Modify or Add the Below Section:

```
[GemEngine]
```

```
LibPath = C:\\Users\\Administrator\\Desktop\\setup-CodeSign-Luna\\cryptoki.dll
```

```
LibPath64 = C:\\Users\\Administrator\\Desktop\\setup-CodeSign-Luna\\cryptoki.dll
```

```
EnableDsaGenKeyPair = 1
```

```
EnableRsaGenKeyPair = 1
```

```
DisablePublicCrypto = 1
```

```
EnableRsaSignVerify = 1
```

EnableLoadPubKey = 1

EnableLoadPrivKey = 1

DisableCheckFinalize = 1

DisableEcdsa = 1

DisableDsa = 0

DisableRand = 0

EngineInit = "example":0:0:passdev=console

EnableLoginInit = 1

- Replace "example" with the partition name obtained via lunacm.
- Ensure that the cryptoki.dll path is correct for both LibPath and LibPath64.

5. Verify OpenSSL and Gem Engine

5.1 Open a new Command Prompt

- Test the gem engine to confirm successful configuration.

openssl engine gem -t

5.2 Generate an RSA Key Using the HSM

- Uses the HSM-backed engine to generate a 2048-bit RSA private key securely.

openssl genrsa -engine gem 2048

6. Enable/Disable HSM Logging

6.1 Enable logging support

- Turns on detailed cryptographic operation logging for troubleshooting.

vtl cklogsupport enable

6.2 Disable logging support

- Turns off logging when no longer needed.

vtl cklogsupport disable