Prerequisites:

To get the PKCS#11 Engine working smoothly with your Securosys Primus HSM and Encryption Consulting's CodeSign Secure, you'll need a few key things. Here are the steps to install the resources that are essential for setting up the **Windows** environment:

1. Securosys PKCS#11 Provider

The Securosys PKCS#11 Provider (PrimusAPI PKCS#11) is required to interface with the Primus HSM. This library enables communication between your applications and the HSM via the PKCS#11 standard.

Installation Steps:

Step 1: Obtain the Download Link

- Access the Securosys Support Portal to retrieve the **PrimusAPI_PKCS11-DownloadLink-v#.txt** file, which contains the download credentials and version details. You'll need an account on the Securosys Support Portal. If you don't have one, contact Securosys support to gain access.

Step 2: Download the Provider

- Use the curl command to download the provider package. Open a Command Prompt and run the following commands:
  - set USER=support.reader.p11
  - set CRED=<your_credentials>
  - set VERSION=v2.3.4
  - curl -L -o "PrimusAPI_PKCS11-%VERSION%.zip" https://%USER%:%CRED%@securosys.jfrog.io/artifactory/p11/PrimusAPI_PKCS11-%VERSION%.zip

  Replace <*your_credentials*> with the value from the text file.

- Alternatively, you can download the ZIP file directly from the Securosys JFrog Artifactory using a browser here
  - Username: support.reader.p11
  - Password: Take the value from the **PrimusAPI_PKCS11-DownloadLink-v#.txt** file.

Step 3: Install the Provider

- Extract the downloaded ZIP file and locate the MSI installer (e.g., PrimusAPI_PKCS11-<version>-win64.msi) in the extracted folder.

- Double-click the MSI file to run the installer, and follow the prompts to install, ensuring you install to the default location (C:\Program Files\Securosys\Primus P11) unless otherwise required.
  Note: Back up any existing primus.cfg and .secrets.cfg configuration files in the installation directory, as the installer may overwrite them.

Step 4: Configure Environment Variable

- Add the directory location of the installed files to the system PATH for easier access.
    - C:\Program Files\Securosys\Primus P11

Step 5: Verification

- Open a new Command Prompt and run the following command to test the installed tools:
    - ppin -v

2. OpenSSL 3.x:

OpenSSL 3.x is required for cryptographic operations and to leverage the PKCS#11 provider with the Securosys HSM.
Installation Steps:

Step 1: Download OpenSSL

- Download the latest 64-bit OpenSSL 3.x installer for Windows using this link.

Step 2: Install OpenSSL

- Run the downloaded installer with administrative privileges.
- Choose the default installation directory (C:\Program Files\OpenSSL-Win64) unless you have specific requirements.

Step 3: Configure Environment Variable

- Add the OpenSSL binary directory to the system PATH:
    - C:\Program Files\OpenSSL-Win64\bin

Step 4: Verification

- Open a new Command Prompt and run the following command to test openssl installation.
    - openssl version

3. **OpenSC PKCS11 Tool:**

   The OpenSC PKCS#11 Tool provides utilities like pkcs11-tool to manage keys and perform operations on the HSM via the PKCS#11 interface.

   Installation Steps:

   Step 1: Download OpenSC

   - Download the latest OpenSC Windows installer from the OpenSC GitHub releases page here.

   Step 2: Install OpenSC

   - Run the MSI installer as an administrator to the default location (C:\Program Files\OpenSC Project\OpenSC).

   Step 3: Configure Environment Variable

   - Add the OpenSC tools directory to the system PATH:
     - C:\Program Files\OpenSC Project\OpenSC\tools\

   Step 4: Verification

   - Open a new Command Prompt and run the following command to test pkcs11-tool
     - pkcs11-tool --version

4. **Microsoft Visual Studio Build Tools**

   Microsoft Visual Studio Build Tools are required to compile the OpenSC PKCS#11 Wrapper Library (libp11) on Windows

   Installation Steps:

   Step 1: Download Visual Studio Build Tools

   - Download the Microsoft Build Tools for Visual Studio 2022 using this link.

   Step 2: Install Build Tools

   - Run the installer (vs_buildtools.exe) with administrative privileges.

   Step 3: Verify Installation

   - Open the "**x64 Native Tools Command Prompt**" from the Start menu and run

- nmake /?

This should display the help for the nmake utility, confirming the build tools are installed.

NOTE: "x64 Native Tools Command Prompt" should be present inside C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Visual Studio 2022\Visual Studio Tools\VC

5. **OpenSC PKCS#11 Wrapper Library**

The OpenSC PKCS#11 Wrapper Library (libp11) provides the PKCS#11 engine plugin (pkcs11.dll) for OpenSSL to interact with the HSM.

Installation Steps:

Step 1: Download the Source Code

- Clone the OpenSC/libp11 repository from GitHub or download it as a ZIP file.
- Clone using Git (if installed):
  - git clone https://github.com/OpenSC/libp11.git C:\Users\<Username>\source\repos\libp11
- Or download the ZIP from this link and extract it to C:\Users\<Username>\source\repos\libp11.

Step 2: Compile the Library

- Open the "x64 Native Tools Command Prompt".
- Navigate to the libp11 directory
  - cd "C:\Users\<Username>\source\repos\libp11"
- Run the nmake command to build the library
  - nmake /f Makefile.mak OPENSSL_DIR="C:\Program Files\OpenSSL-Win64" BUILD_FOR=WIN64
- **NOTE:** Ensure OPENSSL_DIR points to your OpenSSL installation directory.

Step 3: Verify Compilation

- Check for the pkcs11.dll file in the libp11\src folder. This is the OpenSC PKCS#11 Engine Plugin.

Step 4: Copy the SRC folder

- Copy the src folder that you just created to your OpenSSL bin directory, i.e., C:\Program Files\OpenSSL-Win64\bin

Configuration

After installing the prerequisites, you need to configure the Securosys PKCS#11 Provider, OpenSSL, and the OpenSC PKCS#11 Wrapper Library to enable communication with your Securosys Primus HSM.

1. Configure the Securosys PKCS#11 Provider

The Securosys PKCS#11 Provider requires configuration files (primus.cfg and .secrets.cfg) to specify the HSM connection details, such as the IP address, port, secrets, and logging settings.

Steps:

Step 1: Locate the Configuration File (primus.cfg)

- Navigate to the Securosys PKCS#11 Provider installation directory, typically:
  - C:\Program Files\Securosys\Primus P11

Step 2: Edit the HSM CONFIGURATION SECTION with HSM Details

- Open primus.cfg in a text editor with administrative privileges.
- Add or update the following configuration inside the "HSM CONFIGURATION SECTION", replacing placeholders with your HSM details:

```
hsm0:
{
  host = "HSM HOSTNAME (like a-api.cloudshsm.com)";
  port = "HSM PORT (like 2310)";
  slots:
  {
    slot0:
    {
    client_id  = "Client_ID1 (like Client_0)";
    user_name  = "PARTITION_NAME1";
    proxy_user = "SERVICE_USER"; /* or remove if no proxy needed */
    id = 1;
    }; /* end slot0 */

    slot1:
    {
    client_id  = "Client_ID2";
    user_name  = "PARTITION_NAME2";
    proxy_user = "SERVICE_USER"; /* or remove if no proxy needed */
```

```
    id = 2;
    }; /* end slot1 */
  }; /* end slots */
}; /* end hsm0 */
```

Step 3: Edit the LOG CONFIGURATION SECTION with Logging Details

- Add or update the following configuration inside the "LOG CONFIGURATION SECTION", replacing placeholders with your Logging details:

```
log:
 {
  file            = "C:\Program Files\Securosys\Primus P11\primus.log";  /*
optional for windows */
  trace_linenumber    = false;
  trace_timestamp    = true;
  trace_function     = true;
  trace_inout       = false;
  trace_pid         = true;
  trace_filename     = false;
  trace_mask        = 0x01;
  trace_level       = 6; /* 0-7 log level details */
 }; /* end log */
```

Step 4: Setting up Permanent Secret in .secrets.cfg file

- Open a Command Prompt and navigate to the Primus P11 directory (if not set in the Environment Variable Path) using the below command:
    - cd C:\Program Files\Securosys\Primus P11
- Replace the placeholder value with the HSM user_name value that you have set in primus.cfg file and run the following command:
    - ppin -a -e <HSM_USERNAME>

  Setup the PKCS11_PIN for mentioned HSM_USERNAME

  NOTE: Ensure that you have read and write permissions to modify the .secrets.cfg file with a permanent secret.

Step 5: Verify connection with HSM

- Open a Command Prompt and navigate to the Primus P11 directory (if not set in the Environment Variable Path) using the below command:

    - cd C:\Program Files\Securosys\Primus P11
- Run the ppin tool to test the HSM connection:
    - ppin -t

2. Configure OpenSSL to Use the PKCS#11 Engine

OpenSSL must be configured to load the Securosys PKCS#11 Provider (primusP11.dll) and the OpenSC PKCS#11 Engine Plugin (pkcs11.dll) to perform cryptographic operations with the HSM.

Steps:

Step 1: Locate the OpenSSL Configuration File (openssl.cfg)

- Find the OpenSSL configuration file:
    - C:\Program Files\Common Files\SSL

Step 2: Edit the OpenSSL Configuration

- Open openssl.cfg in a text editor with administrative privileges.
- Add the following at the top of the file to enable dynamic engine loading:
    - openssl_conf = openssl_init
- Add the following at the end of the file to configure the PKCS#11 engine:

```
[openssl_init]
engines = engine_section

[engine_section]
pkcs11 = pkcs11_section

[pkcs11_section]
engine_id = pkcs11
dynamic_path = "C:\\Program Files\\OpenSSL-Win64\\src\\pkcs11.dll"
MODULE_PATH = "C:\\Program Files\\Securosys\\Primus P11\\primusP11.dll"
PIN = "PKCS11_PIN"
init = 0
```

dynamic_path: Path to the OpenSC PKCS#11 Engine Plugin (pkcs11.dll) compiled in the prerequisites.
MODULE_PATH: Path to the Securosys PKCS#11 Provider DLL.
PIN: PKCS11_PIN value for the required HSM username/partition set during the permanent secret steps.

Step 3: Verify OpenSSL Configuration and Connection

- Open a Command Prompt and run:
  - openssl engine pkcs11 -t
- Expected output confirms the PKCS#11 engine is available:

  (pkcs11) PKCS#11 engine

  [available]

3. Test the PKCS#11 Interface with pkcs11-tool

Use the OpenSC pkcs11-tool to verify that the PKCS#11 interface can communicate with the HSM.

Steps:

Step 1: Run pkcs11-tool

- Open a Command Prompt and navigate to the OpenSC tools directory, if not set in the Environment Variable Path:
  - cd “C:\Program Files\OpenSC Project\OpenSC\tools”
- Execute the following command to list available slots on the HSM:
  - pkcs11-tool --module "C:\Program Files\Securosys\Primus P11\primusP11.dll" --list-slots

4. Configure CodeSign Secure

CodeSign Secure requires configuration to connect to the Securosys Primus HSM for secure code signing operations. The **app-config.properties** file specifies the various details for a successful connection to Securosys Primus HSM.

Steps:

Step 1: Locate the app-config.properties File

- Navigate to the CertificateManagement folder inside the CodeSign Secure installation directory and locate the app-config.properties file, typically:
  - C:\CodeSignSecure\src\CertificateManagement

Step 2: Update the HSM Details Fields

- Open app-config.properties in a text editor with administrative privileges.
- Update the following fields, replacing placeholders with your HSM connection details:

HSM_LIB_PATH_SECUROSYS=<Path of primusP11.dll file>

HSM_PIN_SECUROSYS=<PKCS11_PIN for required partition/username>

HSM_TOKEN_SECUROSYS=<HSM Partition Name/User Name>

HSM_SLOT_SECUROSYS=<HSM Partition Slot Number>

- Save the file with the modified details.