IBM Security Secret Server
Version 10.8

HSM Integration Guide

Contents

Last updated: June 23, 2020

Introduction

Secret Server integrates with hardware security modules, or HSMs, to provide additional security of Secret Server's encryption key. When Secret Server is configured to use an HSM, the encryption key is protected by the HSM. HSMs offer several security features that traditional servers cannot. Depending on the model and design of the HSM, most HSMs are designed to be physically tamper-proof. HSMs may also be independent hardware that are on a network, which allows physically placing the HSM is a more secure location that might otherwise be too inconvenient for a server.

To provide broad support for HSMs, Secret Server supports any HSM that can be configured with Microsoft's Cryptography Next Generation provider, or CNG. CNG is a layer provided by Windows Server 2008 and later that HSM manufacturers can interface with. If your HSM properly supports CNG and supports the right algorithms, Secret Server will be able to utilize your HSM.

CNG provider installation and configuration varies from HSM to HSM, however, documentation is available from each HSM vendor on how to correctly install CNG providers.

HSM Requirements

Each HSM must provide support for certain algorithms through CNG.

- **RSA 4096** – support for RSA with 4096-bit keys is required. The HSM must also support RSA for encryption and decryption, in addition to signing.
- **PKCS#1 v1.5 Padding** – The HSM must support PKCS#1 v1.5 padding for RSA encryption.

Additionally, closely follow the requirements and recommendations of the HSM vendor for things such as minimum latency, redundancy, and operating environment.

Due to limitations of the account, the NETWORK SERVICE account is not supported as an account for the IIS Application Pool. It is recommended to configure Secret Server's Application Pool as a service account.

In the advanced settings for the application pool, set "Load User Profile" to true.

Note: Some HSM CNG providers interfere with each other. It is recommended that no more than one HSM CNG provider is configured on a Windows installation at a time.

Silent HSM Operation

Because Secret Server is a web application with no one physically present at the server at most times, Secret Server interacts with the HSM in “silent” mode. This will prevent the HSM from attempting to interact with any users logged onto the server.

Some HSM features require interaction. If the HSM is configured in such a way that requires interaction, Secret Server will be unable to communicate with the HSM and fail during the configuration steps.

An example of such a configuration is Operator Card Sets in Thales network HSMs. If the Thales CNG provider is configured to use an Operator Card Set, or OCS, for key protection instead of Module protection, someone must be physically present at the HSM and the Server to insert their operator card when the key is needed. If the OCS quorum is more than a single card, Secret Server cannot interact with the HSM because it requires inserting and removing the OCS cards.

It is recommended that Thales’ CNG provider is configured to use Module protection instead of an OCS. It is possible to use an OCS with Secret Server if the quorum is exactly one card and the card is left in the HSM at all times.

It is recommended to consult your HSM vendor and their documentation to ensure that the HSM and their CNG provider are able to operate in silent mode and are configured to do so.

Configuring HSM Integration

To configure the HSM integration, go to the **ADMIN** menu and click **Configuration**, then select the **HSM** tab. This will start the HSM wizard, which will guide the process of selecting the HSM's CNG provider.

The list of available CNG Providers is done by querying for the list of registered CNG providers. Each provider must correctly report that it is a "Hardware" provider, and that it is not a Smart Card reader. If an error occurs while querying the CNG provider for its properties, it will not appear in the list, however the error is reported to Secret Server's system log. If the desired CNG provider does not appear in the list of CNG providers, ensure that the CNG provider is correctly registered and that IIS has been restarted after the CNG provider is registered. Also check that an error is not occurring while querying the HSM by examining the system log.

Once the CNG providers are selected, Secret Server will simulate encryption and decryption operations and verify the results to check that it is functioning properly. The final step will be to verify the selected providers, and then enable HSM integration. Detailed steps are provided throughout the HSM configuration wizard.

Securing HSM Integration

The wizard to enable and disable HSM integration is protected by the “Administer HSM” role permissions in Secret Server. These permissions should be carefully assigned – if at all. Additionally, an Event Subscription can be created that sends alerts when this role permission is assigned or unassigned from a role.

Configuring the HSM also has its own Event Subscriptions for when the HSM integration is enabled or disabled.

Additionally, an application setting can be added to Secret Server to prevent changes to HSM configuration. Disabling and enabling this requires direct access to the file system where Secret Server is installed.

To enable this, edit the web-appSettings.config file within Secret Server to contain a key called **LockHsmConfiguration** with a value of **True** as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<appSettings>
    <add key="LockHsmConfiguration" value="True" />
</appSettings>
```

This will prevent access to the HSM configuration pages regardless of role permissions. The only way to gain access is to remove this setting, thus proving you at least have access to the server where Secret Server is installed.

HSM Redundancy

This varies from HSM to HSM, and the vendor's documentation on how to back up the HSM should be referenced. Backups are typically either made to common file location, or another HSM, or onto a smart card with the HSM's built-in smart card reader.

As long as the CNG provider is installed on the server and a key exists on the HSM with the same identifier, Secret Server will attempt to use that key.

Testing HSM CNG Configuration

Secret Server does its own testing and verification of the HSM and its CNG provider before the HSM integration can be enabled. To further diagnose any issues with the HSM, the **certutil** command line utility that is part of Windows can test the HSM with the **–csptest** option specified. An example output may contain something like this:

```
Provider Name: SafeNet Key Storage Provider
      Name: SafeNet Key Storage Provider
……
Asymmetric Encryption Algorithms:
   RSA
    BCRYPT_ASYMMETRIC_ENCRYPTION_INTERFACE -- 3
    NCRYPT_ASYMMETRIC_ENCRYPTION_OPERATION -- 4
    NCRYPT_SIGNATURE_OPERATION -- 10 (16)

    NCryptCreatePersistedKey(SafeNet Key Storage Provider, RSA)
      Name: cngtest-6166f8fe-8caf-4e30-8e5c-a-24575
      ……
    Pass
```

Examine the output of the test by looking for your CNG Provider Name for your HSM and verifying the result. It is recommended that this test be run using the same account as the Application Pool Secret Server is using. If the testing tool reports errors, consult your HSM's vendor or documentation for resolution.