Thycotic

Secret Server

v10.1

Integration Guide

Utimaco HSM

utimaco®

Imprint

Copyright 2020	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	06/10/2025
Status	**PUBLISHED**
Document No.	IG-2025-0005

Table of Contents

1 Introduction

This document will guide you through the integration of a Utimaco CryptoServer (HSM, hardware security module) into the Thycotic Secret Server runtime, using the Microsoft CNG provider. This guide is targeted at version 10.1.0023 (Premier) of the Secret Server, for Windows OS.

For guidance on the base installation and configuration of the Secret Server, please see the installation media supplied with that application. The integration steps below assume at least a basic knowledge and configuration of Secret Server IIS web applications.

This document is intended to be used as a quick guide in conjunction with Utimaco's CSP-CNG documentation. For more detailed information on specific topics, please refer to the corresponding guides available.

2 Requirements

2.1 Utimaco CryptoServer

This document assumes an install location of `C:\CryptoServer\`, and uses the SecurityServer-V4.10.x standard installation. Note that this Integration Guide is a quick introduction and how-to, which should be used in conjunction with Utimaco's CSP-CNG manual found in the directory

`C:\CryptoServer\Documentation\Crypto_APIs\CSP-CNG`

Partners using earlier versions of SecurityServer (V4.01.x or earlier) should refer to that version's CSP-CNG documentation for guidance.

2.1.1 Setting up the environment

To allow the library to find the correct configuration file, set the CS_CNG_CFG environment variable to point at it. If you have installed using the SecurityServer installer application, this will have been set for you, and will point at the indicated file:

>_ Console

```
C:\> set CS_CNG_CFG=C:\ProgramData\Utimaco\CNG\cs_cng.cfg
```

If your CryptoServer cluster includes multiple devices, for load balancing, failover or high-availability, it is recommended that you have/add the following values in your configuration:

>_ Console

```
KeysExternal = true
KeyStore = C:\CryptoServer\CNG\keys
# list all devices, each to its own line:
Device = 288@<ipaddr_1>
Device = 288@<ipaddr_2>
# and so on
```

3 Configuration

3.1 Adding the Utimaco CNG Provider

Thycotic Secret Server will attach to the CryptoServer cluster via the CNG provider, based on the registry configuration (SecurityServer versions 4.01 or earlier) or configuration file (SecurityServer 4.10 or later). Whether this is a single device or a cluster of devices will depend on the local configuration.

Please see the Utimaco documentation for use and deployment of the CSP/CNG utilities. How these are configured will depend on the version of SecurityServer you are using. Versions prior to 4.10 use a control panel applet that must be run as root. Please see the installation directory, for

`Documentation\Crypto_APIs\CSP-CNG\CryptoServer_CSP-CNG.pdf`

From version 4.10, the providers rely on a text configuration file rather than on the registry, which simplifies unattended deployment in virtualized environments. For the documentation, see the installation directory, for

`Documentation\Crypto_APIs\CSP-CNG\CryptoServer_Manual_CSP_CNG.pdf`

Note that after the cs2cng.dll Provider has been registered, you must restart IIS before it will be visible within.

3.2 Installing the Secret Server and Licensing

Note that the basic license (which may have been provided for eval purposes, for example) does not provide the nesessary rights to use an HSM. Consequently, use of a CryptoServer under the application requires the "Enterprise Plus" version license.

Install the Thycotic application using their installers. The `.exe` will install the necessary packages and dependencies as needed within the IIS framework, and then launch the second half of the installation process within the IIS framework directly.

3.3 Adding support for the CryptoServer

Log in to the Secret Server application with administrator access. In the ADMIN menu, click Configuration, then select the HSM tab. When ready, click the **Next** button, and the application will look for valid Key Storage Providers.

The tab will present a list of discovered, hardware (not smart-card) based CNG service providers. Select the **Utimaco CryptoServer Key Storage Provider** option, and choose a key size of 2048 or 4096. Click **Next**.

If the **Utimaco CryptoServer Key Storage Provider** option is not available, the most likely problem is a mis-configured `CS_CNG_CFG` file, which may point at a non-existant log file, or at an off-line CryptoServer cluster, or the default user login does not exist on the device(s) targeted.

If the option is there, but the initial tests (performed by the application) do not succeed, you should check two places for hints as to why. For CryptoServer specific error results, see the log file `cs_cng.log` found in the `Logfile` directory (defined in the `CS_CNG_CFG` file). For Thycotic Secret Server specific error results, see the SecretServer system log.

Click **Next** to configure the application to use the storage provider. When it returns correctly, it states "*The HSM is now enabled*."

You will need to make a backup of the `C:\inetpub\wwwroot\SecretServer\encryption.config` after the above, as the file will have been re-encrypted using the newly generated HSM-stored key. Use `cngtool ListKeys` to display the newly created key name (a UUID).

The final step required is to "Recycle the Application Pool". This is an IIS Manager job. If you try to navigate off the application page, you may notice a warning at the top, that includes "no secrets may be modified", and the page returns without navigating away.

Use the Windows **Start** menu to call up the IIS Manager. On the left, in the Connections panel, click on the "Application Pools" item. The list of active Application Pools will appear in the main field, right-click the SecretServer item, and select **Recycle...** .

The SecretServer application will now let you pass on from the **Success** screen.

4 Troubleshooting

4.1 Connection Problems

If you have problems connecting to the HSM, it is a good idea to make sure that your HSM is configured properly.

- Verify your HSM is running

>_Console

```
set CRYPTOSERVER=288@<ipaddr>
```

```
csadm GetState
```

- Make sure your configuration file is configured according to your HSM (e.g. you typed in the correct IP address)

>_Console

```
cngtool ProviderInfo
```

5 Further Information

This document forms a part of the information and support which is provided by Utimaco IS GmbH.

All Utimaco CryptoServer documentation is available at the Utimaco IS GmbH website: https://hsm.utimaco.com, in the support portal (registration, login required).