Venafi

Trust Protection Platform

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-2025-0025

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available from Utimaco's web site at https://utimaco.com/

1.1 About This Guide

This guide provides an integration guide explaining how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with Venafi Trust Protection Platform (VTPP).

1.1.1 Target Audience for This Guide

This guide is intended for administrators of Venafi Trust Protection Platform and of Utimaco HSMs.

1.1.2 Contents of This Guide

After the introduction this guide is divided up as follows:

Chapter 2 Overview

Chapter 3 Integration Requirements and Prerequisites

Chapter 4 PKCS#11 Configuration

Chapter 5 Configure Venafi Trusted Protection Platform

Chapter 6 Troubleshooting *Chapter 7* Further Information

1.1.3 Document Conventions

The following conventions are used in this guide:

Convention	*Use*	*Example*

Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the OK button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file example.conf in the /exmp/demo/ directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or [CSADMIN].

Table 1: Document conventions

Special icons are used to highlight the most important notes and information.

Here you find important safety information that should be followed.

Here you find additional notes or supplementary information.

1.1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	*Meaning*
AES	Advanced Encryption Standard
CD	Compact Disc

CSADM	CryptoServer Command-line Administration Tool
GUI	Graphical User Interface
HSM	Hardware Security Module
LAN	Local Area Network
MBK	Master Backup Key
MS DPAPI	Microsoft Data Protection Application Program Interface
PCIe	PCI Express Interface
Abbreviation	*Meaning*
PKCS#11	Public-Key Cryptography Standard #11
VTPP	Venafi Trust Protection Platform
URL	Uniform Resource Locator

Table 2: List of Abbreviations

2 Overview

2.1 Venafi Trust Protection Platform

The Venafi Trust Protection Platform stores sensitive information such as logon credentials and private key material within its 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 Trust Protection Platform provides a

PKCS#11 driver that can be used to integrate with third party Hardware Security Module's

(HSM's) such as the Utimaco CryptoServer HSM. This provides the ability to configure Venafi Trust Protection Platform to use keys stored on and managed by the HSM, thus truly separating the stored data from the encryption keys.

2.2 Utimaco CryptoServer HSM

CryptoServer is a hardware security module developed by Utimaco IS GmbH. CryptoServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Venafi Trust Protection Platform.

Operating System	*Venafi Trust Protection Platform*	*Utimaco Security Server Version*	*Utimaco HSM*
Windows Server 2012 R2 Windows Server 2016	18.3	SecurityServer 4.31.2	CryptoServer CSe-Series/Se-Series

Table 3: List of Software Requirements

3.2 Software Requirements

Software	*Software Requirements*
Java	Version 8, Update 271 or higher
HSM Utility	SecurityServer/ CyrptoServer Administration (csadm)
HSM Utility	SecurityServer PKCS#11 Tool (p11tool2)
HSM Interfaces	SecurityServer PKCS#11 Provider

Table 4: List of Software Requirements

3.3 Hardware Requirements

Hardware	*Hardware Requirements*
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.31.2 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.31.2 or higher

Table 5: List of Hardware Requirements

Setup an account on the Utimaco support portal and request download access at the following URL. https://support.hsm.utimaco.com/

3.4 Prerequisites

Before you begin, please ensure that you have installed/setup:

- Operating system listed in Tested Versions
- SecurityServer listed in Tested Version
- CryptoServer Default Admin should be replaced with a new admin user
- MBK must be created and stored onto each HSM. Refer the CryptoServer documentations to setup the MBK
- CryptoServer is setup and configured. Refer the CryptoServer documentations to setup the HSM
- PKCS#11 library is setup and configured as per your environment. Refer the CryptoServer documentations to setup and configure the PKCS#11 library

4 PKCS#11 Configuration

Edit the `cs_pkcs11_R2.cfg file` located at "`C:\ProgramData\Utimaco\PKCS11_R2`" and make the appropriate changes to the file.

For more information regarding the commands and command parameters please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

```
Device = 288@<HSM IP address> Hardware (LAN) HSM
```

OR

```
Device = /dev/cs2.0 Hardware (PCIe) HSM
```

Example values

cs_pkcs11_R2.cfg

```
[Global]
# Path to the logfile (name of logfile is attached by the API)

# For unix:
#Logpath = /tmp

# For windows:
Logpath = C:/ProgramData/Utimaco/PKCS11_R2

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1

[CryptoServer]
# Device specifier
Device = 192.168.10.10
```

To make your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging** *Loglevel. Set the* **LogPath** *and Logging* **Loglevel** *to* **1**. *For testing you may want to increase it to* **4**.

The added **LogPath** *points to a writable directory, not to a file.*

If you encounter problems, check the log file named `cs_pkcs11_R2.log` *in the* LogPath *defined directory. When you are done testing, you should change Logging to* 1 *or* 2*. This will limit the logging to only critical and important messages.*

5 Configure Venafi Trusted Protection Platform

We will be configuring the VTPP to use the PKCS11 HSM mechanism. From the Venafi Configuration Console select the Connectors option.

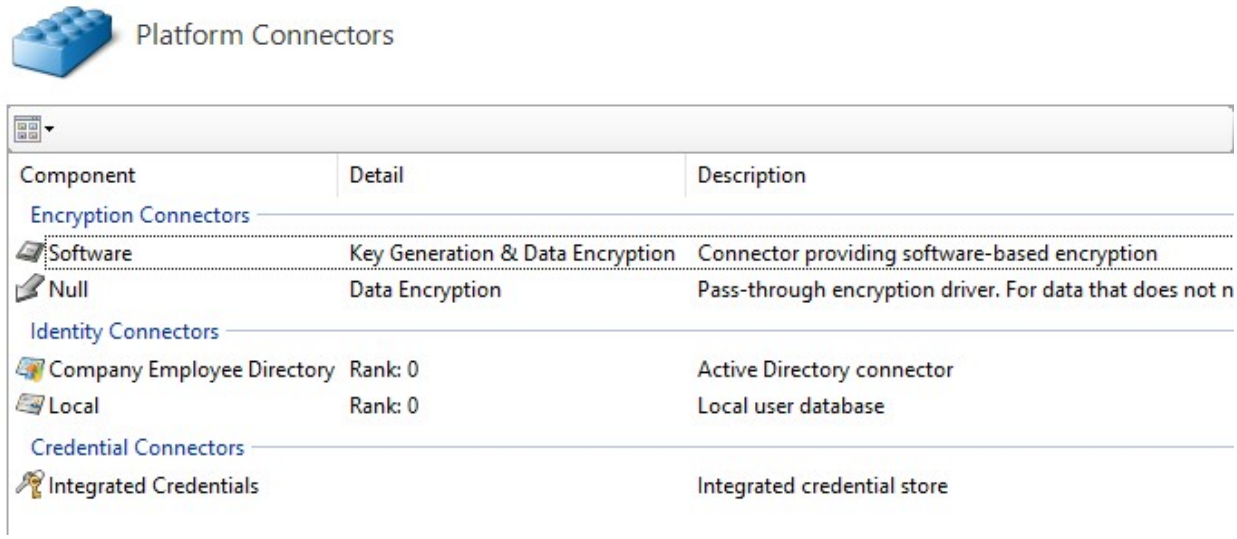

Figure 1: Platform Connectors

Locate the Platform Connectors menu. You will be Creating an HSM Connector. Select Create new HSM (Cryptoki) connector.

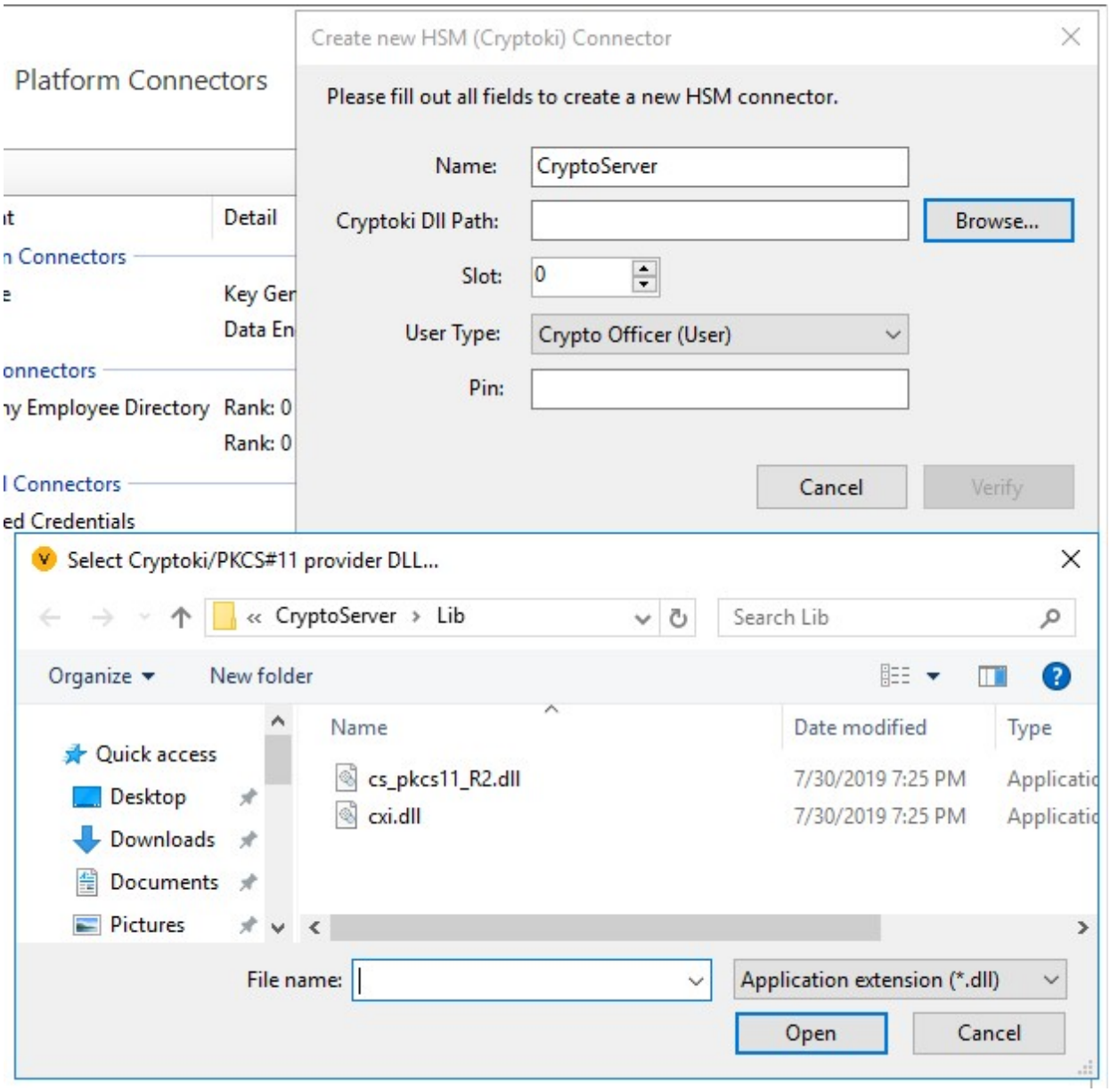

Figure 2: Create HSM Connector

Select a name for the new HSM connector. I have chosen CryptoServer. Next we will browse and find the Utimaco PKCS#11 library.

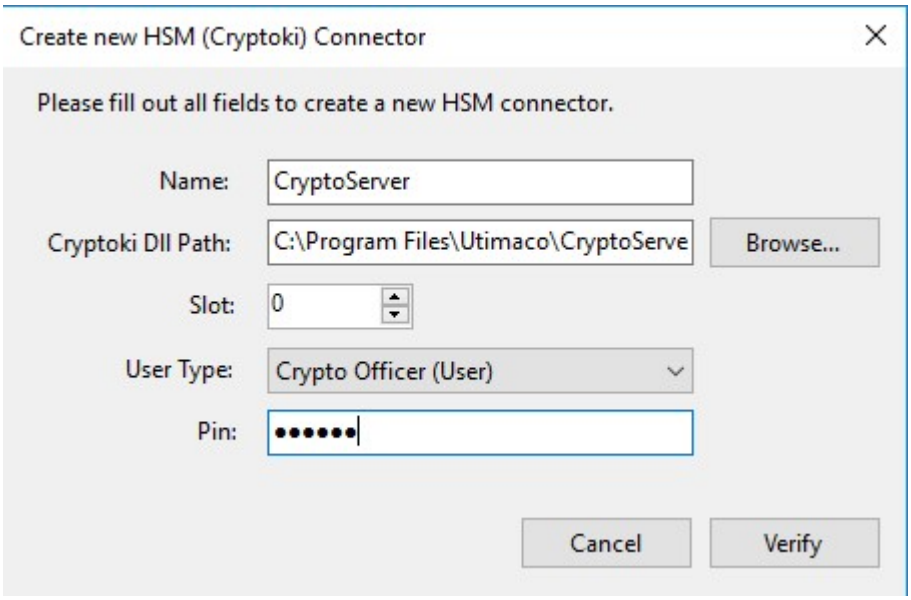

Figure 3: Set Cryptoki Path & Pin

The normal path for the library is located at `C:\ProgramFiles\Utimaco\CryptoServer\Lib\cs_pkcs11_R2.dll`.Set the PIN to be what you configured SLOT_0000 User. In our case that would be "123456" Now press Verify button. This will verify the connection to the HSM.

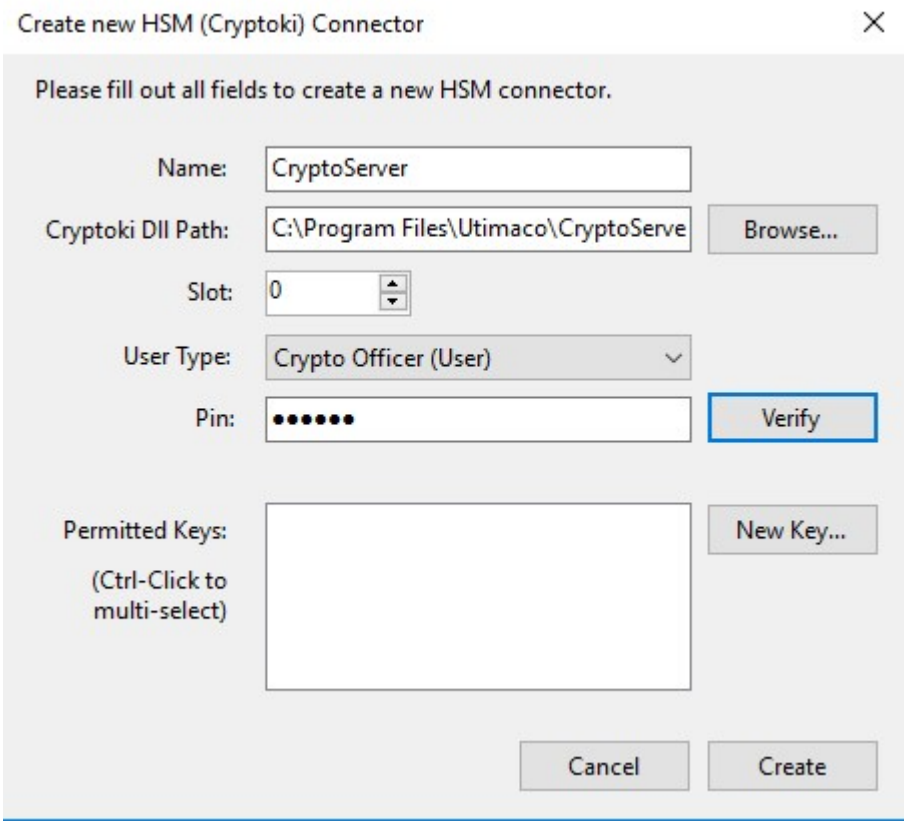

Figure 4: Verify Connection

You should see some activity and the window will reopen with an option to creat keys. If you see this window then it is time to create a New Key. Press the New Key button.

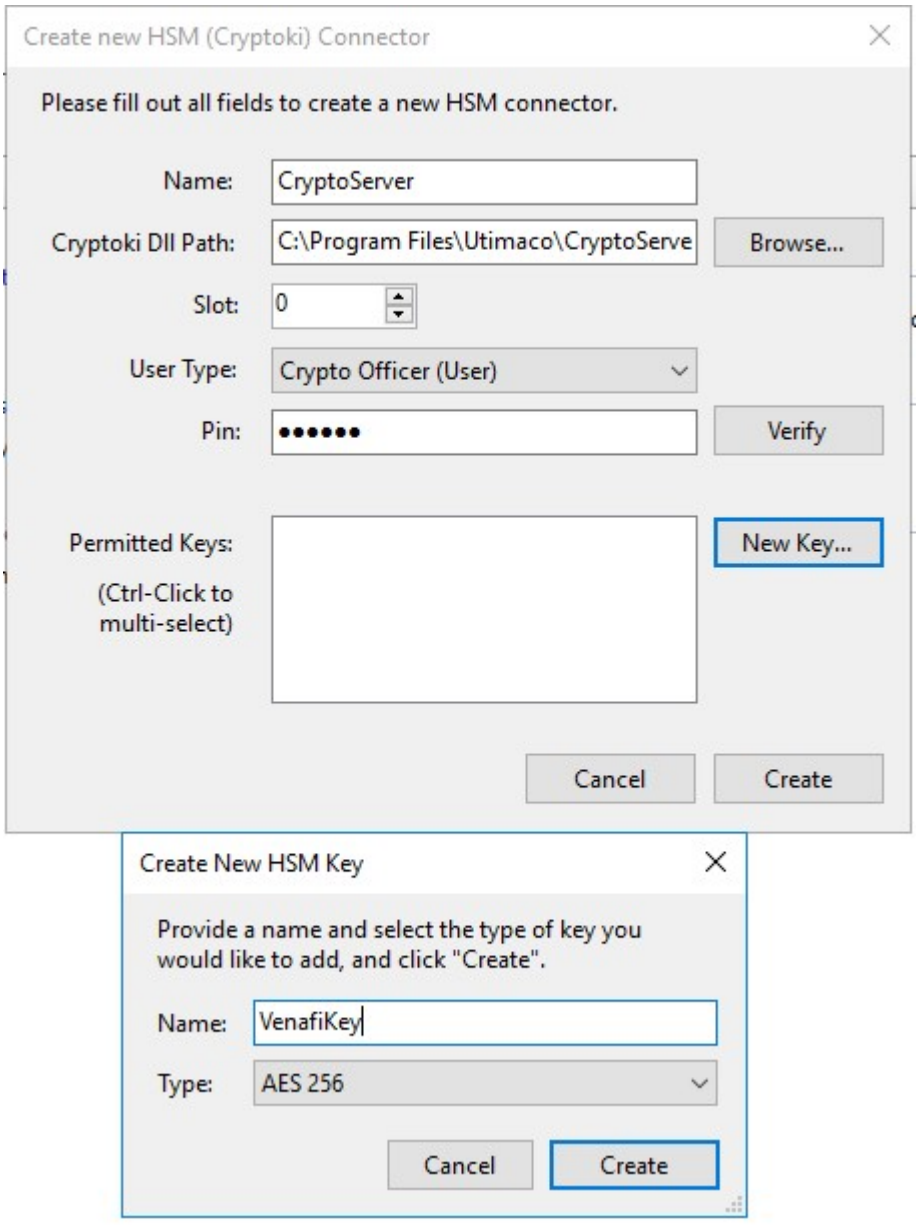

Figure 5: Create New Venafi Key

We will now tell the HSM to create a new key "VenafiKey" of the type AES 256. Press the Create button now.

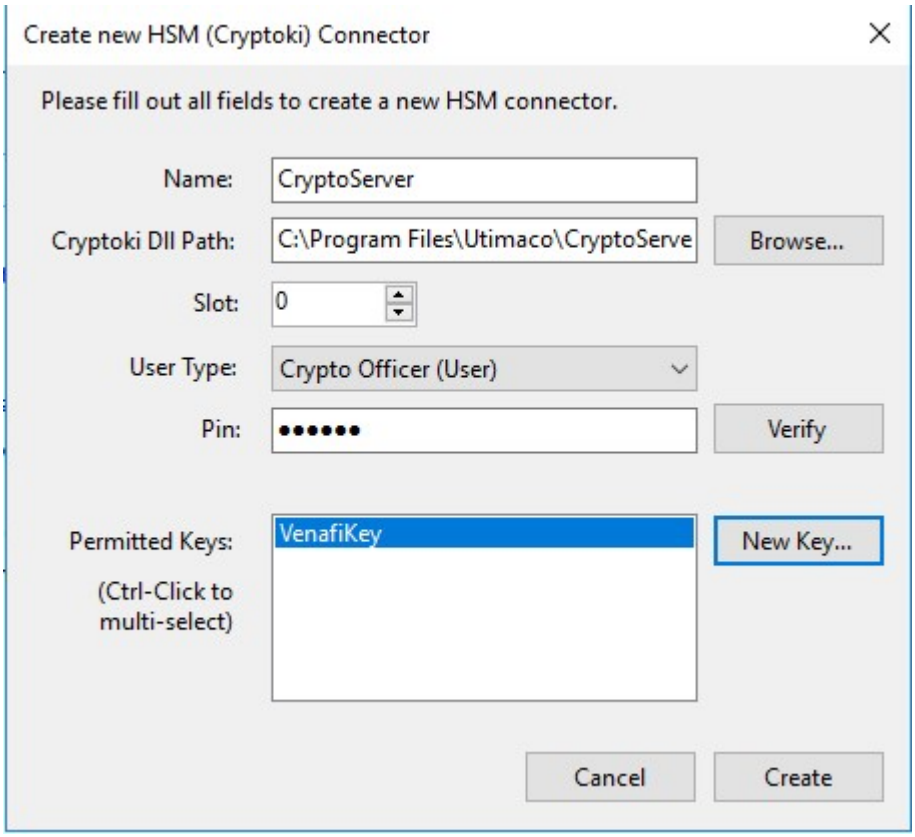

Figure 6: Key Created

You should now see a new key "VenafiKey" visible in the Permitted Keys window. We now have our first working key. Press the Create button. It should proceed to create our new HSM connector.

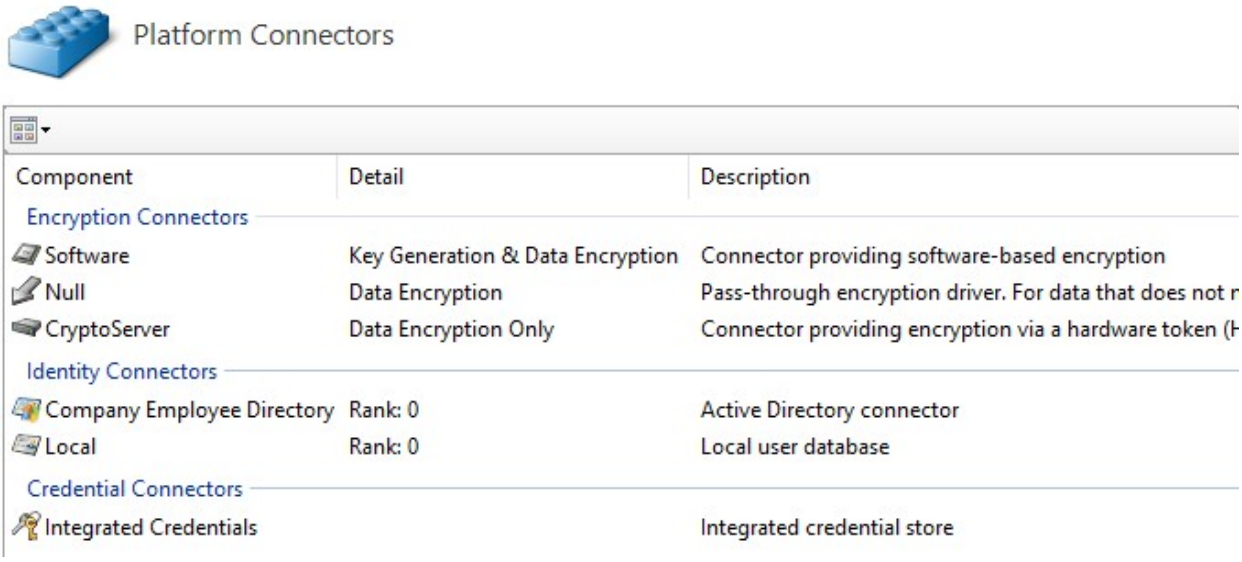

Figure 7: CryptoServer Connector Up

We can see here that we have CryptoServer Encryption Connector currently being used only for Data Encryption. You can make changes to these option by returning to the top level screen and selecting from the Actions panel on the top right of your screen.

5.1 Operational VTPP with Utimaco HSM Integration

Return to the Product Components screen and restart the Venafi Platform and the Website. Then access the web interface, login and refresh the deplay.

At this point you should now have an operational VTPP with Utimaco HSM integrated as the PKCS#11 token device. You now have an HSM backed VTPP installation. Keys will be safely held in the HSM.

6 Troubleshooting

Error	*Diagnosis*
Error: Failed to attach external HSM client library. Please check if you specified the vendor provided PKCS#11 library path correctly	1. Verify whether the correct Path to PKCS#11 library path is specified 2. Verify if the cs_pkcs11_R2.cfg file is available under C: \ProgramData\Utimaco\PKCS11_R2 folder 3. Verify if the cs_pkcs11_R2.cfg file configurations are correct
LoginUser= failed: 05.12.2021 23:45:45 src/p11adm_R2.c[429] p11_login: C_Login [type=1] returned Error 0x00000102 (CKR_USER_PIN_NOT_INITIALIZED)	PKCS#11 Slot is not initialized.
Error:Slot 0000 0000: p11cat.P11.getAuthState(Native Method): CS_GetSessionInfo returned Error 0x00000030 (CKR_DEVICE_ERROR)	1. Verify HSM services are up and running 2. Check the cs_pkcs11_R2.cfg file is having correct IP entry.

Table 6: List of Error and its Diagnosis

7 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

https://utimaco.com/

8 References

Reference	*Title/Company*	*Document No.*
[CSADMIN]	CryptoServer – csadm Manual/ Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004