F5

Big-IP

Integration Guide

SecurityServer

utimaco®

Imprint

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-2025-0026

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 website 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 F5 Big-IP. Utimaco HSM securely generates and stores the private key of SSL certificate and offload the cryptographic operations onto the HSM.

1.1.1 Target Audience for This Guide

This guide is intended for administrators of F5 Big-IP 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 Software Download and Installation

Chapter 5 PKCS#11 Configuration

Chapter 6 Setting up the HSM

Chapter 7 Configure HSM Connectivity to Big-IP

Chapter 8 Generate a Certificate & Key onto HSM

Chapter 9 Troubleshooting

Chapter 10 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.

This message marks the result expected after the successful execution of an instruction

1.1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CSADM	CryptoServer Command-line Administration Tool
CSR	Certificate Signing Request
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HSM	Hardware Security Module
MBK	Master Backup Key
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
SO	Security Officer
URL	Uniform Resource Locator

Table 2: List of Abbreviations

1.2 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.

2 Overview

2.1 F5 Big-IP

F5 BIG-IP is the application services that cover software and hardware designed around application availability, access control, and security solutions. The product specializes in application delivery networking, network security, access & authorization. The product provides encryption to the traffic which passes through networks. Using Utimaco HSM with F5 Big-IP provides the user with an additional layer of security which independently manages the keys, certificates, and many more other things. It also provides encryption and decryption functionality which is add-on to the existing system.

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 F5 Big-IP.

F5 Big-IP	Utimaco Security Server Version	Utimaco HSM
BIGIP-16.1.2-0.0.18	SecurityServer 4.45.1.0	CryptoServer CSe-Series/Se-Series u.trust Anchor Se*k and u.trust Anchor CSAR

Table 3: List of Tested Versions

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 4.50 or higher u.trust Anchor Se*k and u.trust Anchor CSAR with firmware 4.50 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.50 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

The user must first deploy the Big-IP system before following the steps in this guide. BigIP Virtual Edition was tested but the procedures can be applied to other deployments.

- Operating system listed in Tested Versions
- SecurityServer listed in Tested Versions
- 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 The licensed Big-IP system must be used for External Interface and Network HSM.

- The user with admin privileges to the Big-IP server.
- Java version 11.0.12 or higher

4 Software Download and Installation

This section describes the process of installing Utimaco HSM software with the PKCS#11 Provider.

4.1 Download Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation. Copy the downloaded software at the appropriate location on the F5 Big-IP server.

5 PKCS#11 Configuration

1. Create the directory `/etc/utimaco`. We will copy the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg` into this directory. It is located in your CryptoServer-V4.50 directory, `Linux/x86-64/Crypto_APIS/PKCS11_R3/sample`.

›_ Console

```
# mkdir /etc/utimaco

# cd <install directory>/Software/Linux/x86-64/Crypto_APIs/PKCS11_R3/sample # cp
cs_pkcs11_R3.cfg /etc/utimaco # cd /etc/utimaco
```

2. Edit the cs_pkcs11_R3.cfg file located at "/etc/utimaco/" 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_R3.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_R3

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

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

For deployments with u.trust Anchor, the port number will be in the range 4001 thru 4032 or 4001@192.168.10.10 for example.

*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_R3.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.*

5.1 Configure the PKCS#11 Library

To install the PKCS#11 provider library and tools, you will need to copy the PKCS#11 provider library provided by Utimaco and command line tools to a place where F5 Big-IP can find it.

1. Create utimaco folder under `/opt` directory and further create 2 directories `/etc/utimaco/bin` and `/etc/utimaco/lib`.
2. Copy pkcs11 library file `libcs_pkcs11_R3.so` from Utimaco CryptoServer software to the `/opt/utimaco/lib` directory and make the file executable.

›_ Console

```
# mkdir -p  /opt/utimaco/bin && mkdir /opt/utimaco/lib

# chmod  +x /opt/utimaco/lib/ libcs_pkcs11_R3.so
```

3. Copy the csadm and p11tool2 files from Utimaco CryptoServer software to `/opt/utimaco/bin` directory and make both the files executable.

›_ Console

```
# cd ~/path_to_application_folder/ && cp csadm p11tool2 /opt/utimaco/bin

# chmod  +x /opt/utimaco/bin/csadm /opt/utimaco/bin/p11tool2
```

6 Setting up the HSM

We will access the HSM using the IP address of the GP HSM device.

6.1 Initialize a Slot

F5 Big-IP uses the token label to specify the slot to be used. To avoid any problems, please make sure the token label you are using is unique.

To initialize a slot with a custom label; use the following commands on the machine where you installed the p11tool2 tool.

The first p11tool2 command creates the SO or Security Officer for slot 0 user and the second p11tool2 command initializes the slot 0 User.

6.2 Setting up your PKCS#11 Users

Following the Utimaco documentation for setting up your PKCS#11 users.

For our example we have chosen the HSM PIN as "123456", to use for our SO and Crypto User.

›_ Console

```
# /opt/utimaco/bin/p11tool2 slot=0 Label=BIGIPDemo

Login=BIGIPADMIN,BIGIPADMIN.key InitToken=123456

# /opt/utimaco/bin/p11tool2 slot=0 LoginSO=123456 InitPin=123456
```

6.3 Check the Slot

Check the PKCS#11 slot. Results should be similar to the following output.

›_ Console

```
# /opt/utimaco/bin/p11tool2 LoginUser=123456 GetSlotInfo

CK_SLOT_INFO (slot ID: 0x00000000):

slotDescription 3130332e 362e3333 2e313231 202d2053 |103.6.33.121 - S|

4c4f545f 30303030 20202020 20202020 |LOT_0000 |

20202020 20202020 20202020 20202020 | |

20202020 20202020 20202020 20202020 | |

manufacturerID 5574696d 61636f20 49532047 6d624820 |Utimaco IS GmbH |

20202020 20202020 20202020 20202020 | |

flags: 0x00000005

CKF_TOKEN_PRESENT : CK_TRUE

CKF_REMOVABLE_DEVICE : CK_FALSE

CKF_HW_SLOT : CK_TRUE

hardwareVersion : 5.01

firmwareVersion : 2.04
```

6.4 List Users and Verify MBK

1. Use the csadm command, list and confirm the users created.

›_ Console

```
# /opt/utimaco/bin/csadm DEV=192.168.10.10 listusers
Name Permission Mechanism Attributes
BIGIPADMIN 22000000 RSA sign Z[0]
SO_0000 00000200 HMAC passwd A[CXI_GROUP=SLOT_0000]
USR_0000 00000002 HMAC passwd Z[0]A[CXI_GROUP=SLOT_0000]
```

2. Now check to confirm the Utimaco HSM has an MBK.

›_ Console

```
# /opt/utimaco/bin/csadm DEV=192.168.10.10 LogonSign=BIGIPADMIN,BIGIPADMIN.key
MBKListKeys
slot name len algo type k generation date key check value

-----------------------------------------------------------------

3 MYMBK 32 AES XOR 2 2012/08/15 13:08:39
CC06067E3C8692DE:D53279C7B862EC54
```

7 Configure HSM Connectivity to BIG-IP

7.1 Configure Utimaco PKCS#11 Provider with Big-IP

1. To start with, login to the Configuration utility of F5 Big-IP from the browser
2. On the Left Pane go to `System > Certificate Management > HSM Management > External HSM`
3. Now in the General Properties, click on the dropdown and select the Vendor as auto and set the PKCS11 Library Path to `/opt/utimaco/lib/libcs_pkcs11_R3.so`
4. In the Partitions, create a new Partition with the Name as auto & Password as 123456
5. Click on Add to save credentials button and then click on Finished button at the bottom

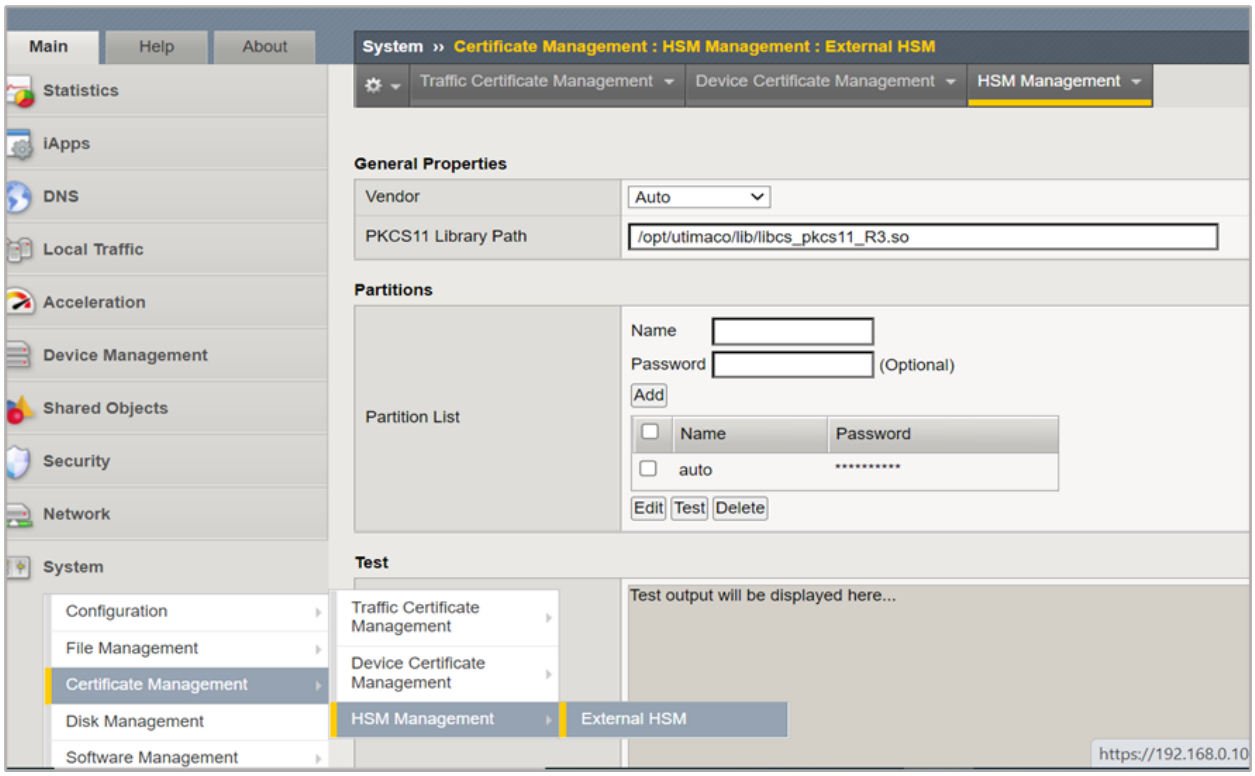

Figure 1: External HSM Management

8 Generate a Certificate & Key onto HSM

Certificate used by F5 Big-IP can be self-signed or signed by third party Certificate Authority. Below are the two methods for generating a certificate and key.

8.1 Generate a Self-Signed Certificate

There are two ways for creating a self-signed certificate and key.

- By Traffic Management Shell tmsh
- By using the Configuration Utility (GUI)

8.1.1 Generate a Key & Certificate using tmsh

1. Generate a key & certificate

›_ Console

```
# tmsh create sys crypto key <key_name> gen-certificate common-name
<cert_name> security-type nethsm
For Example
# tmsh create sys crypto key f5-testkey gen-certificate common-name
utimaco.bigip.com security-type nethsm
```

2. Verify that the key was created

›_ Console

```
# tmsh list sys crypto key f5-testkey
sys crypto key default.key {
key-size 2048
key-type rsa-private
security-type normal
}
sys crypto key f5_api_com.key {
key-size 4096
key-type rsa-private
security-type password
}
sys crypto key f5-testkey {
key-id s7cb7a32bd11d323gad1dc23fhd9a1a8
key-size 2048
key-type rsa-private
nethsm-partition auto
security-type nethsm
}
```

3. Save the configuration

›_ Console

```
# tmsh save sys config
```

8.1.2 Generate a Key & Certificate using GUI

1. Log in to the Configuration utility
2. In the Main tab, select `System > Certificate Management > Traffic Certificate Management`. The user will see the Traffic Certificate Management screen 3. Click on the **Create** button

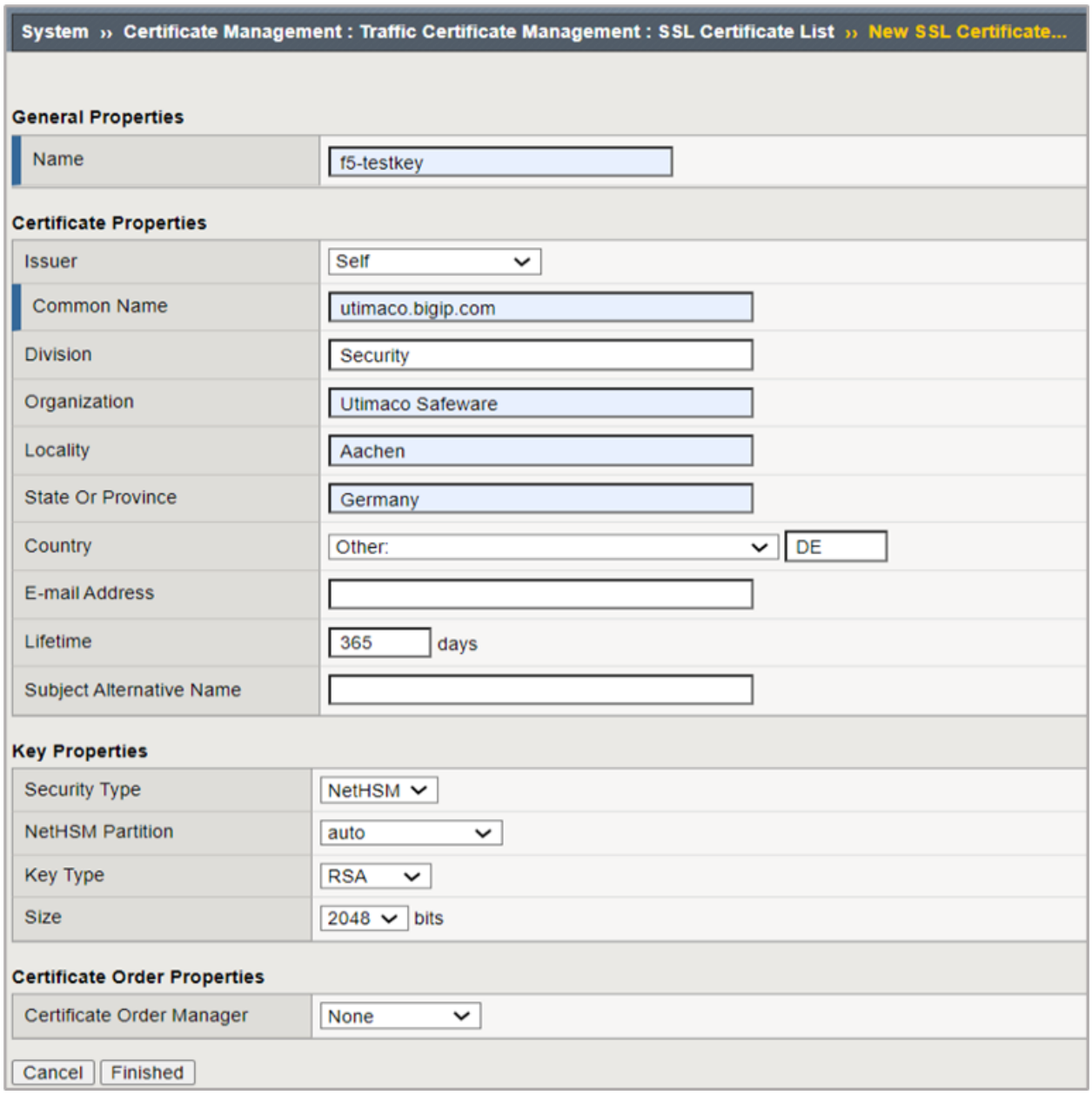

Figure 2: Generate Self-Signed Certificate

3. Enter a name for the SSL certificate
4. Select Self from the Issuer drop-down
5. Enter the other details from Certificate Properties section as required
6. In Key Properties, select NetHSM from the Security Type drop-down
7. Select auto from the NetHSM partition drop-down

8. Select the Algorithm from Key Type drop-down
9. Select a key size from the Size drop-down
10. Click on the Finished button

8.2 Request a Certificate from a Certificate Authority

Generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA). 1. Log in to the Configuration utility

2. In the Main tab, select `System > Certificate Management > Traffic Certificate Management`. The user will see the Traffic Certificate Management screen

3. Click on the Create button. The New SSL Certificate window appears

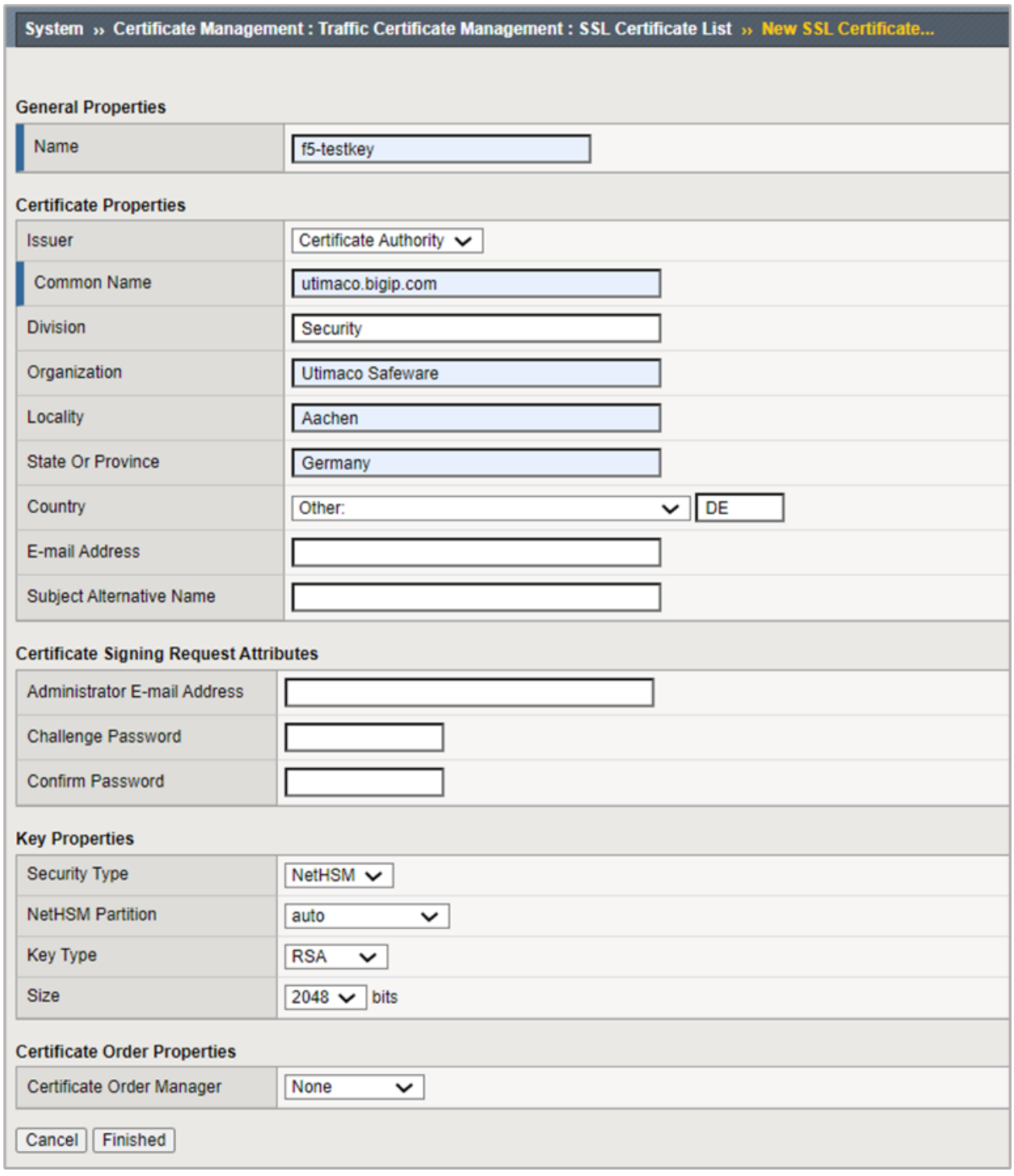

Figure 3: Request a certificate from a Certificate Authority Window

4. Enter a name for the SSL certificate, and select Certificate Authority from the Issuer List
5. Enter the other details from Certificate Properties section as required

6. Enter the Certificate Signing Request Attributes as required
7. In Key Properties, select NetHSM from the Security Type drop-down
8. Select auto from the NetHSM partition drop-down
9. Select the Algorithm from Key Type drop-down
10. Select a key size from the Size drop-down
11. Click on the Finished button
12. The Certificate Signing Request screen displays
13. Perform any one of the following to download the request into a file on your system
    a. Copy the certificate, in the Request text field
    b. Select the download button, for Request File
14. Submit the request to the certificate authority to be signed
15. Click on the Finished button
16. The user will see an option displayed to import the signed certificate

8.3 Verify a Key generated on HSM

Use p11tool to verify if the Keys are generated on HSM.

›_ Console

```
# /opt/utimaco/bin/p11tool2 LoginUser=123456 ListKeys
CKO_PRIVATE_KEY:

+ 1.1
CKA_KEY_TYPE = CKK_RSA
CKA_SENSITIVE = CK_TRUE
CKA_EXTRACTABLE = CK_FALSE
CKA_LABEL = f5-testkey___fcd9a1a2
CKA_ID =
0x63376362 37613132 62643131 64333233 |c7cb7a12bd11d323|
64616431 64633233 66636439 61316132 |dad1dc23fcd9a1a2|
```

When keys created on the HSM through F5 Big-IP, the last eight digits of the CKA_ID of the keys gets appended to the CKA_LABEL as described above.

The ASCII CKA_ID value shown in the above console window matches with the **key-id** in the below console window.

›_ Console

```
# tmsh list sys crypto key f5-testkey___fcd9a1a2
sys crypto key default.key {
key-size 2048
key-type rsa-private
security-type normal
}

sys crypto key f5_api_com.key {
key-size 4096
key-type rsa-private
security-type password
}

sys crypto key f5-testkey {
key-id c7cb7a12bd11d323dad1dc23fcd9a1a2
key-size 2048
key-type rsa-private
nethsm-partition auto
security-type nethsm
}
```

8.4 Deleting a Key from the BIG-IP

1. In the Main tab, select System > Certificate Management > Traffic Certificate Management. The Traffic Certificate Management screen opens
2. The Traffic Certificate Management screen opens
3. From the SSL Certificate List, select the key to delete
4. Click on the Delete button
5. The key you selected is only deleted from BIG-IP
6. If the user wants to delete the keys from HSM

›_ Console

```
# /opt/utimaco/bin/p11tool2 LoginUser=123456 Label="<Key Name>" DeleteObject
```

8.5 Importing a pre-existing Key to the BIG-IP

There are two ways for importing keys

- By using the Configuration Utility (GUI)
- By Traffic Management Shell tmsh

8.5.1 Import a Key using Configuration Utility (GUI)

1. Generate a key using PKCS#11 tool

›_ Console

```
# p11tool2 [Slot=<slot_id>] LoginUser=<user_pin>
[PubKeyAttr=<pub_key_attr>] [PrvKeyAttr=<prv_key_attr>]
GenerateKeyPair=<mech>

For Example
# /opt/utimaco/bin/p11tool2 LoginUser=123456 PubKeyAttr=CKA_LABEL="f5-
testkey",CKA_ID=0x38356438333562383238656532666239323031393163326530393437363431
64
PrvKeyAttr=CKA_LABEL="f5-
testkey",CKA_ID=0x38356438333562383238656532666239323031393163326530393437363431
64
GenerateKeyPair=RSA
```

2. In the Main tab, select System > Certificate Management >Traffic Certificate Management > SSL Certificate list > Import. The SSL Certificate/Key Source page opens
3. Select Key, from the Import type drop-down

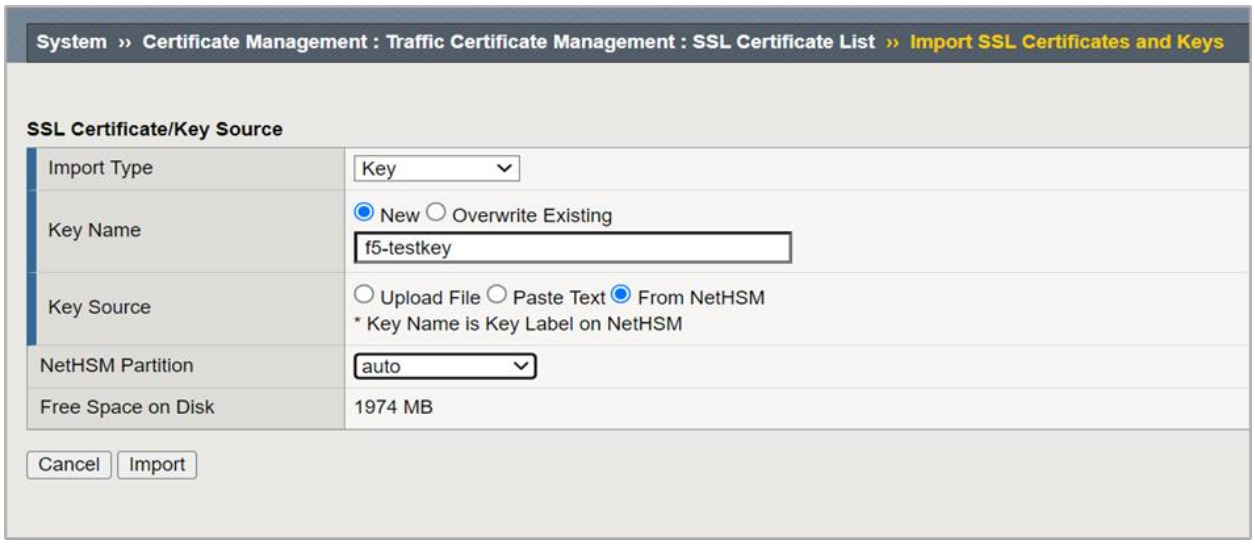

Figure 4: Import SSL Certificates and Keys Window

4. Enter the Key Name in Key Name text box (Use the same key label as generated using p11tool2)
5. Select New radio button from Key Name.
6. Select From NetHSM, within Key Source
7. Select auto from the NetHSM partition drop-down
8. Click on the Import button, to import the key

8.5.2 Import a Key using tmsh

1. Generate a key using PKCS#11 tool

›_ Console

```
# p11tool2 [Slot=<slot_id>] LoginUser=<user_pin>

[PubKeyAttr=<pub_key_attr>] [PrvKeyAttr=<prv_key_attr>]

GenerateKeyPair=<mech>

For Example

# /opt/utimaco/bin/p11tool2 LoginUser=123456 PubKeyAttr=CKA_LABEL="f5-

testkey",CKA_ID=0x38356438333562383238656532666239323031393163326530393437363 4

3164 PrvKeyAttr=CKA_LABEL="f5-

testkey",CKA_ID=0x38356438333562383238656532666239323031393163326530393437363 4

3164 GenerateKeyPair=RSA
```

2. Alternatively, if the user wants to add/import the existing key via console

›_ Console

```
# tmsh install sys crypto key <nethsm_key_label> from-nethsm security-type
nethsm
```

3. Save the configuration

›_ Console

```
# tmsh save sys config
```

9 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_R3.cfg file is available under /etc/utimaco folder 1. Verify if the cs_pkcs11_R3.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. Refer Initialize a Slot
Key management library returned bad status: -36, Nethsm is not installed	Verify if pkcs11d is service is up and running # bigstart status/restart pkcs11d

Key management library returned bad status: -18, A vendor error has occurred.	1. Check if PKCS#11 user is created. Refer Initialize a Slot 2. Check if HSM is up and running 3. Restart the pkcs11d is service # bigstart restart pkcs11d
Data Input Error: The requested key(f5key1) already exists in this scope	They key name already exist. Try with a unique key name
From Configuration Utility, if user is trying to Import a pre-existing NetHSM Key and got below error Import Failed: Key management library returned bad status: 0, Unable to read POST response data	1) Check with the key attributes are correct 2) Make sure the Name and the Label of the Key matches while importing 3) Verify if the key exists which you are trying to import in Big-IP
While testing the PKCS#11 configuration when user runs **pkcs11d_test_suite** command. The below error might occur, [Sanity]: Begin Utimaco::HSM::Exception thrown in finalize [Sanity]: Failed	1. Check if Security Server Application is Up Running and connected to HSM. 2. Check if the Configuration File pointing towards IP Address of HSM.

Table 6: List of Error and its Diagnosis

10 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/

11 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