F5

BIG-IP

17.5.1

Integration Guide

u.trust GP HSM Se-Series

6.1.1

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH Krefelder Straße 220 52070 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	2.0.0
Date	2025-12-09
Status	PUBLISHED
Document No.	IG-2025-0026

Table of Contents

1 Introduction

1.1 About This Guide

This guide provides an integration guide explaining how to integrate Utimaco CryptoServer Hardware Security Module (HSM) with F5 BIG-IP. Utimaco HSM securely generates and stores the private key of SSL certificates and offloads the cryptographic operations onto the HSM.

1.2 Target Audience

This guide is intended for administrators of F5 BIG-IP and of Utimaco HSMs.

1.3 Purpose of the Integration

The integration of F5 BIG-IP with Utimaco SecurityServer (HSM) serves a critical role in enhancing the security, compliance, and performance of cryptographic operations within enterprise environments.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
CSADM	CryptoServer Command-line Administration Tool
CSR	Certificate Signing Request
GUI	Graphical User Interface
PKCS#11	PKCS Part 11: The Cryptographic Token Interface Standard
SO	Security Officer

Abbreviation	Meaning
MBK	Master backup key
P11CAT	The PKCS#11 graphical interface tool
TMSH	Traffic Management Shell
SSL/TLS	Secure Socket Layer / Transport Layer Security
CXI	Cryptographic eXtended Interface
FIPS	Federal Information Processing Standards

Table 1: Abbreviations

1.5 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	Click **Add** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`./p11tool2 LoginUser=12345678 GetSlotInfo`
Italic	References and important terms	Visit the official *Utimaco Portal*.

Table 2: Document Conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

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

2 Product Overview

2.1 Overview of F5 BIG-IP

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

2.2 Overview of 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.

2.3 Joint Value Proposition

The integration of Utimaco SecurityServer with F5 BIG-IP delivers a secure, compliant, and high-performance solution for managing cryptographic operations in enterprise environments. This integration is designed to meet the needs of organizations requiring strong data protection, regulatory compliance, and operational efficiency in their application delivery infrastructure.

- Ensures that private keys used for SSL/TLS and other cryptographic operations are generated, stored, and used exclusively within the certified boundary of the Utimaco HSM.
- Protects against key compromise, insider threats, and unauthorized access by leveraging hardware-based security.
- Enables auditability and centralized control over key usage and lifecycle management.
- Offloads cryptographic processing from F5 BIG-IP to the HSM, reducing CPU load and improving SSL/TLS throughput.
- Supports high-volume environments with minimal impact on application performance.
- Utilizes standard interfaces such as PKCS#11, ensuring compatibility and ease of integration.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements. This guide assumes that the user has already installed and configured F5 BIG-IP.

3.1 Tested Versions

The following integrations have been successfully tested between the Utimaco HSM and F5 BiG-IP.

F5 BIG-IP	Utimaco Security Server Version	Utimaco HSM
BIG-IP 17.5.1	SecurityServer 6.1.1	u.trust GP HSM Se-Series

Table 3: List of Tested Versions

3.2 Hardware and Software Requirements

3.2.1 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.1.1 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.1.1 or higher

Table 4: List of Hardware Requirements

3.2.2 Software Requirements

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

Table 5: List of Software Requirements

3.3 Prerequisites

Before you begin, please ensure that you have:

- Installed the SecurityServer version listed in *Tested Versions*.
- Replaced the CryptoServer Default Admin with a new admin user.
- Created the MBK and stored it on each HSM. Refer to the CryptoServer documentation to set up the MBK.
- Set up and configured the CryptoServer. Refer to the CryptoServer documentation to set up the HSM.
- Set up the PKCS#11 library and configured it according to your environment. Refer to the CryptoServer documentation to set up and configure the PKCS#11 library.
- The BIG-IP license External Interface and Network HSM in an active module.
- Set up the user with admin privileges on the BIG-IP server.

4 Installation and Configuration

4.1 Setting Up u.trust GP HSM Se-Series

1. Copy the downloaded software to the appropriate location on the BIG-IP machine.
2. Create a directory **/etc/utimaco**. Copy the Utimaco PKCS#11 configuration file cs_pkcs11_R3.cfg into this directory. It is located in **Linux/Crypto_APIS/PKCS11_R3/sample**.
3. Edit the cs_pkcs11_R3.cfg file located at "**/etc/utimaco/**" and update the Device value to the HSM IP.

```
[Global]
# 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

# Prevents expiring session after inactivity of 15 minutes

KeepAlive = true

# Set the Device to connect with
#[CryptoServer]
# Device specifier

Device = <HSM_IP>
```

4. Create **utimaco** folder under **/opt** directory and further create two directories: **/etc/utimaco/bin** and **/etc/utimaco/lib**.
5. Copy pkcs11 library file libcs_pkcs11_R3.so from **Linux\Crypto_APIs\PKCS11_R3\lib** directory to the **/opt/utimaco/lib** directory and make the file executable.

```
[admin@bibip1:Active:Standalone] lib # pwd
/opt/utimaco/lib
[admin@bibip1:Active:Standalone] lib # ls
libcs_pkcs11_R3.so
```

Figure 1 : libcs_pkcs11_R3.so file and path

6. Copy the csadm and p11tool2 files from **Linux\Administration** directory to **/opt/utimaco/bin** directory and make both the files executable.

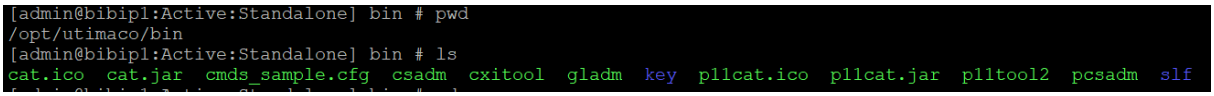

Figure 2 : csadm and p11tool2 files

For detailed guidance on commands and their parameters, please refer to the Utimaco CryptoServer documentation.

The device could be a CryptoServer HSM, available in either PCIe or LAN form factors. Depending on the type, the device configuration line will follow one of these formats:

- LAN-based HSM:
  `Device = 288@ipaddress`
- PCIe-based HSM:
  `Device = /dev/cs2.0`

Make sure to select the appropriate format based on your specific hardware setup.

To simplify your testing process, it's recommended that you enable the PKCS#11 log file by adjusting the logging settings. Specifically:

- Set the `LogPath` to a writable directory (not a specific file).
- Set the `Logging Loglevel` to 1 for basic logging. Increase it to 4 for more detailed output during testing.

This will generate a log file named `cs_pkcs11_R3.log` within the specified `LogPath` directory. Reviewing this log can help with troubleshooting if you encounter issues.

Once testing is complete, it's advisable to reduce `Logging Loglevel` to `1` or `2` to limit output to only critical or important messages.

4.2 Setting Up BIG-IP

F5 BIG-IP must be installed on the target machine to carry on with the integration process. For a detailed installation procedure of BIG-IP, refer to the F5 documentation according to the desired version of BIG-IP (refer to BIG-IP 17.5.1-Install Steps for installation steps).

If the license is not configured during installation and setup, please follow these steps:

1. Open and log in to the BIG-IP Configuration utility (GUI).
2. Navigate to **System->License**.
3. Enter the license key in **Base Registration Key** and select **Manual** (if there are no network connections for the BIG-IP).
4. Click the **Next** button.

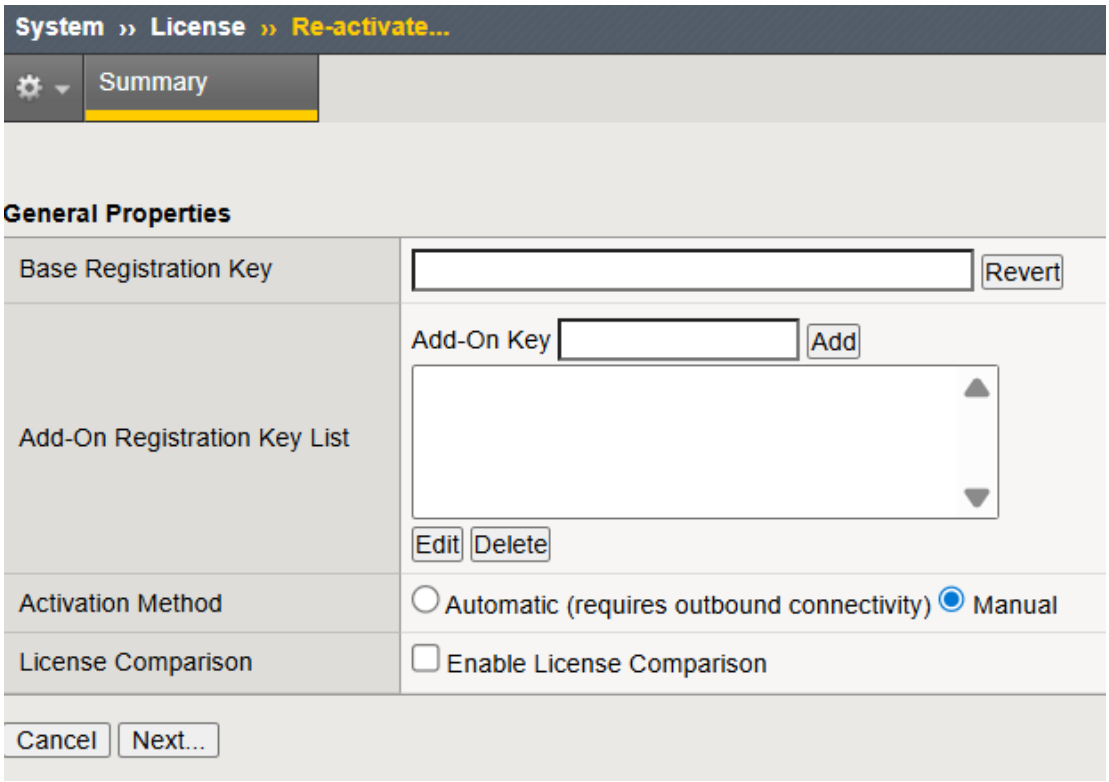

Figure 3 : License screen

5. Copy the dossier details to F5 Licensing Server and create a License. Paste the License details and click **Next** . Check the instructions given on the screen.

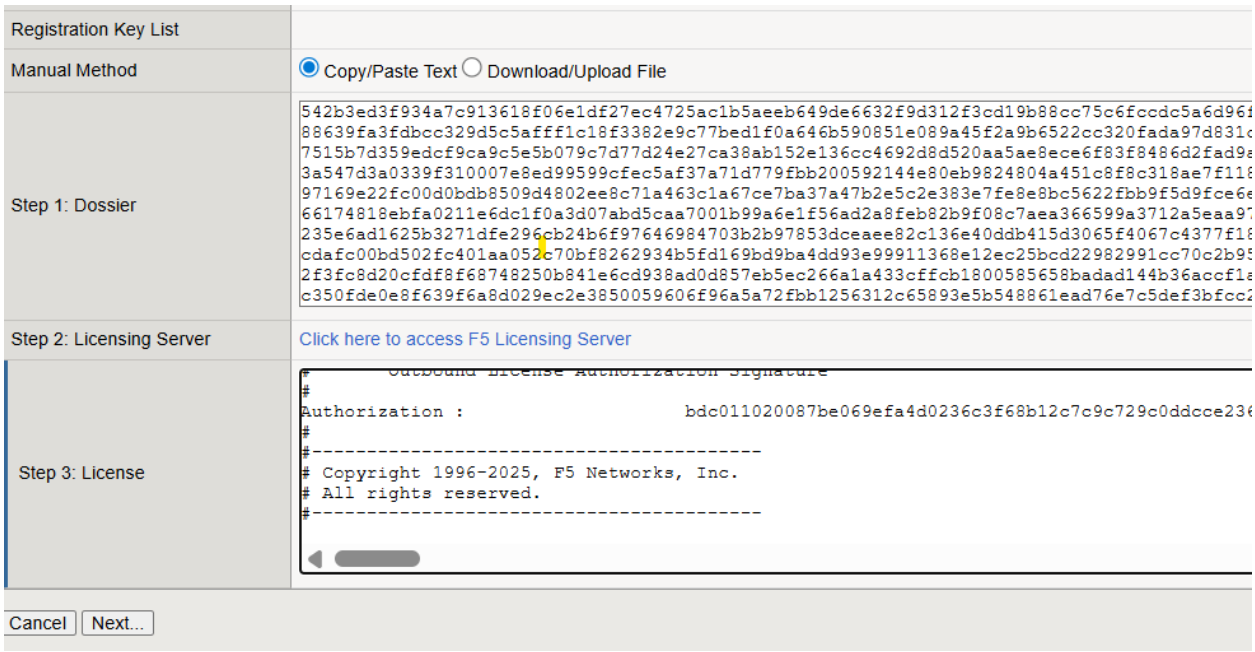

Figure 4 : License generated

6. Check that the license has External Interface and Network HSM under Active Modules.

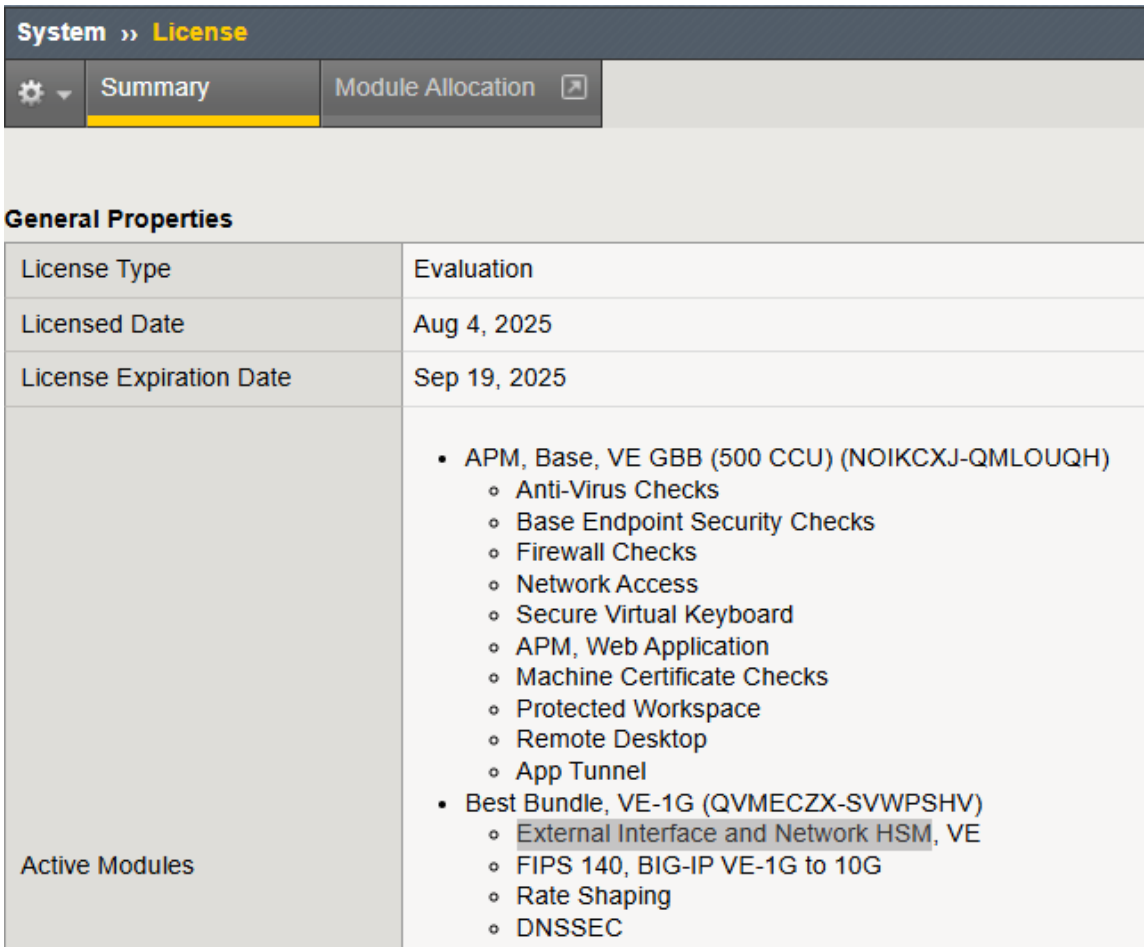

Figure 5 : Network HSM available in Active Module

5 Integration Steps

5.1 Configuration on u.trust GP HSM Se-Series

5.1.1 Initialize a Slot

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

1. Create a security officer (SO) and initialize a new token.

```
#./p11tool2 slot=0 Label=BIGIPDEMO Login=ADMIN,./key/ADMIN.key Force=1
 InitToken=87654321
```

2. Change the pin of the security officer (SO).

```
#./csadm dev=<port>@<HSM IP> Logonpass=SO_0000,87654321
 changeuser=SO_0000,12345678
```

3. Initialize a crypto user with a pin.

```
#./p11tool2 slot=0 LoginSO=12345678 InitPin=87654321
```

4. Change the pin of the crypto user.

```
#./csadm dev=<port>@<HSM IP> logonpass=USR_0000,87654321
 changeuser=USR_0000,12345678
```

5. Check the user list.

```
#./csadm dev=<port>@<HSM IP> LogonSign=ADMIN,./key/ADMIN.key ListUsers
Name      Permission   Mechanism      Attributes
ADMIN      22000000    RSA sign       Z[0]I[0]
SO_0000    00000200    HMAC passwd
Z[0]I[0]A[CXI_GROUP=SLOT_0000]L[BIGIPDEMO                        ]
USR_0000   00000002    HMAC passwd    Z[0]I[0]A[CXI_GROUP=SLOT_0000]
```

6. Check the slot info.

```
#./p11tool2 LoginUser=12345678 GetSlotInfo
CK_SLOT_INFO (slot ID: 0x00000000):

  slotDescription          33303031 40313237  2e302e30 2e31202d |3001@127.0.0.1 -|
                           20434c55 53544552  5f303030 30202d20 | CLUSTER_0000 - |
                           534c4f54 5f303030  30202020 20202020 |SLOT_0000       |
                           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        : 5.02
  firmwareVersion        : 6.01
```

7. Check the token details.

```
#./p11tool2 LoginUser=12345678 GetTokenInfo
CK_TOKEN_INFO (slot ID: 0x00000000):
  label                  42494749 5044454d  4f202020 20202020 |BIGIPDEMO       |
                         20202020 20202020  20202020 20202020 |                |

  manufacturerID         5574696d 61636f20  49532047 6d624820 |Utimaco IS GmbH |
                         20202020 20202020  20202020 20202020 |                |

  model                  43727970 746f5365  72766572 20202020 |CryptoServer    |

  serialNumber           53493030 33303031  5f303030 30202020 |SI003001_0000   |
```

F5 BIG-IP uses the token label to identify and specify the slot to be used during cryptographic operations with the HSM. It is strongly recommended that you assign a unique token label to ensure smooth integration and avoid conflicts.

5.1.2 Creating and Storing the Master Backup Key (MBK) on an HSM

The Master Backup Key (MBK) serves as a critical safeguard for encrypted data, ensuring recovery in case of key loss or corruption. This section outlines the steps to securely generate and store the MBK within the Hardware Security Module (HSM).

1. Generate an MBK.

```
#./csadm dev=<port>@<HSM IP> LogonSign=ADMIN,./key/ADMIN.key
Key=mbk1.key#12345678,mbk2.key#12345678 MBKGenerateKey=AES,32,2,2,BIGIPMBK
```

2. Import the key shares of an MBK from the key files to slot #3.

```
#./csadm dev=<port>@<HSM IP> LogonSign=ADMIN,./key/ADMIN.key
Key=mbk1.key#12345678,mbk2.key#12345678 MBKImportKey=3
```

3. List all MBKs currently stored on the device.

```
# ./csadm dev=<port>@<HSM IP> LogonSign=ADMIN,./key/ADMIN.key MBKListKeys
slot name     len algo type   k  generation date      key check value
-------------------------------------------------------------------------------
-----
3    BIGIPMBK 32  AES  XOR    2  2025/08/17
08:35:28  091789ef535e4a6d:0a2fe9cee8fef467
7    AUTO-GEN 32  AES  SHARE  1  2025/03/18
15:49:25  1c08733306225874:e40861094c0ff123
```

5.2 Configuration on BIG-IP

1. To start, log in 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. 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 and **Password** as 12345678.

5. Click on **Add** to save credentials button and then click on the **Finished** button at the bottom.

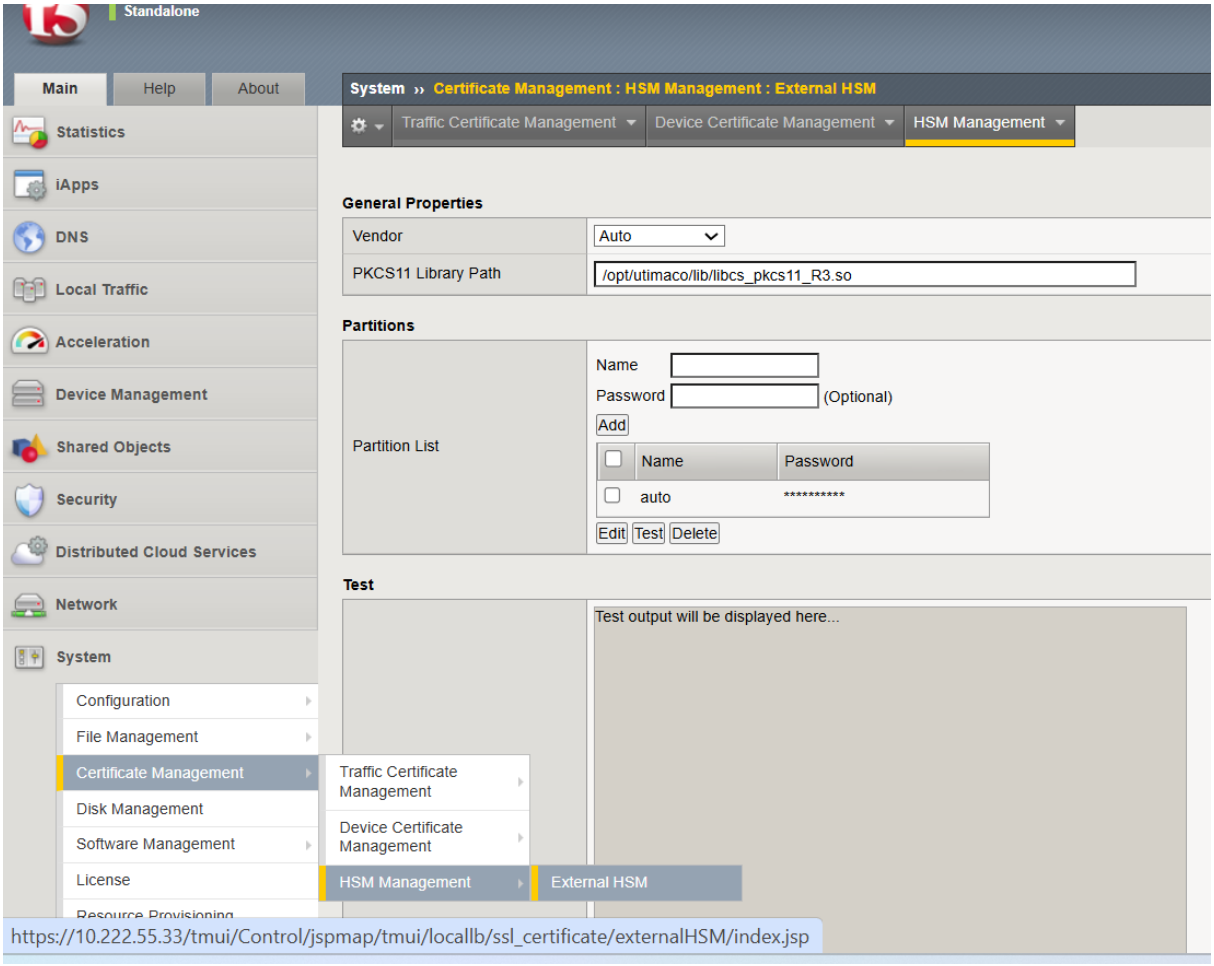

Figure 6 : External HSM Management

5.2.1 Generate a Certificate & Key Into HSM

There are two ways to create a self-signed certificate and key:

1. By using the BIG-IP Configuration Utility (GUI).
2. By Traffic Management Shell (tmsh).

5.2.1.1 Generate a Key & Certificate Using GUI

1. Log in to the BIG-IP Configuration utility.

2. In the Main tab, select System > Certificate Management > Traffic Certificate Management. The Traffic Certificate Management screen will be displayed.
3. Click on the **Create** button.
4. Enter a name for the SSL certificate in the **Name** field.
5. Select Self from the **Issuer** drop-down.
6. Enter the other details from the Certificate Properties section 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 the **Key Type** drop-down.
10. Select a key size from the **Size** drop-down.
11. Click on the **Finished** button.

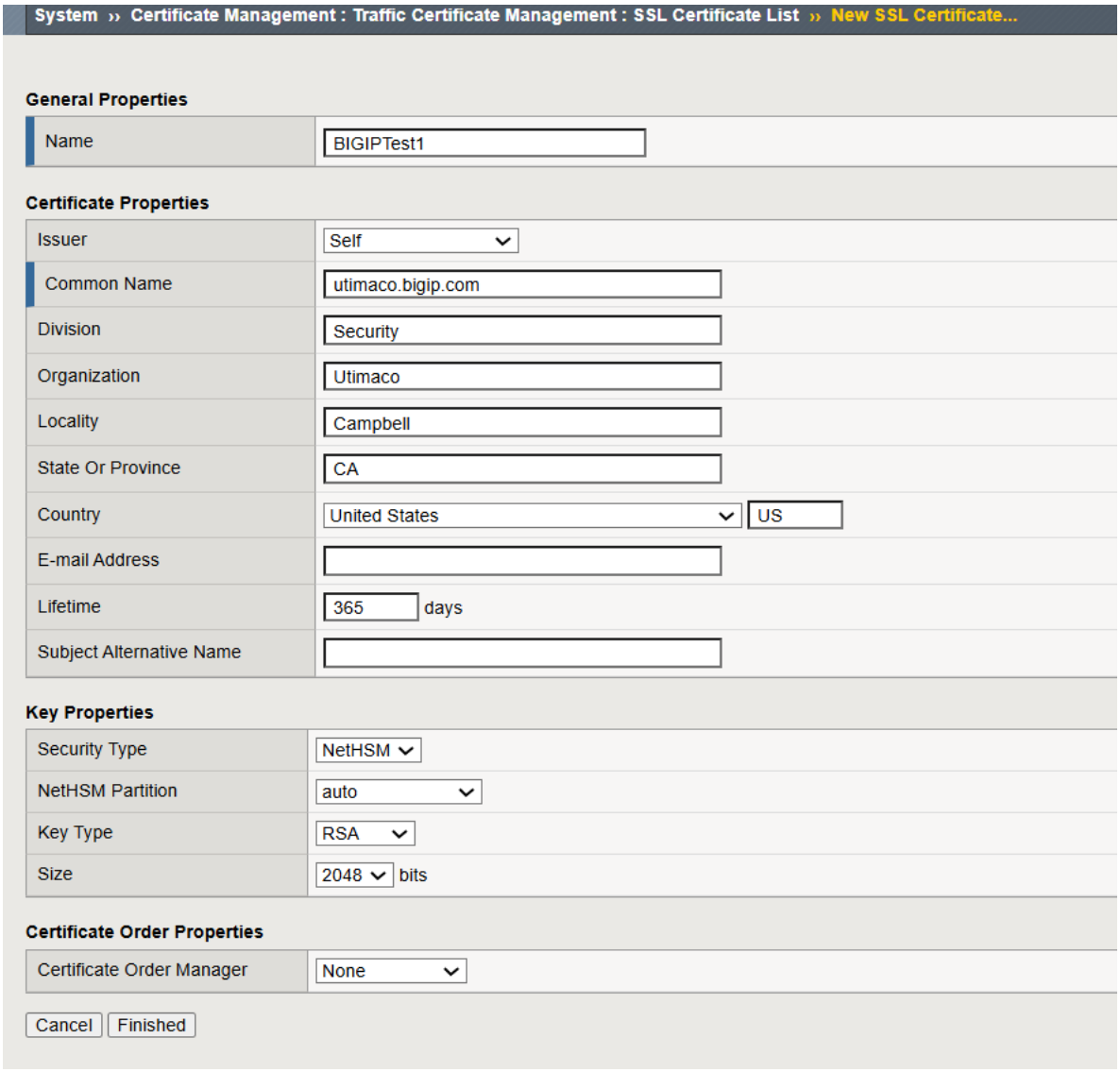

Figure 7 : Generate a Self-Signed Certificate

12. Click on the generated certificate name. A screen will open with the **Certificate** and **Key** tabs. Click on the **Key** tab to see the generated key details.

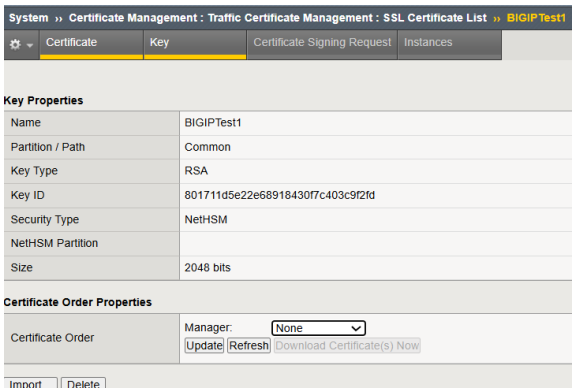

Figure 8 : Key Details

5.2.1.2 Generate a Key & Certificate Using TMSH

1. Generate a key and certificate.

```
(tmos)# create sys crypto key f5-testkey gen-certificate common-name
utimaco.bigip.com nethsm-partition-name auto security-type nethsm
```

2. Verify that the key was created.

```
(tmos)# list sys crypto key f5-testkey
sys crypto key f5-testkey {
    key-id 9745a1d81e2b84a36eee720aa05505a8
    key-size 2048
    key-type rsa-private
    nethsm-partition auto
    security-type nethsm
}
```

3. Save the configuration.

```
(tmos)# save sys config

Saving running configuration...
  /config/bigip.conf
  /config/bigip_base.conf
  /config/bigip_user.conf
Saving Ethernet map ...done
Saving PCI map ...
```

```
 - verifying checksum .../var/run/f5pcimap: OK
done
 - saving ...done
```

4. Verify the key available in the configuration GUI.

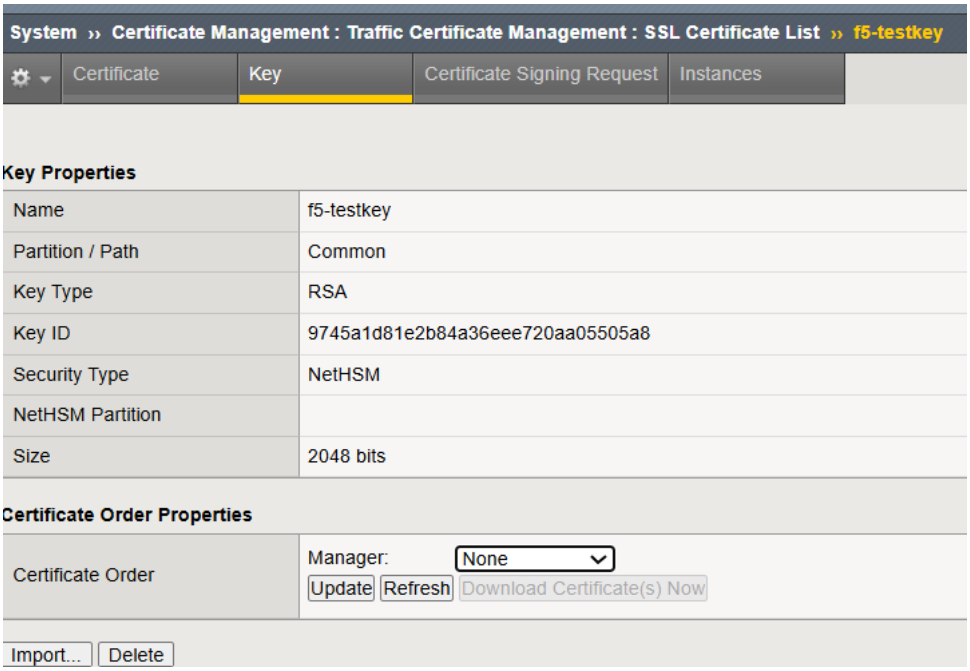

Figure 9 : Generated Key available in GUI

5.2.2 Verify Key Availability on the HSM

Login to BIG-IP CLI and use p11tool to verify if the Keys are available on the HSM.

```
#./p11tool2 LoginUser=12345678 ListObjects
 CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = 709BEDBE-5200-47CC-92E7-4A639C9AB0BC
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       = BIGIPTest1___03c9f2fd
  CKA_ID                          =
                0x38303137 31316435 65323265 36383931 |801711d5e22e6891|
                  38343330 66376334 30336339 66326664 |8430f7c403c9f2fd|


  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = 74E283EC-82A4-4587-8F84-C3A7C8847578
  CKA_SENSITIVE                   = CK_TRUE
```

```
  CKA_EXTRACTABLE                = CK_FALSE
  CKA_LABEL                      = f5-testkey___a05505a8
  CKA_ID                         =
                0x39373435 61316438 31653262 38346133 |9745a1d81e2b84a3|
                  36656565 37323061 61303535 30356138 |6eee720aa05505a8|
```

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

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

There are two ways to import keys:

1. By using the BIG-IP Configuration Utility (GUI).
2. With Traffic Management Shell (tmsh).

5.2.3.1 Import a Key Using BIG-IP Configuration Utility (GUI)

1. Generate a key using the PKCS#11 tool.

```
#./p11tool2 slot=0 LoginUser=12345678 PubKeyAttr=CKA_LABEL="F5-
BIGIPImport1",CKA_ID=0x525341 PrvKeyAttr=CKA_LABEL="F5-BIGIPImport1",CKA_ID=RSA
GenerateKeyPair=RSA
```

2. Verify that the key was generated.

```
# ./p11tool2 LoginUser=12345678 ListObjects
+ 1.2
  CKA_KEY_TYPE                   = CKK_RSA
  CKA_UNIQUE_ID                  = 99A6F928-E14B-4A22-9B1F-C7261D587076
  CKA_LABEL                      = F5-BIGIPImport1
  CKA_ID                         = 0x525341 (RSA)
+ 2.1
  CKA_KEY_TYPE                   = CKK_RSA
  CKA_UNIQUE_ID                  = 44A64C8C-FA89-4676-9CF2-46F92A9B90D9
  CKA_SENSITIVE                  = CK_TRUE
  CKA_EXTRACTABLE                = CK_FALSE
  CKA_LABEL                      = F5-BIGIPImport1
  CKA_ID                         = 0x525341 (RSA)
```

3. Open the BIG-IP configuration utility.

4. In the Main tab, select **System > Certificate Management >Traffic Certificate Management > SSL Certificate list > Import**. The SSL Certificate/Key Source page opens.
5. Select Key from the **Import Type** drop-down.
6. Enter the Key Name in the **Key Name** text box (use the same key label as generated using p11tool2).
7. Select the **New** radio button from **Key Name**.
8. Select From NetHSM within **Key Source.**
9. Select auto from the **NetHSM Partition** drop-down.
10. Click on the **Import** button to import the key.

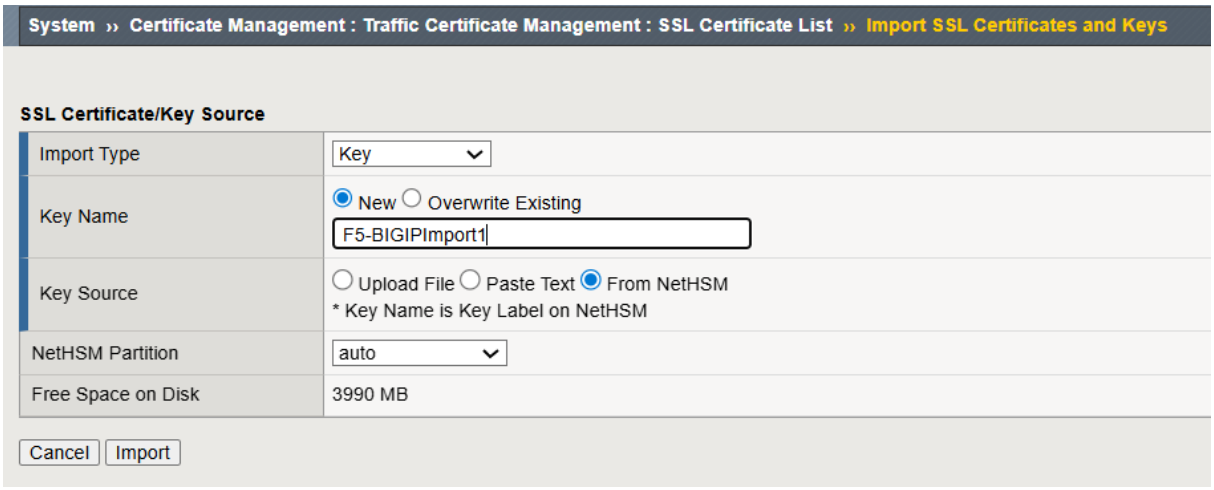

Figure 10 : Import SSL Certificates and Keys Window

11. Go to the **SSL Certificate List** screen and check that the imported key is available in the table.

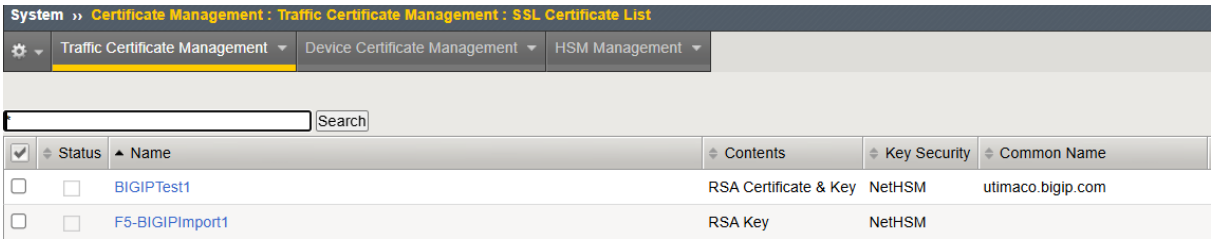

Figure 11 : Imported Key displayed in table

12. Click on the Key name and click on the **Key** tab to check the **Key ID**.

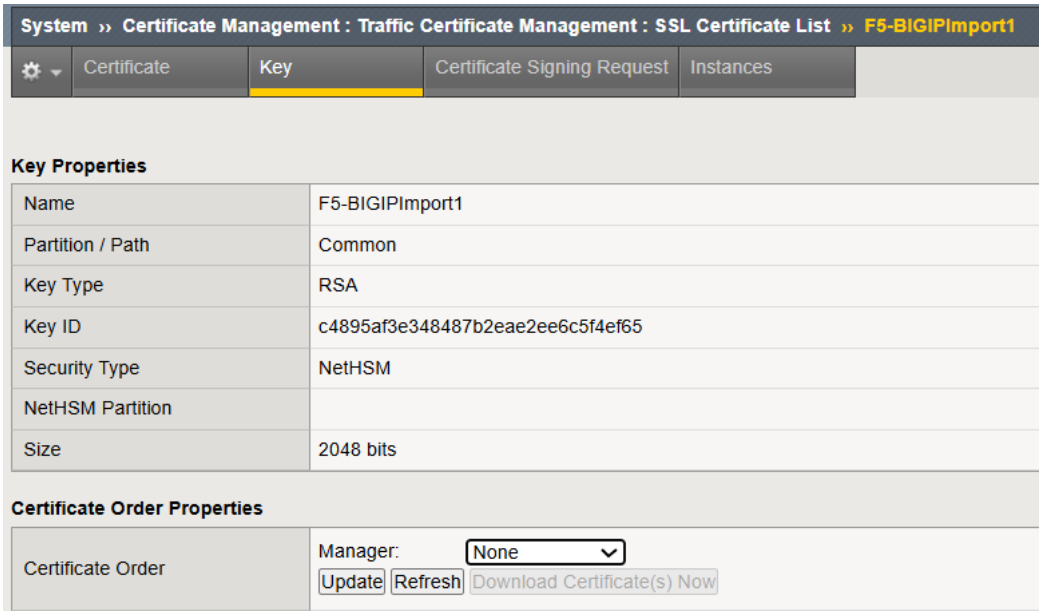

Figure 12 : Imported Key Details

5.2.3.2 Import a Key Using TMSH

1. Generate a key using PKCS#11 tool.

```
#./p11tool2 slot=0 LoginUser=12345678 PubKeyAttr=CKA_LABEL="F5-
BIGIPImport2",CKA_ID=0x525341 PrvKeyAttr=CKA_LABEL="F5-BIGIPImport2",CKA_ID=RSA
GenerateKeyPair=RSA
```

2. Verify that the key was generated.

```
#./p11tool2 LoginUser=12345678 ListObjects

  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = BC4C09DC-1446-45FC-8318-7EF5DF7F7A86
  CKA_LABEL                       = F5-BIGIPImport2
  CKA_ID                          = 0x525341 (RSA)

  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = 862415F9-DAD1-4E10-95C7-AA4D685D2C25
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       = F5-BIGIPImport2
```

```
CKA_ID                          = 0x525341 (RSA)
```

3. Open BIG-IP in tmsh and run the command below.

```
(tmsh)#install sys crypto key F5-BIGIPImport2 from-nethsm security-type nethsm
(tmsh)#save sys config
```

4. Open the BIG-IP configuration utility.
5. In the Main tab, select System > Certificate Management >Traffic Certificate Management > SSL Certificate list and check the imported keys available in the table.

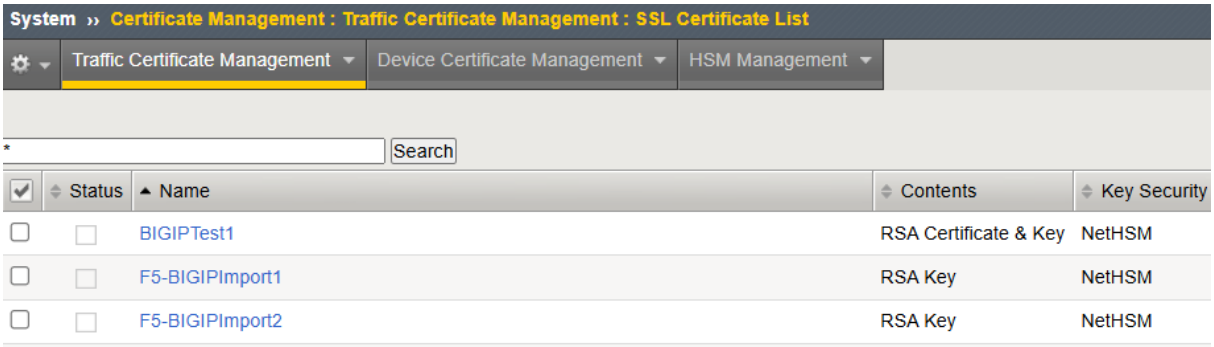

Figure 13 : Imported Key displayed in table

6. Click on the Key name and click on the Key tab to check the Key ID.

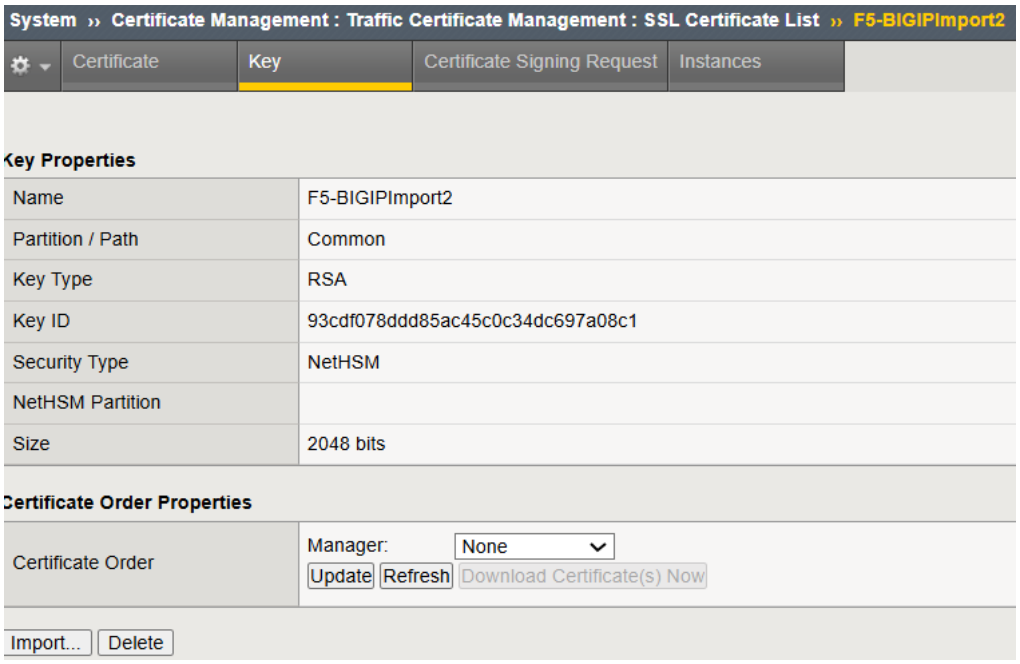

Figure 14 : Imported Key Details

6 Verification and Testing

6.1 Deleting a Key from the BIG-IP

1. In the BIG-IP configuration utility, 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 selected is only deleted from BIG-IP.

```
# ./p11tool2 LoginUser=12345678 ListObjects

  CKA_KEY_TYPE                    = CKK_RSA
 CKA_UNIQUE_ID                   = 44A64C8C-FA89-4676-9CF2-46F92A9B90D9
 CKA_SENSITIVE                   = CK_TRUE
 CKA_EXTRACTABLE                 = CK_FALSE
 CKA_LABEL                       = F5-BIGIPImport1
 CKA_ID                          =
               0x63343839 35616633 65333438 34383762 |c4895af3e348487b|
                 32656165 32656536 63356634 65663635 |2eae2ee6c5f4ef65|

 CKA_KEY_TYPE                    = CKK_RSA
 CKA_UNIQUE_ID                   = 709BEDBE-5200-47CC-92E7-4A639C9AB0BC
 CKA_SENSITIVE                   = CK_TRUE
 CKA_EXTRACTABLE                 = CK_FALSE
 CKA_LABEL                       = BIGIPTest1___03c9f2fd
 CKA_ID                          =
               0x38303137 31316435 65323265 36383931 |801711d5e22e6891|
                 38343330 66376334 30336339 66326664 |8430f7c403c9f2fd|
```

6. Try to create a new Certificate and Key with the same name. BIG-IP will return an error.
7. Delete the key from HSM.

```
 # ./p11tool2 LoginUser=12345678 Label=F5-BIGIPImport1  DeleteObject
2 Objects deleted
```

8. Create a new Key through **System > Certificate Management > Traffic Certificate Management**.

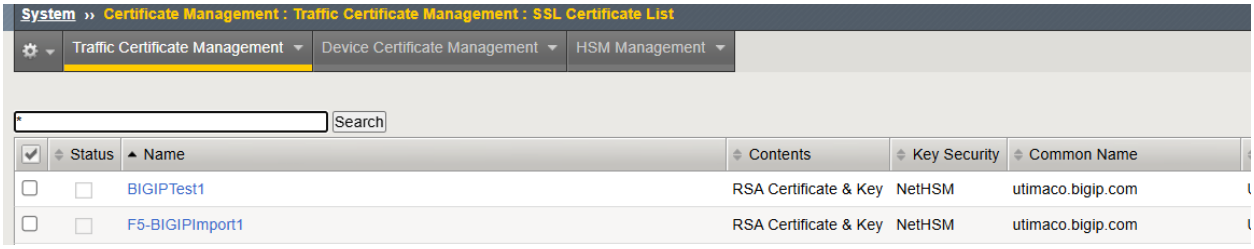

Figure 15 : New Key Created

9. Verify the object in the HSM.

```
 # ./p11tool2 LoginUser=12345678 ListObjects


CKO_PRIVATE_KEY:

+ 1.1
  CKA_KEY_TYPE                    = CKK_RSA
  CKA_UNIQUE_ID                   = 56860D8C-A6C6-481D-82AC-C2110F652C61
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       = F5-BIGIPImport1___5119ac99
  CKA_ID                          =
                0x64336432 65363731 31346635 62363931 |d3d2e67114f5b691|
                  64373836 35316433 35313139 61633939 |d78651d35119ac99|
```

6.2 Logs and Validation Steps

Effective logging is essential for monitoring, troubleshooting, and validating system behavior during configuration and testing. Whether you're integrating security modules like PKCS#11 or managing BIG-IP operations, logs provide critical insights into system events, errors, and performance.

This section outlines the key logging mechanisms involved in both the PKCS#11 module and the BIG-IP environment. It includes guidance on enabling, locating, and interpreting log files to support smooth testing and reliable diagnostics.

6.2.1 PKCS#11 Logs

To facilitate easier testing and troubleshooting, it's recommended to enable PKCS#11 logging. This can be done by configuring the Logging Loglevel and LogPath parameters in the configuration file.

LogPath should point to a writable directory (not a specific file) where log files can be stored.

Logging Loglevel controls the verbosity of the logs:

- Set it to 1 for basic logging.
- For detailed testing and debugging, increase the level to 4.

The generated log file will be named cs_pkcs11_R3.log and located in the directory specified by LogPath. Reviewing this log file can help identify and resolve issues that arise during testing.

Once testing is complete, it is advisable to reduce the Logging Loglevel to 1 or 2 to limit logging to only critical or important messages, thereby optimizing performance and reducing unnecessary log data.

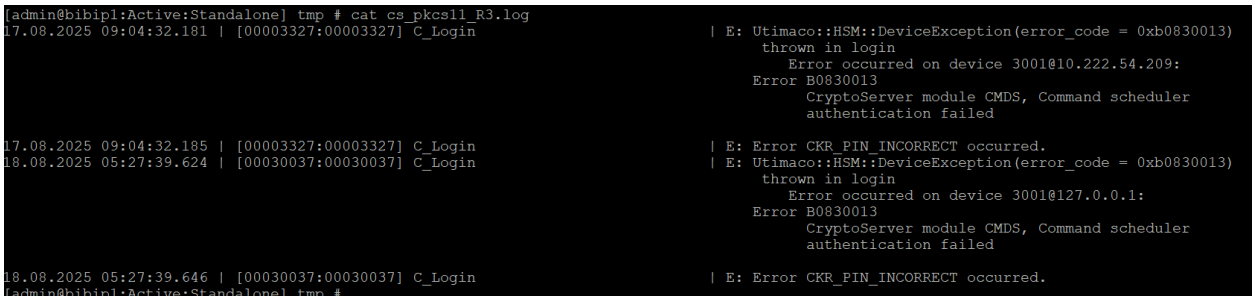

Figure 16 : Sample PKCS11 Log

6.2.2 BIG-IP Logs

In BIG-IP, several logs and trace files are available to monitor and troubleshoot the operations. Out of all logs available, Audit and System logs are most important to the integration.

1. Audit Log

Location: /var/logs/audit

GUI : System → Logs → Audit

Purpose: This log records user login and logout events, configuration changes made (via GUI, CLI, or API), command executions, and system-level actions such as module provisioning and license updates. These logs are essential for security auditing, ensuring compliance with standards (eg., PCI-DSS and HIPAA), troubleshooting unauthorized changes, and tracking administrative activities.

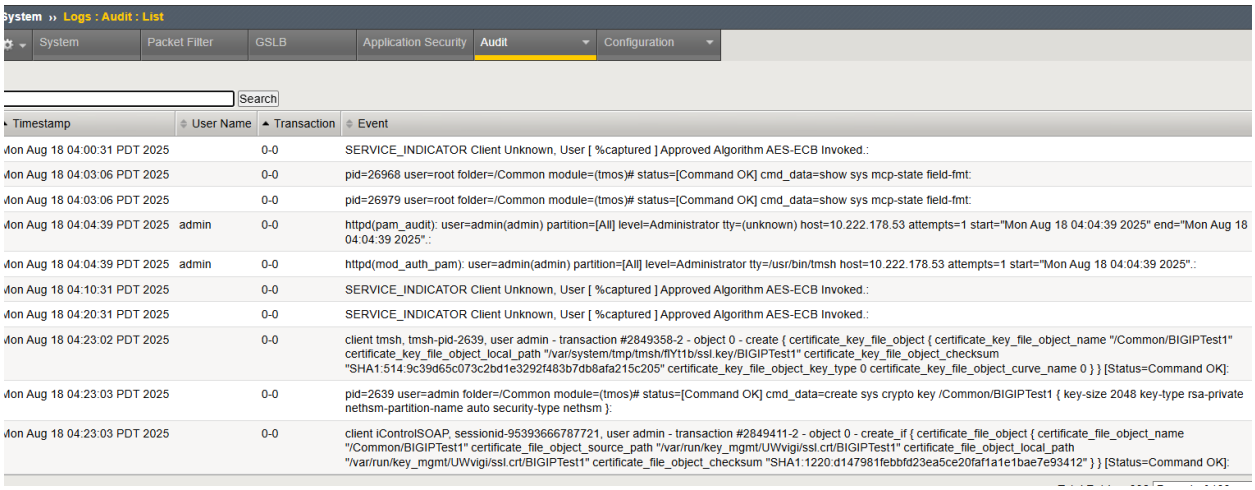

Figure 17 : Sample Audit Logs

2. **System Logs**

Location : /var/logs/messages

GUI : System → Logs → System

Details: System logs include system messages, daemon logs, startup and shutdown events, resource usage warnings, interface or link status changes, and issues related to licensing and module provisioning. System logs are used to monitor and troubleshoot the overall health and operation of the system.

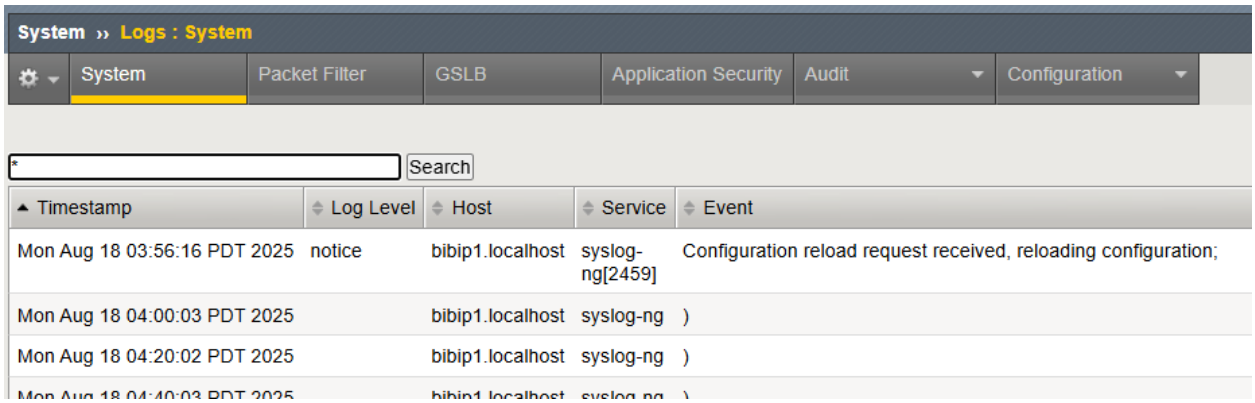

Figure 18 : Sample System Log

7 Troubleshooting

7.1 Common Issues and How to Resolve Them

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. 3. 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.
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. 2. Check if HSM is up and running . 3. Restart the pkcs11d service # bigstart restart pkcs11d

Error	Diagnosis
Data Input Error: The requested key(f5key1) already exists in this scope	The key name already exists. Try with a unique key name.
From Configuration Utility, if the user is trying to import a pre-existing NetHSM Key and gets the following error: Import Failed: Key management library returned bad status: 0, Unable to read POST response data.	1. Check that the key attributes are correct. 2. Make sure the Name and the Label of the Key match while importing. 3. Verify if the key exists that 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 the SecurityServer Application is up, running, and connected to HSM. 2. Check if the Configuration File is pointing towards the IP Address of the HSM.

Table 6: List of Error and its Diagnosis

7.2 Log Locations and Interpretation

Understanding where logs are stored is essential for effective troubleshooting. Below are the key log file locations for both PKCS#11 and BIG-IP.

7.2.1 PKCS#11 Log File

- Log File Name: cs_pkcs11_R3.log
- Location: Defined by the LogPath parameter in the PKCS#11 configuration file. Example: \tmp for Linus and C:\ProgramData\Utimaco\PKCS11_R3\ for Windows

- Details: This log captures detailed information about PKCS#11 operations, including initialization, cryptographic actions, and error messages. The verbosity is controlled by the Logging Loglevel setting.

7.2.2 BIG-IP Audit and System Log Files

1. Audit Log

Log File Name: audit

Location:

Folder : /var/logs

GUI : System → Logs → Audit

Details: Audit logs in BIG-IP record user login and logout events, configuration changes made (via GUI, CLI, or API), command executions, and system-level actions such as module provisioning and license updates. These logs are essential for security auditing, ensuring compliance with standards (eg., PCI-DSS and HIPAA), troubleshooting unauthorized changes, and tracking administrative activities.

2. System Logs

Log File Name: messages

Location:

Folder : /var/logs

GUI : System → Logs → System

Details: System logs include system messages, daemon logs, startup and shutdown events, resource usage warnings, interface or link status changes, and issues related to licensing and module provisioning. System logs are used to monitor and troubleshoot the overall health and operation of the system.

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 References

This document provides a detailed guide for integrating Utimaco's u.trust GP HSM Se-Series with F5 BIG-IP. For further details on Utimaco's full range of products, solutions, and documentation, please visit the official Utimaco Portal.

9.2 Command Summary (CLI commands used)

Command Used	Purpose
#./p11tool2 slot=<slot#> Label=<TokenLabel> Login=<AdminUser>,<AdminKeyPath> Force=1 InitToken=<SO_PIN>	To Initialize Token with Security Officer PIN
#./csadm dev=<device> Logonpass=SO/USR_<slot#>,<old_PIN> changeuser=SO/USR_<slot#>,<new_PIN>	To Change User or SO PIN
#./p11tool2 slot=<slot#> LoginSO=<SO_PIN> InitPin=<User_PIN>	To Initialize User PIN
#./csadm dev=<device> LogonSign=<AdminUser>,<AdminKeyPath> ListUsers	To List all users details
#./p11tool2 LoginUser=<User_PIN> GetSlotInfo	To Get Slot Information
#./p11tool2 LoginUser=<User_PIN> GetTokenInfo	To Get Token Information
#./csadm dev=<device> LogonSign=<AdminUser>,<AdminKeyPath> Key=<MBK1_Label>#<User_PIN>,<MBK2_Label>#<User_PIN> MBKGenerateKey=AES,32,2,2,<Keyname>	To Generate MBK keys

Command Used	Purpose
#./csadm dev=<device> LogonSign=<AdminUser>,<AdminKeyPath> Key=<MBK1_Label>#<User_PIN>,<MBK2_Label>#<User_PIN> MBKImportKey=<slot#>	To Import MBK keys
#./csadm dev=<device> LogonSign=<AdminUser>,<AdminKeyPath> MBKListKeys	To List MBK keys
#<tmsh> create sys crypto key <KeyName> gen-certificate \ common-name <CN> nethsm-partition-name auto security-type NetHSM	To Create Crypto Key and Certificate
#<tmsh> list sys crypto key <KeyName>	To List Crypto Key Details
#<tmsh> save sys config	To Save the Configuration
#./p11tool2 slot=<slot#> LoginUser=<User_PIN> PubKeyAttr=CKA_LABEL="<Label>",CKA_ID=RSA PrvKeyAttr=CKA_LABEL="<Label>",CKA_ID=RSA GenerateKeyPair=RSA	To Generate RSA Key Pair in HSM
#<tmsh>install sys crypto key <KeyName> from-nethsm security-type nethsm	To Install Key from NetHSM

Table 7: CLI Commands