Oracle Key Vault

Integration Guide

Utimaco GP 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-2025-0012

Table of Contents

1 Introduction

Oracle Key Vault is a full-stack software appliance that contains an operating system, database, and key-management application to help organizations store and manage their keys and credentials.

The administrators should deploy Key Vault in a secure location and typically need not access the internal components of the appliance for day-to-day operations. However, there are patches and scenarios where administrators might need to physically access the machine, or directly connect to the internal operating system via SSH. When an HSM is deployed with Oracle Key Vault, the Root of Trust (RoT) remains in the HSM. The HSM RoT protects the wallet password, which protects the TDE master key, which in turn protects all the encryption keys, certificates, and other security artifacts managed by the Oracle Key Vault server. This mitigates the risk of administrators potentially extracting keys and credentials from systems they can physically access. The HSM in this RoT usage scenario does not store any customer encryption keys. Customer keys are stored and managed directly by the Oracle Key Vault server.

Utimaco CryptoServer is a hardware security module or HSM, a physically protected specialized computer unit designed to securely perform sensitive cryptographic operations, manage and store cryptographic keys and data.

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

http://hsm.utimaco.com.

2 Document Conventions

We use the following document conventions:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Document conventions

We use special icons 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.

Certifications

Chapters with certification-specific content are marked accordingly at the beginning of the chapter, e.g. FIPS 140-3.

3 Overview

Utimaco provides a PKCS#11 library interface to our HSM hardware.

- `libcs_pkcs11_R3.so` (shared)
- `libcs_pkcs11_R3_m.a` (static)

Utimaco provides tools for managing users and PKCS#11 on the HSMs.

- Utimaco CryptoServer Admin Tool (csadm)
  Administration tool for the CryptoServer HSM LAN and PCIe card
- Utimaco CXI Tool (cxitool)
  Administration tool for creation, use and management of CXI keys
- UtimacoPKCS#11 Tool (p11tool2)
  Administration tool for PKCS#11 slots, SO and USER and PKCS#11 keys

Combined, the tools are used to configure the Utimaco HSM to hold cryptographic materials. The HSM holds the Root of Trust symmetric encryption key for OKV.

4 Supported Software and HSM Models

Software Packages

- Utimaco `libcs_pkcs11_R3.so` and CryptoServer HSM
- Oracle Key Vault 21.2 or newer release with PKCS11 support

HSM Models Supported

- CryptoServer GP HSM Cse Series, and Se2 Series CSLAN
- U-Trust Anchor CSAR GP HSM CSLAN

HSM Releases Tested

- SecurityServer 4.40.0.2
- SecurityServer 4.45.2.0

Setup an account on the Utimaco support portal and request download access at the following URL.

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

5 Software Download and Extraction

This section describes the process of installing Utimaco HSM software on the Oracle Key Vault server.

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. All Utimaco docs are included.

If you have purchased an HSM from Utimaco, locate the included product bundle, which contains the Linux software packages.

Extract Software

The Utimaco HSM software comes in a zip file package. Create a directory, place the zip file into the directory and unzip.

You will see the `./Software/Linux/x86-64/Crypto_APIs/PKCS11_R3/lib` which contains the `libcs_pkcs11_R3.so` PKCS#11 provider and the `./Software/Linux/x86-64/Adminstration` which contains the csadm, cxitool, and p11tool2.

You will need to place this software in the correct location on your OKV system.

6 PKCS#11 Configuration

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-V4.45.2.0 directory, `Linux/x86-64/Crypto_APIS/PKCS11_R3/sample`.

```
# 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
```

Edit the `cs_pkcs11_R3.cfg` file you copied to direct it to use your Utimaco HSM device.

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

```
# Set the log path

[Global]

# Path to the logfile (name of logfile is attached by the API)

# For unix:

LogPath = /tmp

# Set the Loglevel

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

Logging = 1

# Set the Device to connect with

[CryptoServer]

# Device specifier
Device = 288@10.0.0.164
```

For deployments with u.trust Anchor, the port number will be in the range 4001 thru 4032 or 4001@10.0.0.164 for example.

For this example the Utimaco HSM is at IP address 10.0.0.164. You need to set the Device to reflect your actual HSM IP address. Ensure that the file `cs_pkcs11_R3.cfg` is accessible to OKV. Recommend setting the permissions to `chmod 555` and `chown oracle:oinstall`.

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.

7 Software Installation

Login to the Oracle Key Vault Server through SSH as user"support", and then switch user (`su -`) to `root`. Follow the instructions included in the product bundle included with your HSM purchase. You will be installing the commands and libraries to the Oracle Key Vault server.

Since you are installing for a Linux environment you will need to manually copy the tools and libraries. Oracle OKV expects to find these components in the `/opt/utimaco` sub-directory. Make certain you add this directory to the $PATH variable in your user environment. This would be the `.bashrc` or `.profile` file found with each user.

Copy the command line tools to the `/opt/utimaco/bin` directory. These command line tools can be used to verify proper connection and operation of the Utimaco HSM. Copy the `libcs_pkcs11_R3.so` library to the `/opt/utimaco/lib`. It will be referenced by Oracle OKV as the PKCS#11 provider. For detailed information on PKCS#11, see the *CryptoServer PKCS#11 R3 - Developer Guide*.

8 PKCS#11 Provider Installation

To install the PKCS#11 provider library and tools, you will need to copy the pkcs#11 provider library and command line tools to a place where OKV can find it.

Release V4.45.2.0 location of tools:

```
# cd <install directory>/Software/Linux/x86-64/
```

```
# cp ./Crypto_APIs/PKCS11_R3/lib/libcs_pkcs11_R3.so
```

```
/opt/utimaco/lib
```

```
# cp ./Administration/p11tool2 /opt/utimaco/bin
```

```
# cp ./Administration/cxitool /opt/utimaco/bin
```

```
# cp ./Administration/csadm /opt/utimaco/bin
```

```
# chmod 550 /opt/utimaco/bin/*
```
_ Make commands executable

```
# chmod 440 /opt/utimaco/lib/*
```
_ Make readable by OKV

9 Replace ADMIN with OKVADMIN User

Now would be a good time to change the default ADMIN user to define your own OKVADMIN user. The currently defined ADMIN user is common to all Utimaco HSM. This is a security issue, as anyone with a copy of the `ADMIN.key` can access your HSM as ADMIN or the root user.

We will cover the process of creating your own new RSA key file. Creation of the new OKVADMIN user and the deletion of the existing ADMIN user. This new OKVADMIN user will have the same permissions mask as the exiting ADMIN user. It will now be accessed via your new RSA key file.

You also have the option of creating (2) ADMIN users and providing a (4) eyes access control. The details of this option are covered in the Utimaco csadm documentation included with the software bundle.

Locate the default `ADMIN.key` which can be found in the Utimaco Software at the following location. It is the default RSA key for the ADMIN user.

`./Software/Linux/x86-64/Administration/key/ADMIN.key`

Here are the steps you need to create a new OKVADMIN user and delete the old default ADMIN user.

```
# csadm listusers

Name      Permission   Mechanism      Attributes
ADMIN      22000000    RSA sign       Z[0]

# csadm KeyType=RSA GenKey=OKVADMIN.key,"OKV Admin Key File“
# csadm LogonSign=ADMIN,ADMIN.key AddUser=OKVADMIN,22000000,rsasign,OKVADMIN.key
# csadm LogonSign=OKVADMIN,OKVADMIN.key DeleteUser=ADMIN
# csadm listusers

Name      Permission   Mechanism      Attributes
OKVADMIN   22000000    RSA sign       Z[0]

# csadm LogonSign=OKVADMIN,OKVADMIN.key <CSADM Command>
```

Secure the `OKVADMIN.key` . You have the option of placing it onto a smartcard and using that mechanism for administrator authentication

10 PKCS#11 Setting up PKCS#11

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

10.1 Initialize a Slot

Oracle OKV 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 and the second p11tool2 command initializes the Slot 0 User.

Make sure that you secure the new `OKVADMIN.key` which you just created. You will need that key to perform any Administrative functions on the Utimaco HSM.

10.2 Setting up your PKCS#11 users

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

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

```
# /opt/utimaco/bin/p11tool2 slot=0 Label=OKVDemo Login=OKVADMIN,OKVADMIN.key
InitToken=123456
# /opt/utimaco/bin/p11tool2 slot=0 LoginSO=123456 InitPin=123456
```

Now check to see that you can access the Slot 0.

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

  CK_INFO:
  cryptokiVersion    : 3.00
  manufacturerID       5574696d 61636f20  49532047 6d624820 |Utimaco IS GmbH|
                       20202020 20202020  20202020 20202020 |               |
  flags              : 0x00000000
  libraryDescription   43727970 746f5365  72766572 20504b43 |CryptoServer PKC|
                       53233131 204c6962  72617279 20523320 |S#11 Library R3|
  libraryVersion     : 1.14
```

10.3 List users and verify MBK

Use the `/opt/utimaco/bin/csadm` command, list and confirm the users created.

```
# /opt/utimaco/csadm DEV=10.0.0.164 listusers
Name      Permission   Mechanism      Attributes
OKVADMIN   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]
```

Now check to confirm the Utimaco HSM has an MBK.

```
# csadm Dev=10.0.0.164 LogonSign=OKVADMIN,OKVADMIN.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
```

If no MBK is present you will need to generate one, before you can create any KEYS in the HSM.

Look at the `csadm help=MBKGenerateKey` and `help=MBKImportKey` for how to make this happen. Details can be found in the csadm document.

CryptoServer csadm Manual 5.7 Commands for Managing the Master Backup Keys

10.4 Check the slot

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

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

CK_SLOT_INFO (slot ID: 0x00000000):

slotDescription
31302e31 392e3732 2e323031 202d2053 |10.0.0.164  -  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 : 2.03
```

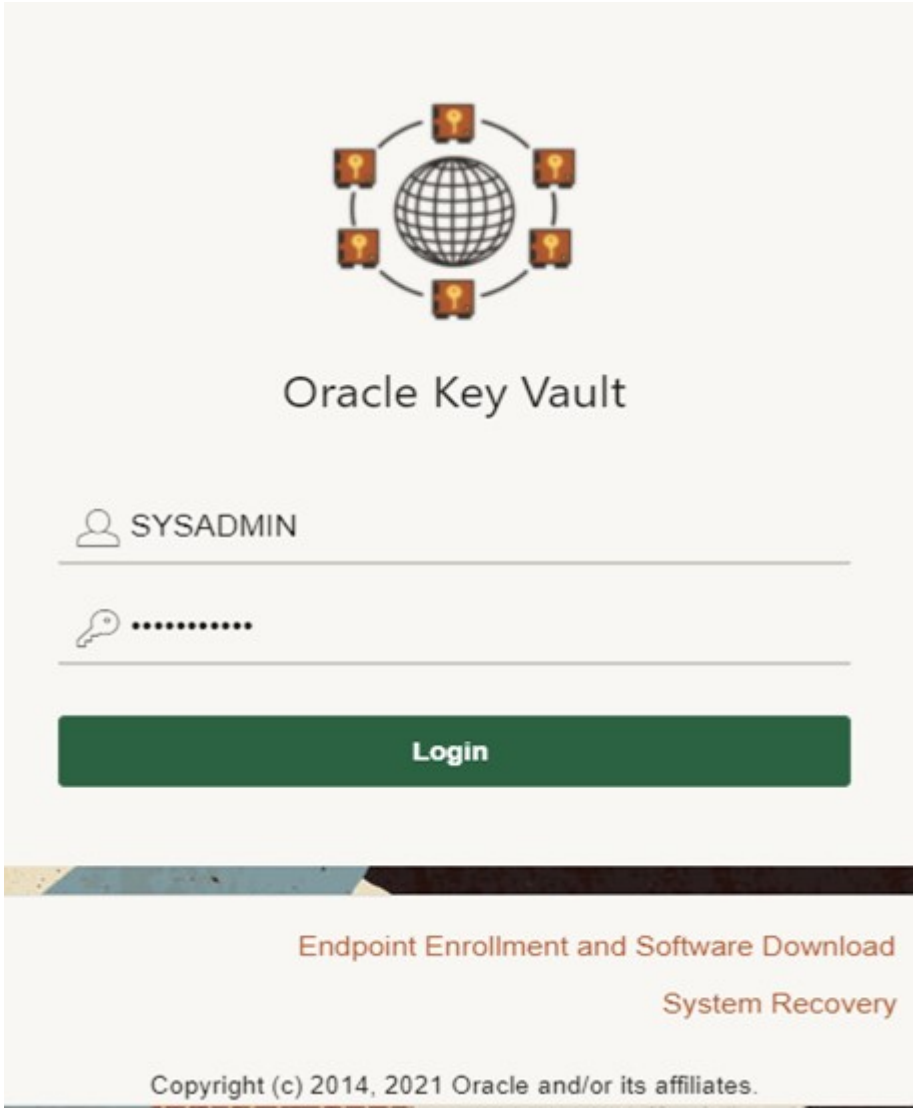
OKV should now be able to access The Utimaco PKCS#11 HSM provider.

11 Oracle Key Vault login

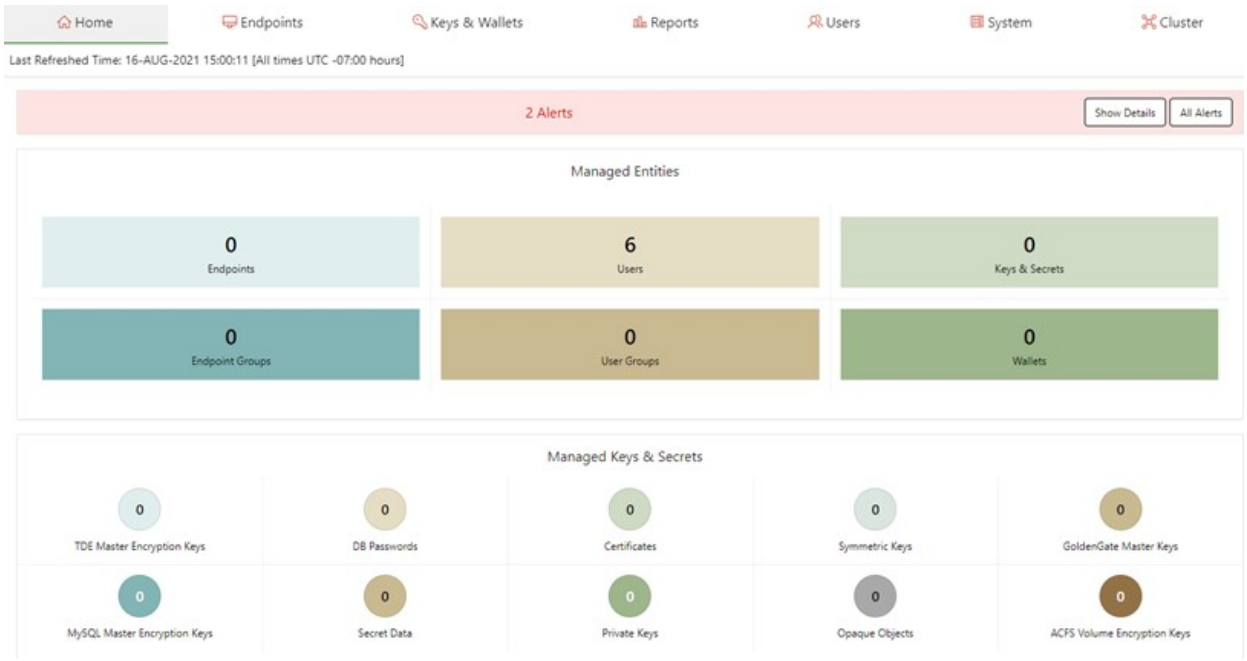
Now that you have the Utimaco HSM PKCS#11 stack configured, you need to connect OKV to the provider.

You will start with initial steps in the OKV web GUI. Then proceed to login via the ssh shell and complete some command line operations.

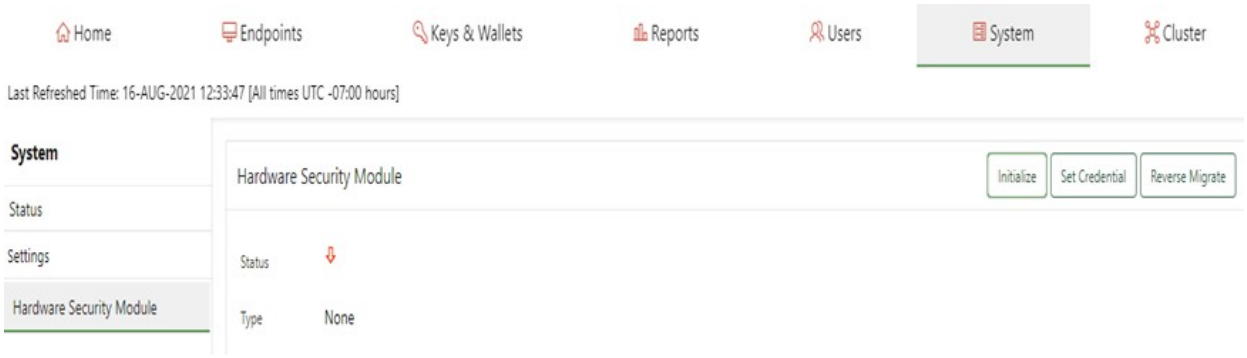
1. Login as the SYSADMIN user that we defined earlier in the OKV setup.



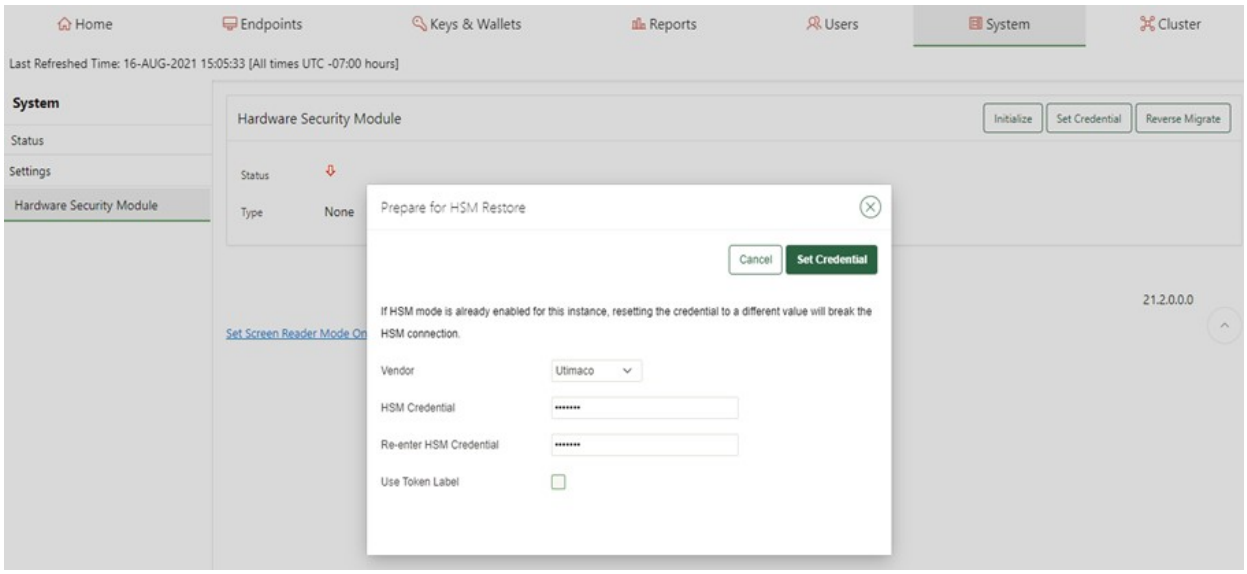
2. You are now in the Oracle OKV Console. You will need to select the **System** tab at the top right of your browser.



3. Now we will Initialize and Set Credential for the HSM
   Ensure that you have the PIN value that were set earlier when you configured the PKCS#11 user. In my case I used the PIN “123456".
   Confirm that the Utimaco PKCS#11 provider library has been installed in the directory that OKV expects. This is specific to the HSM vendor. In our case `/opt/utimaco/li` b.



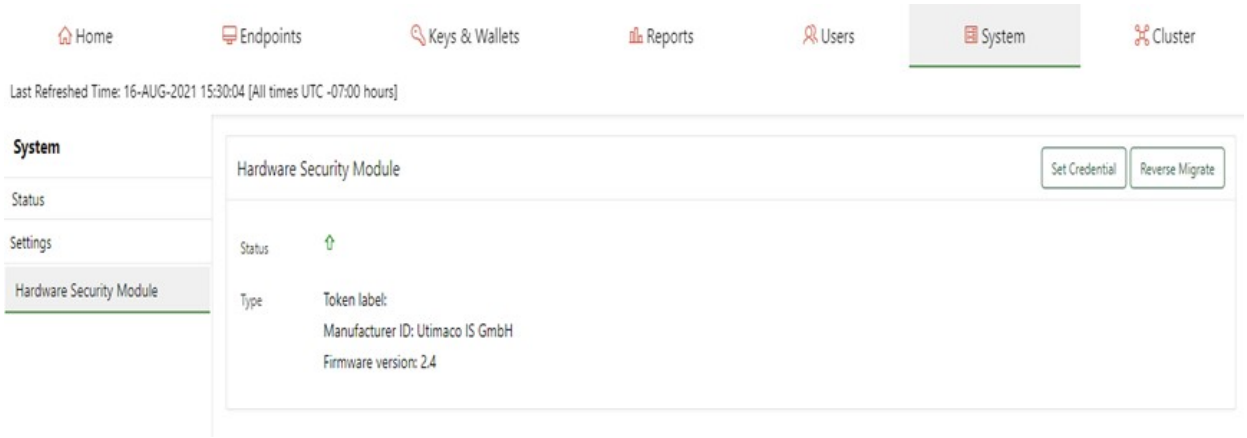
4. Set the HSM vendor to Utimaco. Then set the PIN value for the PKCS#11 token and then confirm that value in the next field. Ensure that the PIN values match.



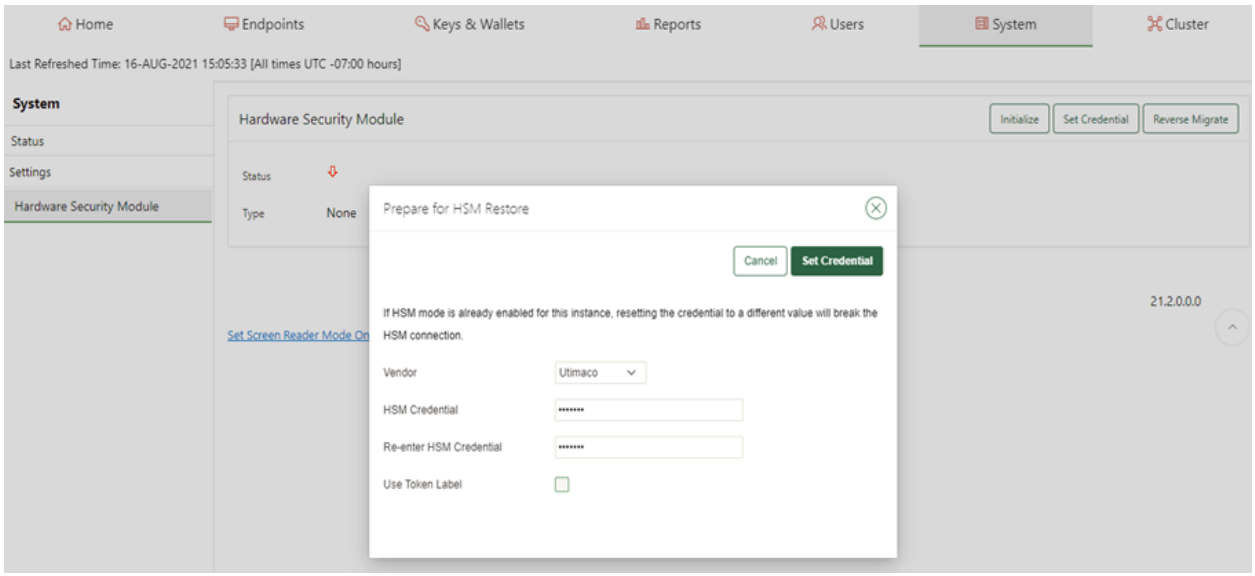
5. A successful initialization will show the following msg.

```
Token label:
Manufacturer ID: Utimaco
IS GmbH and the Firmware version: 2.4
```

You are now ready to set the credentials next.



6. Select the HSM Vendor option and set Utimaco. Then enter the PIN you defined for the Slot 0000 token. Enter it twice.Then select **Set Credential** button.



7. Now you will need to login via ssh to the OKV server and run the following command. Use the ssh RSA key you created when you initialize the OKV instance credentials.

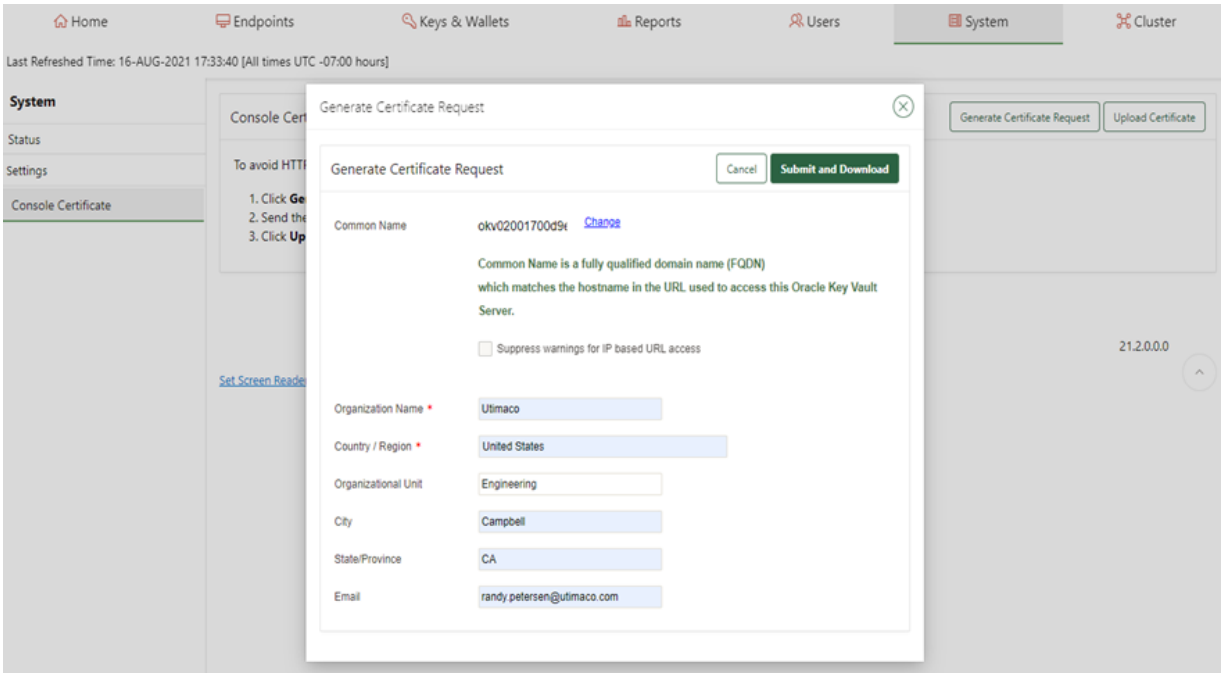
```
# ssh -i ./ssh-key-date.key support@<OKV server IP>

# su -

# /opt/utimaco/bin/p11tool2 GetSlotInfo

CK_SLOT_INFO (slot ID: 0x00000000):

  slotDescription      33303031 4031302e  302e302e 31363420 |10.0.0.164       |
                       2d20534c 4f545f30  30303020 20202020 |- SLOT_0000      |
                       20202020 20202020  20202020 20202020 |                 |
                       20202020 20202020  20202020 20202020 |                 |

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

8. Using the p11tool2 run the following command. It should show the OKV HSM RoT AES key has been set.

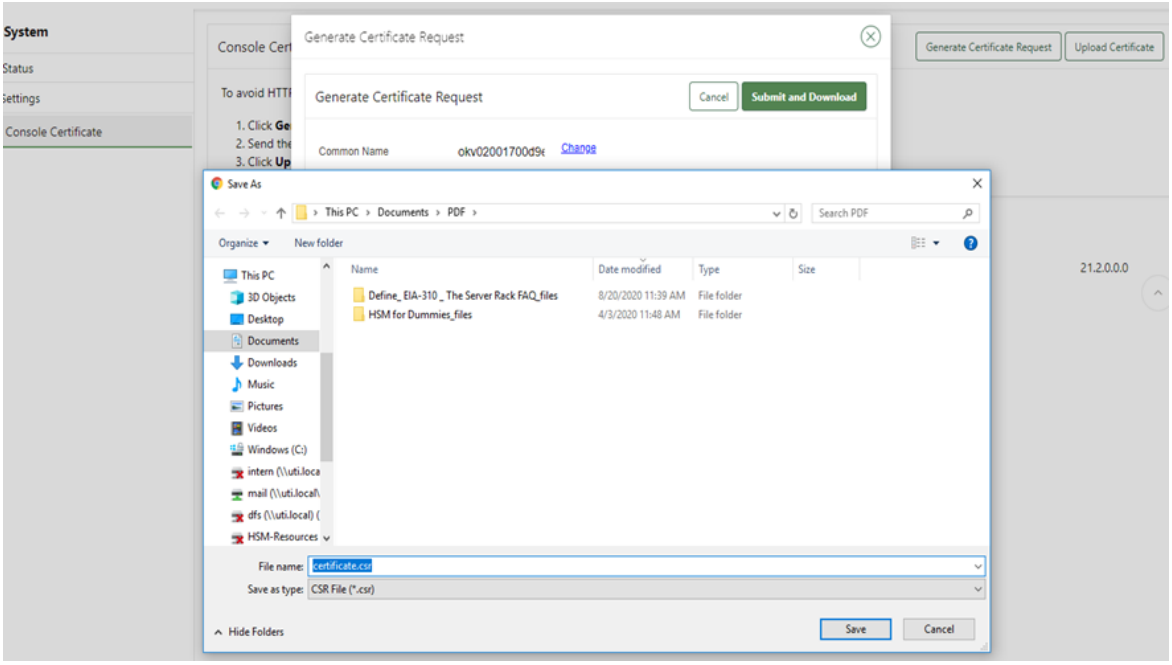
```
# /opt/utimaco/p11tool2 LoginUser=utimaco ListObjects

CKO_DATA:

+ 1.1
  CKA_LABEL                       = OKV 21.2 HSM Key Number
```

```
CKO_SECRET_KEY:

+ 2.1
  CKA_KEY_TYPE                    = CKK_AES
  CKA_SENSITIVE                   = CK_TRUE
  CKA_EXTRACTABLE                 = CK_FALSE
  CKA_LABEL                       = OKV 21.2 HSM Root Key
  CKA_ID                          = 0x00000001 ()
```

9. Check out a crypto operation to see that OKV is working. Generate a Certificate Signing Request.



10. Download the certificate request to your laptop.



11. Display the CSR as generated by OKV.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDHjCCAgYCAQAwgZoxGDAWBgNVBAMMD29rdjAyMDAxNzAwZDllMzEQMA4GA1UE
CgwHVXRpbWFjbzEUMBIGA1UECwwLRW5naW5lZXJpbmcxETAPBgNVBAcMCENhbXBi
ZWxsMQswCQYDVQQIDAJDQTEpMCcGCSqGSIb3DQEJARYacmFuZHkucGV0ZXJzZW5A
dXRpbWFjby5jb20xCzAJBgNVBAYTAlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAmzHixXBPlZN9+vRXvGhP0GdfzcBV6XvTTRqU2DSS0/3FVp8xZIZJ
j9H1bBmFqbEW7RxlMOIh9/uXk5UEj7P3Aiez+nSmz+Ca2tTbTvf3vzFDUk/OsKvv
VlGdpponKLqVlFExpS+bjnBuGlgo9hmQgLruc1GDC57DEyURvnASAmKL+wGqJsdE
V1kn70IDlDZZ6A4p4sOLLOgJItsWVzApk2AANc0bLB/+BSiFUKFDxBSyAqpl7NHn
QzAgLbThuEJdkoZ9vFt4/VU1+HeA83xp5F207ain1jDtXfvRvNWMHRdFbLJDn6MX
zpOLJXUfICE7sxfqFBMwiBcP96okTzNzdwIDAQABoD4wPAYJKoZIhvcNAQkOMS8w
LTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF4DATBgNVHSUEDDAKBggrBgEFBQcDATAN
BgkqhkiG9w0BAQsFAAOCAQEALojYxYGsfSw1RjzwXcxGfveyhH4/5aqhVfwqiA7h
S8s+W7w1Zwu6Qg2V9NISuS9Y3Ek/BXCMyaylEAm1rYp85anAg+RdalgmH+uza9a1
H5PJjDbNjUwjNS6FCuKNWDqf8sT11Q4CY6ka3oU3VTSqOS4eel7b2Fx1hMh01fXK
baSOEfJm7+6f4pLMiuIcrZWSymzBLTP9j//WK3mNynWE0NAXBGfepdhzey3CC31M
A5R3bHvVk2heEK0VnzzWtymDkcK5lGV5/KdEcU+Tpn+7xCePrmYmH6pW20GBpVn4
zT/LU4mpmWvG38BBRJuD/58K7iLGXFg1DCchffyJfwd69w==
-----END CERTIFICATE REQUEST-----:
```

12. Use openssl to verify the created CSR and output the PEM format.

```
# openssl req -text -noout -verify –in cert.csr >cert.pem
verify OK
```

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: CN=okv02001700d9e3, O=Utimaco, OU=Engineering, L=Campbell, ST=CA/
        emailAddress=ruser@utimaco.com, C=US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9b:31:e2:c5:70:4f:95:93:7d:fa:f4:57:bc:68:
                    4f:d0:67:5f:cd:c0:55:e9:7b:d3:4d:1a:94:d8:34:
                    92:d3:fd:c5:56:9f:31:64:86:49:8f:d1:f5:6c:19:
                    85:a9:b1:16:ed:1c:65:30:e2:21:f7:fb:97:93:95:
                    04:8f:b3:f7:02:27:b3:fa:74:a6:cf:e0:9a:da:d4:
                    db:4e:f7:f7:bf:31:43:52:4f:ce:b0:ab:ef:56:51:
                    9d:a6:9a:27:28:ba:95:94:51:31:a5:2f:9b:8e:70:
                    6e:1a:58:28:f6:19:90:80:ba:ee:73:51:83:0b:9e:
                    c3:13:25:11:be:70:12:02:62:8b:fb:01:aa:26:c7:
                    44:57:59:27:ef:42:03:94:36:59:e8:0e:29:e2:c3:
                    8b:2c:e8:09:22:db:16:57:30:29:93:60:00:35:cd:
                    1b:2c:1f:fe:05:28:85:50:a1:43:c4:14:b2:02:aa:
                    65:ec:d1:e7:43:30:20:2d:b4:e1:b8:42:5d:92:86:
                    7d:bc:5b:78:fd:55:35:f8:77:80:f3:7c:69:e4:5d:
                    b4:ed:a8:a7:d6:30:ed:5d:fb:d1:bc:d5:8c:1d:17:
                    45:6c:b2:43:9f:a3:17:ce:93:8b:25:75:1f:20:21:
                    3b:b3:17:ea:14:13:30:88:17:0f:f7:aa:24:4f:33:
                    73:77

 Exponent: 65537 (0x10001)
 Attributes:
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         2e:88:d8:c5:81:ac:7d:2c:35:46:3c:f0:5d:cc:46:7e:f7:b2:
         84:7e:3f:e5:aa:a1:55:fc:2a:88:0e:e1:4b:cb:3e:5b:bc:35:
         67:0b:ba:42:0d:95:f4:d2:12:b9:2f:58:dc:49:3f:05:70:8c:
         c9:ac:a5:10:09:b5:ad:8a:7c:e5:a9:c0:83:e4:5d:6a:58:26:
         1f:eb:b3:6b:d6:b5:1f:93:c9:8c:36:cd:8d:4c:23:35:2e:85:
         0a:e2:8d:58:3a:9f:f2:c4:f5:d5:0e:02:63:a9:1a:de:85:37:
         55:34:aa:d1:2e:1e:7a:5e:db:d8:5c:75:84:c8:74:d5:f5:ca:
         6d:a4:b4:11:f2:66:ef:ee:9f:e2:92:cc:8a:e2:1c:ad:95:92:
         ca:6c:c1:2d:33:fd:8f:ff:d6:2b:79:8d:ca:75:84:d0:d0:17:
         04:67:de:a5:d8:73:7b:2d:c2:0b:7d:4c:03:94:77:6c:7b:d5:
         93:68:5e:10:ad:15:9f:3c:d6:b7:29:83:91:c2:b9:94:65:79:
         fc:a7:44:71:4f:93:a6:7f:bb:c4:27:8f:ae:66:26:1f:aa:56:
         db:41:81:a5:59:f8:cd:3f:cb:53:89:a9:99:6b:c6:df:c0:41:
         44:9b:83:ff:9f:0a:ee:22:c6:5c:58:35:0c:27:21:7d:fc:89:
         7f:07:7a:f7
```

OKV has connected to the provider successfully.

12 References

Here are some useful documents to help you. They are located at the Oracle OKV site and on the Utimaco web site or in product bundle.

Oracle OKV Documents

- https://docs.oracle.com/en/database/oracle/key-vault/21.2/index.html

Utimaco HSM Administration Documents

- CryptoServer_csadm_Manual_Systemadministrators.pdf
- CryptoServerLAN_Manual_Systemadministrators.pdf
- CryptoServer_Manual_P11CAT.pdf
- CryptoServer_Manual_Systemadministrators.pdf
- CryptoServer_Troubleshooting.pdf

Utimaco PKCS#11 Documents

- CryptoServer_PKCS11_R3_DevGuide.pdf
- PKCS11_HandsOn.pdf