Red Hat and Utimaco HSMApache Certificate System RHEL 7.3

v9

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-2025-0011

All rights reserved

No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.

Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them.

All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1 Integration Details

This is the version constellation, tested by Utimaco.

Operating System	SecurityServer	Red Hat Certificate System
RHEL 7.3	4.10.0.x	9
RHEL 7.3	4.20.0.x	9

If you are using a different platform constellation, and there are discrepencies, please bring these back to the attention of Utimaco (support-cs@utimaco.com), noting the title of this document, and what changes you needed to make.

This document is intended to be used in conjunction with the *Red Hat Certificate System* documentation, see https://www.redhat.com/en/technologies/cloud-computing/certificate-system and the Utimaco PKCS#11 Developers Guide 2, see `<install>/Documentation/Software/Crypto_APIs/PKCS11_R2`.

In order to use this guide, it is assumed that you have the needed, in-depth knowledge of RHEL administration.

Specifically, there must be a local DNS that can be used to serve the qualified domain name of the install server for Dogtag, the underlying technology for the RHEL/CentOs CA instance. This requires active and correctly configured DNS, LDAP, etc, and that these be running prior to starting the ntegration.

Setting up these services is beyond the scope of this document.

TIP

This document is intended to be used as a quick guide in conjunction with Utimaco's PKCS#11 documentation. For more detailed information on specific topics, please refer to the corresponding Utimaco-supplied guides or 3d party installation suggestions/documentation when available.

2 Requirements

2.1 Utimaco CryptoServer

This integration uses the SecurityServer-V4.10.x product CD. Utimaco's PKCS#11 documentation can be found on the product CD: `<install>/Documentation/Crypto_APIs/PKCS_11_R2/`.

The 'appliance' described below is the linux server running the Red Hat Certificate System instance. Where necessary to differentiate, the CryptoServer CSLAN appliance will be referred to as the CSLAN.

Red Hat Certificate Services uses a PKCS#11 backend, so the CryptoServer HSM must be configured for PKCS#11 use, described below.

Additionally, the RHCS runtime also requires a host name found in an active DNS server, as well as a running directory server (LDAP, eg Red Hat Directory Server) instance available to it.

2.2 PKCS#11 R2

In the SecurityServer software, Utimaco includes a PKCS#11 provider library, called 'PKCS#11 R2'. The configuration steps below assume initial configuration of the HSM or HSM cluster has been done (Master Backup Keys imported, etc), and that the HSM(s) is/are ready for use.

It is recommended that you read the entire integration guide prior to implementing the steps below. Other sections may have additional recommendations on how to configure the tokens and or slots, beyond what is described in the generic PKCS#11 configuration section below.

3 Utimaco PKCS#11 Configuration

In order to use the Utimaco HSM as a PKCS#11 device, you need two files from the product CD. The files needed are `cs_pkcs11_R2.cfg` and `libcs_pkcs11_R2.so`.

If you do not already have a PKCS#11 R2 Slot 0 available on the CryptoServer cluster, the quickest way is to follow chapter two of the *PKCS#11 Hands On* pdf. This document is available in the Utimaco SecurityServer installation, at `<install>/Software/Crypto_APIs/PKCS#11_R2/doc/`. The hands-on guide describes setting up a Security Officer token and slot PIN in detail. See the provided documentation for details on how to manage the PKCS#11 API if doing so programmatically.

You can use p11tool2 or p11cat (the PKCS#11 CryptoServer Administration Tool) to set up the slot. The below steps use the p11cat tool, and are an extract of the Hands On pdf. The below assumes no error states will be seen.

3.1 Token creation

The cs_pkcs11_R2.cfg file serves as a configuration file for the PKCS#11_R2 shared object library. Use cp (or scp), to copy these two files from the installation media to the appliance, placing them into /opt/cs/pkcs11_r2 or similar, making note of any changes to this recommendation.

Additionally, the ADMIN.key may optionally be copied to an easy-to-find directory location. This is done as a convenience.

TIP

This assumes you are using the factory-default ADMIN user and the corresponding ADMIN.key credential (keyfile, or factory-default configured smartcard), which will not be the case for a live deployment. If you are using your own corporate HSM Administrator login(s), use that/those here, instead.

The target directory used here for the files is arbitrary.

3.2 Local Setup

3.2.1 SecurityServer 4.10.0.x

>_Console

```
$ mkdir -p /opt/cs/pkcs11_R2
$ cd <install>/Software/Linux/x86-<bitdepth>/Crypto_APIs/PKCS11_R2/sample
$ cp cs_pkcs11_R2.cfg /opt/cs/pkcs11_R2
$ cd ../lib
$ cp libcs_pkcs11_R2.so /opt/cs/pkcs11_R2
$ cd <install>/Software/All_Supported_Operating_Systems/Administration/key
$ cp ADMIN.key /opt/cs
$ cd /opt/cs/pkcs11_R2
```

3.2.2 SecurityServer 4.20.0.x

>_Console

```
$ mkdir -p /opt/cs/pkcs11_R2
$ cd <install>/Software/Linux/x86-<bitdepth>/Crypto_APIs/PKCS11_R2/sample
$ cp cs_pkcs11_R2.cfg /opt/cs/pkcs11_R2
$ cd ../lib
$ cp libcs_pkcs11_R2.so /opt/cs/pkcs11_R2
$ cd <install>/Software/All_Supported_Operating_Systems/Administration/key
$ cd <install>/Software/Linux/x86-<bitdepth>/Administration/key
$ cp ADMIN.key /opt/cs
$ cd /opt/cs/pkcs11_R2
```

File locations can change between versions.

3.3 Setting up the environment

In order for the library to find the configuration file, set the CS_PKCS11_R2_CFG environment variable to point at the configuration file, and the CRYPTOSERVER environment variable to point at the HSM (Simulator, CSLAN or PCIe):

>_Console

```
$ export CS_PKCS11_R2_CFG=/opt/cs/pkcs11_r2/cs_pkcs11_R2.cfg
$ export CRYPTOSERVER=288@10.10.10.200
```

3.3.1 Edit the cs_pkcs11_R2.cfg file in /etc/utimaco directory

Edit the `cs_pkcs11_R2.cfg` copy to direct it to use the HSM. The device may be either the Simulator or a *CryptoServer* (PCIe or CSLAN) device. This example represents an abbreviated set of options, see the documentation for a complete list, and how they are used.

cs_pkcs11_R2.cfg

```
[Global]
LogPath = /tmp
Logging = 4

KeepAlive = true
SlotCount = 1

[CryptoServer]
# Device = 3001@127.0.0.1
# Device = 288@10.10.10.200
# Device = /dev/cs2a
Device = 288@10.10.10.200
```

Device list shows the syntax for the Simulator (3001@...), a CSLAN (288@...) and for a PCIe card installed into the server (/dev/...). The syntax also supports clustering of multiple HSMs to improve performance or provide for highavailability and/or fault tolerence. See the documentation for KCS#11 at (`<install>/Documentation/Crypto_APIs/PKCS11_R2).`

TIP

When moving to production, consider disabling the log by setting `Logging = 0` .

TIP

Ensure you have set KeepAlive to 'true' If HSM connection drops the PIN must be reentered; the system default (KeepAlive = false) is to drop a connection after 15 minutes of no use.

3.4 Create the PKCS#11 User and Security Officer

First, demonstrate that we have access to the HSM, at the Device Specifier found in the configuration file above.

The steps below use a combination of `csadm` and `p11tool2` commands.

The following steps are also possible using the CAT (CryptoServer Administration Tool) and the P11CAT (PKCS#11 CryptoServer Administration Tool).

To verify access, use the csadm tool:

>_Console

```
$ csadm GetState
```

The response to a GetState command is either a table of current data about the state of the CryptoServer, or it is a connection timeout message:

>_Console

```
$ csadm GetState
mode = Operational Mode
state = INITIALIZED (0x00100004)
temp = 23.7 [C]
alarm = OFF
bl_ver = 5.01.0.4 (Model: Se-Series Gen2)
hw_ver = 5.01.0.0
uid = 40000018 84f59001 | @
adm1 = 53653530 30202020 43533630 30303133 | Se500 CSP1013
adm2 = 53656375 72697479 53657276 65722020 | SecurityServer
adm3 = 494e5354 414c4c45 44202020 20202020 | INSTALLED
```

TIP

CryptoServers (HSMs and the Simulator) come with a default **ADMIN** user and **ADMIN. key** keyfile, which can be used as the initial login. Utimaco recommends that you delete this **ADMIN** user once you have installed your own admin users. Do not delete the **ADMIN.key**, however, as returning an HSM to its factory configuration will return the **ADMIN** (and delete all the other users and all key material).

3.5 Login as the ADMIN User

A quick way to test whether you have authenticated access to the CryptoServer is to use a logon command, but without a command. If the user is correctly authenticated, there is no error.

>_Console

```
$ csadm LogonSign=ADMIN,/opt/cs/ADMIN.key
$
```

The error message on a failed logon depends on the type of error received. Consult the documentation for various remedies.

3.6 PKCS#11 CryptoServer p11tool2

>_Console

```
$ p11tool2 ListSlots=status
     slot ID   token init.   PIN init.
     --------------------------------
  0: 00000000  no            no
```

If the response is yes yes the slot is already configured.

Setting up slot 0 is a two-step process. The first step is to log on as the 'Generic' user, who is any set of users who have HSM admin credentials (such as the factory default ADMIN user). The Generic user is used to create the Security Officer (SO) PIN.

>_Console

```
rhel7# p11tool2 Slot=0 Login=ADMIN,/opt/cs/ADMIN.key Label={p11_slot_label}
   InitToken=654321
```

The 'p11_slot_label' in the console text above should be notable and it will be required below when providing the necessary configuration to the pkispawn instance.

TIP

You can chose something different for the PINS discussed here (and below), but remember them for later use. Consider noting them somewhere.

The second step is to use the SO's PIN to configure the User's PIN, and reissue the `ListSlots` command to verify the steps completed correctly.

>_Console

```
$ p11tool2 Slot=0 LoginSO=654321 InitToken=123456
$ p11tool2 ListSlots=status
      slot ID   token init.   PIN init.
      --------------------------------
   0: 00000000  yes           yes
```

3.7 Installation

3.7.1 Initialize a Slot

The Red Hat Certificate System uses the PKCS#11 token **label** to specify the slot to be used, rather than a slot number. To avoid any problems, please make sure the token label you are using is unique. The discussion below assumes that the slot label has been set to redhatcertsrvc.

3.7.2 Preparing the Operating System

To setup the CA, follow the offical Red Hat documentation.

Complete Chapter 6. Prerequisites and Preparation for Installation, then follow 7.2.1. Installing and Configuring a CA until you reach point 4 (When setting up the CA on a host that uses an IPv6 address, apply the steps described in Section 12.6, Enabling IPv6 for a Subsystem.). Do not proceed to the `pkispawn -s CA` step, until after configuring for use of the CryptoServer.

We will supply `pkispawn` with a custom configuration which enables the HSM.

3.7.3 pkispawn' with Custom Configuration

In order to use the HSM, CryptoServer-specific information must be supplied to the pkispawn application. This is done by overriding several default values via a custom configuration file.

The following file represents the minimum parameters required to allow use of the CryptoServer.

If you want to further configure the CA to your specific needs, consult the official Red Hat documentation. Advanced configuration is outside the scope of the Utimaco Integration Guide series; Utimaco System Engineering will not be able to discuss which extended configurations may be of use in our local environment, nor how they may or should be configured, or what side-effects may result with their use.

Create the following file:

```
[DEFAULT]
pki_admin_password=verysecurepassword
pki_ds_password=verysecurepassword
pki_client_pkcs12_password=verysecurepassword

# Provide HSM parameters
pki_hsm_enable=True
pki_hsm_libfile=/opt/cs/PKCS11_R2/libcs_pkcs11_R2.so
pki_hsm_modulename=UtimacoCryptoServer
pki_token_name={p11_slot_label}
pki_token_password=123456

# Provide PKI-specific HSM token names
pki_audit_signing_token=pki_audit_signing_token
pki_ssl_server_token=pki_ssl_server_token
pki_subsystem_token=pki_subsystem_token

[CA]
# Provide CA-specific HSM token names
pki_ca_signing_token=pki_ca_signing_token
pki_ocsp_signing_token=pki_ocsp_signing_token
```

Edit the file to suit your needs, then run

>_Console

```
pkispawn -s CA -f pkispawn.conf
```

After the successful installation, verify that the keys were created in the HSM. Do so for example by running p11tool2.

>_Console

```
root@ns1# p11tool2 slot=0 LoginUser=123456 ListObjects
...
```

You now have a running, HSM-backed CA.

3.8 Troubleshooting

3.8.1 Connection Problems

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

- Verify your HSM is running

  >_Console

  ```
  export CRYPTOSERVER=288@<ipaddr>csadm GetState
  ```

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

  >_Console

  ```
  p11tool2 GetSlotInfo=status
  ```

- Verify that you are using the right **libcs_pkcs11_R2.so**, there are 32-bit and 64-bit versions.
- Verify that the slot label set with the `Label=…` parameter agrees with the pki_token_name attribute in the `pkispawn.conf` file.

3.8.2 Persisting Problems

For persisting or other problems, do not hesitate to contact us. Further information and contact information can be found down below.

4 Further Information

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

All of the Utimaco CryptoServer documentation is also available at the Utimaco IS GmbH support website: https://hsm.utimaco.com/services/support

5 Technical Support

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.