

SSH Communications Security Universal SSH Key Manager

Integration Guide

CryptoServer HSM



Imprint

Copyright 2026	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	1.0.0
Date	2026-08-12
Status	PUBLISHED
Document No.	IG-2025-0010
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	Introduction	5
2	CryptoServer HSM	6
3	Requirements.....	7
3.1	Utimaco CryptoServer HSM.....	7
3.2	PKCS#11 R2	7
3.2.1	Setting up the environment.....	7
3.2.2	Module configuration	7
3.2.3	Token creation.....	8
4	Configuration	9
4.1	Adding the Utimaco PKCS#11 library.....	9
5	Troubleshooting	12
5.1	Connection Problems	12
5.2	General advice.....	12
5.3	Common misconfigurations	12
5.4	Persisting Problems	12
6	Further Information	13

Partner Name	SSH Communications Security
Product Name	Universal SSH Key Manager
Partner v[Version]	
Document Type	Integration Guide
Utimaco Product	CryptoServer HSM
Utimaco v[Version]	
Document Image	
Document Number	IG-2025-0010
Document Version	1.0.0
Status	PUBLISHED

1 Introduction

This document will guide you through the integration of a Utimaco CryptoServer (HSM, hardware security module) into the SSH Communications Security Universal SSH Key Manager (UKM) as a PKCS#11 module. This guide is targeted at version 1.7 of the SSH UKM Appliance for Red Hat & CentOS operating systems.

For guidance on the base installation and configuration of the SSH UKM Appliance, please see the "Universal SSH Key Manager (tm) 1.7.x Installation Manual (Red Hat & CentOS)" PDF supplied with the appliance. The integration steps below assume at least a basic knowledge of the web interface for the server frontend.

This guide was written based on version 1.7.1 of the Universal SSH Key Manager.

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 guides available.

2 CryptoServer HSM

This integration uses the SecurityServer-V4.01.x product CD. Note that this is a quick guide which should be used in conjunction with Utimaco's PKCS#11 manual. Utimaco's PKCS#11 documentation can be found on the product CD: <utimaco folder>/Documentation/ Crypto_APIs/ PKCS_11_R2/ .

On the SSH Universal Key Manager appliance, create the directory /opt/cs/pkcs11_r2 or as appropriate. This guide uses that path for simplicity.

3 Requirements

3.1 Utimaco CryptoServer HSM

This integration uses the SecurityServer-V4.01.x product CD. Note that this is a quick guide which should be used in conjunction with Utimaco's PKCS#11 manual. Utimaco's PKCS#11 documentation can be found on the product CD: `<utimaco folder>/Documentation/Crypto_APIs/PKCS_11_R2/`.

On the SSH Universal Key Manager appliance, create the directory `/opt/cs/pkcs11_r2` or as appropriate. This guide uses that path for simplicity.

3.2 PKCS#11 R2

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

`cs_pkcs11_R2.cfg` serves as a configuration file for the PKCS#11_R2 shared object library. Use `scp` to copy these two files from the installation media to the appliance, placing them into `/opt/cs/pkcs11_r2`.

3.2.1 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:

`>_Console`

```
# export CS_PKCS11_R2_CFG=/opt/cs/pkcs11_r2/cs_pkcs11_R2.cfg
```

3.2.2 Module configuration

To establish a connection with your HSM you need to edit the configuration file. It is highly recommended to take a look at Utimaco's manual to adapt the PKCS#11 module to fit your needs. Depending on the device you are using (PCI/CSLAN/Simulator) you need to adjust the Device Specifier.

You will need to edit the configuration file so that the active `[CryptoServer] Device = 288@<ipaddr>` line points at the remote HSM or cluster that you are targeting. Also consider setting the SlotCount to 1. Further configuration options are available, see the PKCS#11 Administrator manual in the Documentation folder referenced above.

3.2.3 Token creation

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 `<utimaco folder>/Software/Crypto_APIS/PKCS#11_R2/doc/`. The hands-on guide describes setting up a Security Officer and slot PIN.

You can use `p11tool2` or `p11cat` (the PKCS#11 CryptoServer Administration Tool) to do so. See the provided documentation for details on how to manage the PKCS#11 API.

4 Configuration

4.1

Adding the Utimaco PKCS#11 library

Please see the Utimaco documentation for use and deployment of the PKCS#11 R2 Configuration file, pointed to by the environment variable CS_PKCS11_R2_CFG. The SSH UKM appliance will attach to a single PKCS#11 implementation at a time, whether this is one or more physical HSMs will depend on the CS_PKCS11_R2_CFG file.

Log in to the Universal SSH Key Manager appliance, at the web address <https://<ipaddress>/appliance/#/login>. The Username and Password are the default account username and password (that you would use if you were using ssh to log in to the appliance).

ssh communications security

UNIVERSAL SSH KEY MANAGER APPLIANCE TM 1.71-1569

Please sign in

Username

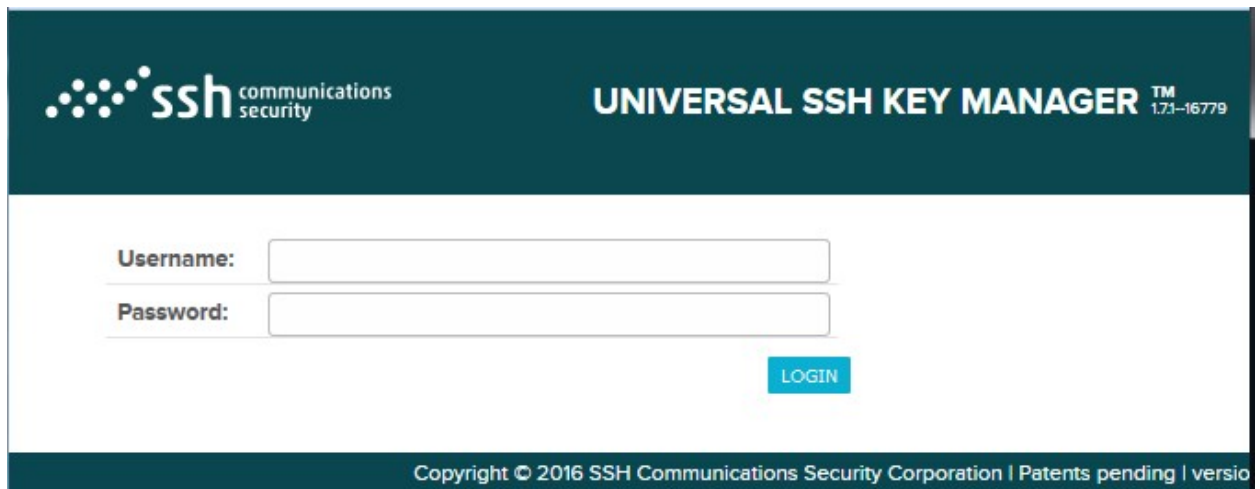
Password

Sign in

Copyright © 2016 SSH Communications Security Corporation | Patents pending | Version 1.71 (1569)

Figure 1: appl sign in

Use the "Frontend" link to log into the Key Manager. The default user is called 'superuser', and will use the password you set up for it during the appliance installation.



The screenshot shows the login interface of the Universal SSH Key Manager. At the top, there is a dark teal header with the 'ssh communications security' logo on the left and the text 'UNIVERSAL SSH KEY MANAGER' with a trademark symbol and the number '1.7.1-16779' on the right. Below the header, the main content area is white and contains two input fields: 'Username:' and 'Password:'. To the right of the 'Password:' field is a blue 'LOGIN' button. At the bottom of the page, a dark teal footer contains the text 'Copyright © 2016 SSH Communications Security Corporation | Patents pending | versio'.

Figure 2: keym sign in

Click on any javascript-generated panels to dismiss them. Click on the SETTINGS tab, and then the GENERAL sub-tab.

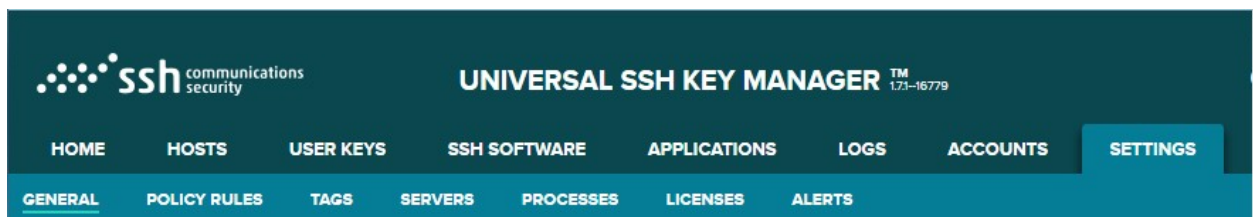


Figure 3: setts genrl

Click on HSM to get to the PKCS#11 Dialog.

GENERAL **POLICY RULES** **TAGS** **SERVERS** **PROCESSES** **LICENSES** **ALERTS**

Global settings / HSM

Categories

- [Host](#)
- [Backend](#)
- [Global](#)
- [Authentication](#)
- [E-mail server](#)
- [Frontend](#)
- [Host credentials](#)
- HSM**

Path to PKCS11 library

PIN code

Confirm pin code

Default PKCS11 key fingerprint

APPLY Restored

Figure 4: pkcs11 setup

Enter the filename of the Utimaco PKCS#11 R2 implementation in the "Path to" entry, and enter the PIN value for Slot 0 (twice).

GENERAL **POLICY RULES** **TAGS** **SERVERS** **PROCESSES** **LICENSES** **ALERTS**

Global settings / HSM

Categories

- [Host](#)
- [Backend](#)
- [Global](#)
- [Authentication](#)
- [E-mail server](#)
- [Frontend](#)
- [Host credentials](#)
- HSM**

Path to PKCS11 library

PIN code

Confirm pin code

Default PKCS11 key fingerprint

APPLY DEFAULT

Figure 5: pkcs11 setup2

When 'Apply' is clicked, the PIN values will collapse, and the "Default PKCS11 key fingerprint" drop-down will auto-populate with any visible Private keys found on Slot 0 of the Utimaco CryptoServer cluster. Select the correct key to click 'APPLY' to set it as the Default key.

5 Troubleshooting

5.1 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
```

- Verify that you are using the right libcs_pkcs11_R2.so, there is a 32-bit and a 64-bit version

5.2 General advice

5.3 Common misconfigurations

5.4 Persisting Problems

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

6 Further Information

This document will guide you through the integration of a Utimaco CryptoServer (HSM, hardware security module) into the SSH Communications Security Universal SSH Key Manager (UKM) as a PKCS#11 module. This guide is targeted at version 1.7 of the SSH UKM Appliance for Red Hat & CentOS operating systems.

For guidance on the base installation and configuration of the SSH UKM Appliance, please see the "Universal SSH Key Manager (tm) 1.7.x Installation Manual (Red Hat & CentOS)" PDF supplied with the appliance. The integration steps below assume at least a basic knowledge of the web interface for the server frontend.

This guide was written based on version 1.7.1 of the Universal SSH Key Manager.

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 guides available.