IDnomic

OpenTrust PKI

4.8.0

Integration Guide

CryptoServer HSM

3.10.3

utimaco®

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	2026-07-20
Status	PUBLISHED
Document No.	IG-2026-0075

Table of Contents

1 Introduction 4
1.1 Concepts 4
2 Requirements 5
2.1 Supported Operating Systems 5
3 Procedures 6
3.1 Install SafeGuard CryptoServer Hardware 6
3.2 Install SafeGuard SecurityServer Software 6
3.3 Configure PKCS#11 R2 6
3.3.1 PKCS#11 R2 Slot Initialization 8
3.4 Set Up OpenTrust PKI 8
3.4.1 Integrate OpenTrust PKI with a SafeGuard CryptoServer 9
3.4.2 Certification Authority Creation 10
4 Further Information 12
4.1 References 12
5 Contact and Support Information 13

1 Introduction

This paper provides an integration guide explaining how to integrate a Hardware Security Module (HSM) -- SafeGuard® CryptoServer with OpenTrust PKI on a Linux operating system platform.

1.1 Concepts

OpenTrust PKI is an open, modular and highly scalable solution designed to address more advanced security solutions to combat high level risks. This innovative and market-proven solution is one of OpenTrust's core products for building a trusted ecosystem. OpenTrust PKI creates, issues and manages the digital identities of users or devices within a Public Key Infrastructure. It oversees the complete credential management for Public Key certificates in IT infrastructures, encompassing any kind of smart card or token that embeds an X.509 certificate and a key pair.

The modular architecture of OpenTrust PKI allows support for singular or multiple applications, management of certificates and keys locally or centrally, and can be implemented within a centralized or decentralized architecture. In its basic and lighter structural design, the public-key operations (PKO) centre forms an integral component of OpenTrust PKI. OpenTrust PKI supports full local or centralized certificate and key life cycle management for all entities (such as users, devices and applications) and multiple CAs for singular or multiple applications.

The SafeGuard® CryptoServer is a hardware security module developed by Utimaco IS, i.e. a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data. In a SafeGuard® CryptoServer security system security relevant actions can be executed, and security relevant information can be stored. It can be used as a universal, independent security component for heterogeneous computer systems.

2 Requirements

Ensure that you have a copy of the *CryptoServer Administration Guide* and the *CryptoServer PKCS#11 Interface*. You should also have prepared an installed Linux operating system (CentOS 6). If you are using PCI(e) card, you must also compile and install the necessary driver for that card.

HSM Model	SafeGuard® CryptoServer CS-Series/S-Series/Se-Series
HSM Firmware	SafeGuard® CryptoServer 3.10.3
Software	SafeGuard® CryptoServer 3.10.3 OpenTrust PKI 4.8.0 PKCS11 API >= 2.10

Table 1: Software and hardware requirements

2.1 Supported Operating Systems

The interoperability of the SafeGuard® CryptoServer solution, an operating system and the OpenTrust PKI have been tested successfully for the following combinations:

Operating System	SafeGuard® CryptoServer Version	OpenTrust Version	PKI	PCI Support	Ethernet Support
CentOS 6 x86/64	3.10.3	4.8.0		Yes	Yes

Table 2: Tested versions

3 Procedures

To integrate the SafeGuard® CryptoServer with OpenTrust PKI and verify the functionality, complete the following steps:

1. Install SafeGuard® CryptoServer hardware.
2. Install SafeGuard® CryptoServer software.
3. Configure PKCS#11 R2.
4. Set up OpenTrust PKI.

3.1 Install SafeGuard CryptoServer Hardware

For more information on commonly installing and setting up SafeGuard® CryptoServer PCI(e) / LAN, see the documentation *SafeGuard® CryptoServer PCI(e) / LAN Operating and Installation Manual* [1] [2].

There is no need to install any specific software for running SafeGuard® CryptoServer. The SafeGuard® CryptoServer comes with an already preinstalled set of firmware software.

3.2 Install SafeGuard SecurityServer Software

The SafeGuard SecurityServersoftware - this includes administrative and library software - has to be installed on your computer system manually. To install the necessary PKCS#11 R2 libraries it is referred to the *SafeGuard® CryptoServer PKCS#11 R2 Manual*[3]. Further configuration steps are explained next.

3.3 Configure PKCS#11 R2

The PKCS#11 R2 library and configuration files for Linux operating system must be installed manually. Here are some of the basic steps to install and configure PKCS#11 R2.

- Make a directory, mount the installation media (CDROM, USB) and copy files from the installation media to the server.

```
# mkdir /mnt/usb OR mkdir /mnt/cdrom

# mount /dev/sdb1 /mnt/usb  for usb mouting

# mount /dev/sr0 /mnt/cdrom for CDROM mounting

# cp /mnt/usb/SG_SecurityServer-V3.10.3/Software/Linux/x86-64/Crypto_APIs/
PKCS11_R2 '

/lib/libcs_pkcs11_R2.so /usr/local/lib64/

# cp /mnt/usb/SG_SecurityServer-V3.10.3/Software/Linux/x86-64/Crypto_APIs/
PKCS11_R2 '

/bin/p11tool2 /usr/local/bin/

# chmod +x /usr/local/lib64/libcs_pkcs11_R2.so /usr/local/bin/p11tool2
```

- Create HSMs configuration file (edit a version taken from the installation media):

```
# mkdir /etc/utimaco

# cp SG_SecurityServer-V3.10.3/Software/Linux/x86-64/Crypto_APIs/PKCS11_R2 '

/sample/cs_pkcs11_R2.cfg /etc/utimaco/

# chmod +x /etc/utimaco/cs_pkcs11_R2.cfg
```

- Edit the CryptoServer section to specify the device or the network address/port of the HSMs, e.g. for a simulator running on a PC at the 127.0.0.1 address.

```
[CryptoServer]

# Device specifier (here: CryptoServer is CSLAN with IP address 192.168.0.1)

Device = 3001@127.0.0.1

Check the connectivity with the HSM by using below command:

# /usr/local/bin/p11tool2 GetTokenInfo
```

For more information, look into the *PKCS#11 R2 Manual* [3].

3.3.1 PKCS#11 R2 Slot Initialization

We assume that you already initialized slot 0. For initializing a slot and cryptographic keys generation, you can use p11tool2 or p11cat application. We can create a key pair by using the command below, which will be used in OpenTrust PKI.

PKCS#11 R2

```
# p11tool2 LoginUser=123456 PubKeyAttr=CKA_MODULUS_BITS=2048,CKA_LABEL="PubKey"
'

PrvKeyAttr=CKA_LABEL="PrvKey" GenerateKeyPair=RSA
```

The user pin, slot number and key label will be used later in this document.

3.4 Set Up OpenTrust PKI

We assume that you have the installation CD or the installation files. In this guide, we are going to use the installation package containing the CentOS bundled OS and the OpenTrust PKI product. Follow the steps below to install the CentOS and OpenTrust PKI server application.

1. Insert the installation CD.
2. On the OpenTrust PKI CentOS installer start page, at the boot: prompt, enter: **go.** Only select an option other than **go** after consulting an assigned OpenTrust technical representative.
3. On the Keyboard Type screen, select the type of keyboard being used to run the installer and enter **OK**.
4. On the **Time Zone Selection** screen, select the time zone in which the host machine is located and enter **OK**.
5. After the **Attention!** message, use the password displayed on the screen to log in as root.
    a. At the hostname login: prompt, where hostname is the name of the server that will host the OpenTrust PKI server application, enter: **root.**
    b. At the password prompt, enter the **password**.
6. To change the password for root, enter: **passwd** and follow the prompts until a success message is received.

7. At the root directory, enter:

```
# /root/OpenTrust/opentrust-pki-install
```

8. Above command prompts a new screen. For this installer screen, you need following information to set up OpenTrust PKI server.
    a. IP addresses/subnet masks, hostnames, and the IP addresses of the DNS servers for servers that have been allocated to host the OpenTrust PKI.
    b. IP address or fully qualified DNS name used to access the NTP server or servers that will be used to synchronize the time on the host machine.
    c. IP address or fully qualified DNS name used to access the SMTP server that the OpenTrust PKI server application should use to send mail if the default Postfix mail system will not be used.
    d. Email addresses for the administrators who should receive system mail from the host machine, primarily from the cron service

More information is given in OpenTrust PKI documents which are bundled with OpenTrust PKI package (CentOS, OpenTrust PKI installer and Documentation).

9. If you set up/installed the OpenTrust PKI server correctly, now you can reach the OpenTrust PKI server application by pointing your browser at https:// dnsnameusedtoacesshostmachine.

3.4.1 Integrate OpenTrust PKI with a SafeGuard CryptoServer

OpenTrust PKI provides .rpm and .deb packages that allow the OpenTrust PKI server application to be used with SafeGuard® CryptoServer. The HSM `.rpm` or `.deb` packages must be applied after setting up the OpenTrust PKI server application and before the creation of the Certificate Authority. Install the following core RPMS which are available along with the rest of OpenTrust PKI packages:

- `opentrust-pki-otc-securityserver3`
- `opentrust-pki-engine_pkcs11`
- `opentrust-pki-libp11`

Above packages and other packages can be found in `/root/OpenTrust/RPMS` path. Note that you also must install other packages (which are available with core packages) prior to installing core packages due to packages dependencies. According to our experience with installing and configuring OpenTrust PKI, you need to download an extra package called `libtool2-ltdl-2.2.6b-3.4.x86_64.rpm`, place it with other packages and install this package prior to installing core packages.

To install packages, follow the steps below:

```
# cd /root/OpenTrust/RPMS/

# rpm -ivh package_name.rpm
```

3.4.2 Certification Authority Creation

Once you successfully installed all required packages and initialized the application modules (see *PKI_Server_Installation_and_Upgrade_Guide-4.8*), you are ready to create the Certification Authority. The Keys are created earlier which are to be declared using their label in the form presented at the Create a Certification Authority wizard. Here is the snapshot of the Certificate Authority wizard:

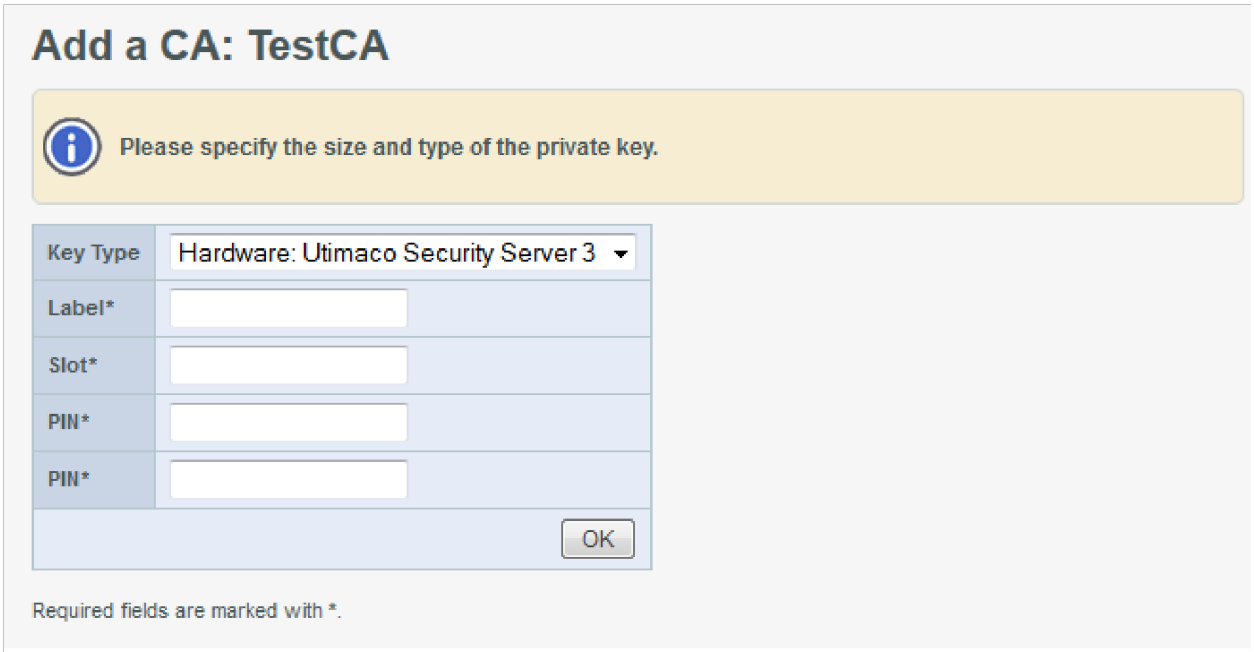

Figure 1 : Add a CA: TestCA

Once you have set up the Certificate Authority, you can use this application according to your requirements. Moreover, the certificate for CA that will be used to sign the certificates for internal modules must have been signed using the SafeGuard CryptoServer, therefore SafeGuard CryptoServer must be selected as the Key Type for at least one CA created during initialization.

4 Further Information

This document forms a part of the information and support which is provided by Utimaco IS.

Additional documentation can be found on the product CD in the documentation directory.

All SafeGuard® CryptoServer product documentation is also available at the Utimaco IS website: http://hsm.utimaco.com.

4.1 References

1. UTIMACO IS GMBH. *SafeGuard CryptoServer - LAN Operating and Installation Manual*, 2013.
2. UTIMACO IS GMBH. *SafeGuard CryptoServer - PCI Operating and Installation Manual*, 2013.
3. UTIMACO IS GMBH. *SafeGuard CryptoServer PKCS#11 (R2) Manual*, 2013.

5 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
Krefelder Str. 220
52070 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.