Xen Project Hypervisor

Xen 4.1.0 / Xen 3.2.1

Integration Guide

CryptoServer HSM

SafeGuard SecurityServer 2.30.2

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	2026-07-17
Status	PUBLISHED
Document No.	IG-2026-0069

Table of Contents

1 Introduction

This paper provides an integration guide explaining how to install a Hardware Security Module (HSM) - SafeGuard CryptoServer - within a Xen guest environment.

1.1 Concepts

Xen is a virtual-machine monitor which allows several guest operating systems to execute on the same computer hardware concurrently. In the structure of Xen systems, the Xen Hypervisor is located at the lowest and most privileged layer. Above this layer several operating systems may come, which the hypervisor schedules across the physical CPUs. The host operating system so called dom0 (domain 0) boots (using modified kernel) automatically when the hypervisor boots and receives special management privileges and direct access to all physical hardware by default. Further, the administrator can log into so called domU (U = 0, 1, 2 ...) guest operating systems. Since Xen Hypervisor runs on the hardware directly (bare-metal) unlike classical virtual machines, it is possible to pass-through the PCI slot, which SafeGuard CryptoServer is connected to, up to the guest operating system where the CryptoServer is configured. It is sufficient to install the driver on the guest operating system only.

The SafeGuard CryptoServer is a hardware security module developed by Utimaco Safeware AG, 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 are familiar with Xen installation and have a copy of the *SafeGuard CryptoServer PCI Operating and Installation Manual* [1]. This document also assumes that a Debian based Linux system has been already installed.

2.1 Software and Hardware Requirements

HSM Model	SafeGuard CryptoServer CS-Series/S-Series/Se-Series PCI(e) Smartcard reader reinerSCT cyber Jack e-com
HSM Firmware	SafeGuard SecurityServer 2.30.2
Software	SafeGuard SecurityServer 2.30.2 Xen 4.1.0 / Xen 3.2.1 Debian 5 (i386)

Table 1: Software and hardware requirements

3 Supported Operating Systems

For the interoperability of the SafeGuard CryptoServer solution, operating systems and Xen Hypervisor have been tested successfully for the following combinations:

Operating System Host	Operating System Host	Xen hypervisor	SafeGuard SecurityServer
Debian 5.0.3 (i386)	Debian 5.0.3 (i386)	3.2.1 / 4.1.0	2.30.2
Debian 5.0.3 (i386)	Microsoft Windows XP	3.2.1	2.10.2
Debian 5.0.3 (i386)	Microsoft Server 2008	3.2.1	2.10.2

Table 2: Tested versions

4 Procedures

To integrate the SafeGuard CryptoServer into a Debian based, Xen virtualized guest operating system, complete the following steps:

1. Install the SafeGuard CryptoServer hardware.
2. Install and configure Xen Hypervisor.
3. Configure, create and start the guest system (domU).
4. Install the PCI(e) driver and test the SafeGuard CryptoServer.

4.1 Install the SafeGuard CryptoServer Hardware

For more information on commonly installing and setting up SafeGuard CryptoServer PCI, see the documentation *SafeGuard CryptoServer PCI - Operating and Installation Manual* [1]. There is no need to install any software specific to running SafeGuard CryptoServer. SafeGuard CryptoServer comes with a preinstalled set of firmware software.

4.2 Install and Configure Xen Hypervisor

1. First, install the required packages:

```
# apt-get install xen-hypervisor-i386 linux-image-2.6-xen-686 \
linux-headers-2.6-xen-686 xen-tools pciutils
```

2. Now adjust the corresponding part of `/etc/inittab` to enable the serial console additionally to the VGA output:

```
1:2345:respawn:/sbin/getty 38400 hvc0
2:23:respawn:/sbin/getty 38400 tty1
```

3. Also edit the file `/etc/xen/xend-config.sxp` as follows to adjust the network configuration for Xen:

```
[...]

(network-script network-bridge) [...]

#(network-script network-dummy)

[...]

(vif-script
```

4. After the Xen installation, there should be a new entry in `/boot/grub/menu.lst` for Xen, which causes booting into the modified Xen kernel.
5. For passing through the PCI(e) slot to the quest system, which we are about to create later, it must be hidden from the host system first. List the PCI(e) devices by invoking the command `lspci`:

```
# lspci

[...]

03:07.0 Network and computing encryption device:

Quicklogic corporation Device 0006 (rev 01)

[...]
```

6. Note the number right before the description of the device, which is 03:07.0 in this case and modify the following Xen entry in `/boot/grub/menu.lst`:

```
Module /boot/vmlinuz-2.6.26-2-xen-686 root=/dev/hda1 ro console=tty0 xencons=off
pciback.hide=(03:07.0) noirqdebug
```

7. Reboot the system and check the current kernel by entering `uname r` thereafter:

```
# uname -r

2.6.26-2-xen-686
```

For more information on the Xen Hypervisor software please visit the official Xen Hypervisor web site on *Hypervisor | Xen Project*.

4.3 Configure, Create and Start the Guest System

1. First, we need to modify the default settings for virtual machines in `/etc/xen-tools/xen-tools.conf`, which in this case concerns a Debian installation. Adjust the file as follows:

```
dir = /home/xen

[...]

Memory = 512Mb Swap = 512 Mb dist = lenny Default distribution to install

[...]

dhcp = 1

[...] passwd = 1

[...] kernel = /boot/vmlinuz-`uname -r` initrd = /boot/initrd.img-`uname -r`

[...] mirror = http://ftp.de.debian.org/debian/

[...] serial_device = hvc0

[...]
disk_device = xvda
```

2. Now we can create our guest domain called `cs2-xen` e.g.:

```
# xen-create-image --hostname=cs2-xen --role=udev
```

3. While creating the guest system, you will be prompted for the root password. After providing that, add the PCI device to the guest, that we isolated from dom0 before, by adding the following line to the configuration file `/etc/xen/cs2-xen.cfg`:

```
pci=[03:07.0]
```

4. Start the guest system:

```
# xm create /etc/xen/cs2-xen.cfg
```

You can list all running virtual machines with the following command:

```
# xm list
```

5. First, log onto the guest system using the Xen console:

```
# xm console cs2-xen
```

And prepare it for SSH:

```
# apt-get install udev
```

Add the following line into `/etc/fstab`:

```
none /dev/pts devpts defaults 0 0

# mkdir /dev/pts

# mount -a
```

6. Now, find out the DHCP assigned IP address running the command `ifconfig` and log onto the guest machine using SSH:

```
# ssh <ip-of-domU>
```

7. Check if the correct PCI(e) device is passed through to the guest system:

```
# lspci

00:00.0 Network and computing encryption device:

Quicklogic corporation Device 0006 (rev 01)
```

4.4 Install the PCI(e) Driver and Test SafeGuard CryptoServer

For installing the driver for SafeGuard CryptoServer PCI, we refer to the documentation *SafeGuard CryptoServer PCI - Operating and Installation Manual* [1] respectively. Consider adjusting the path to the Xen modified headers (`linux-headers-2.6.26-2-xen-686`) in the `make.sh` located at the CryptoServerdrivers folder before running that script.

5 Further Information

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

5.1 References

[1] UTIMACO SAFEWARE AG. *SafeGuard CryptoServer PCI - Operating and Installation Manual*, 2011. M010-0003-en.

6 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.