

CryptoServer PCIe

Quick Start Guide for Linux

Document Version: 1.1.19

Product Version: 6.0.0

utimaco[®]

This document provides step-by-step instructions on how to bring the CryptoServer PCIe card into service, how to install the CryptoServer driver on a computer with minimal RHEL installation and how to start administrating your CryptoServer. It does not cover all scenarios and is intended as a supplement to the product documentation provided in the SecurityServer product bundle.

The product bundle is downloadable from the following site:

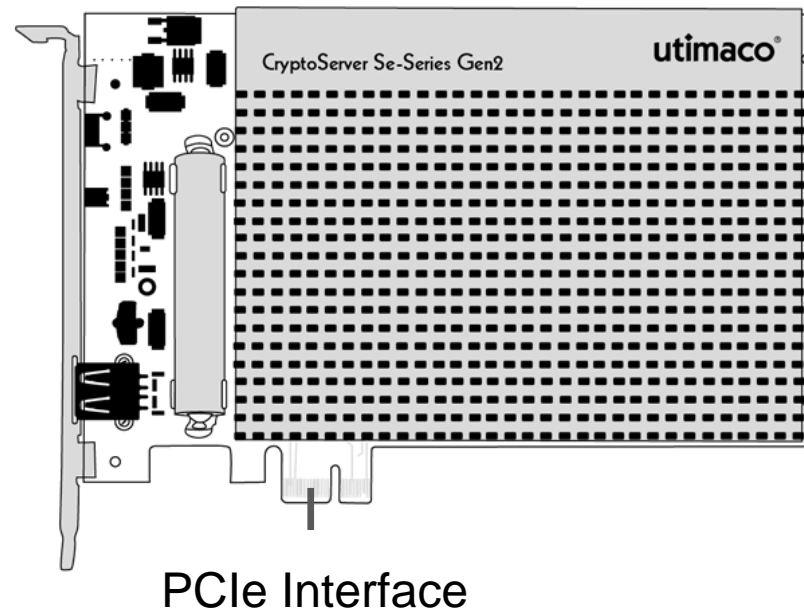
<https://support.hsm.utimaco.com/support/downloads/>

You have to be registered for this download portal and access to a download area, e.g., „SecurityServer Se Gen2“, must have been granted.

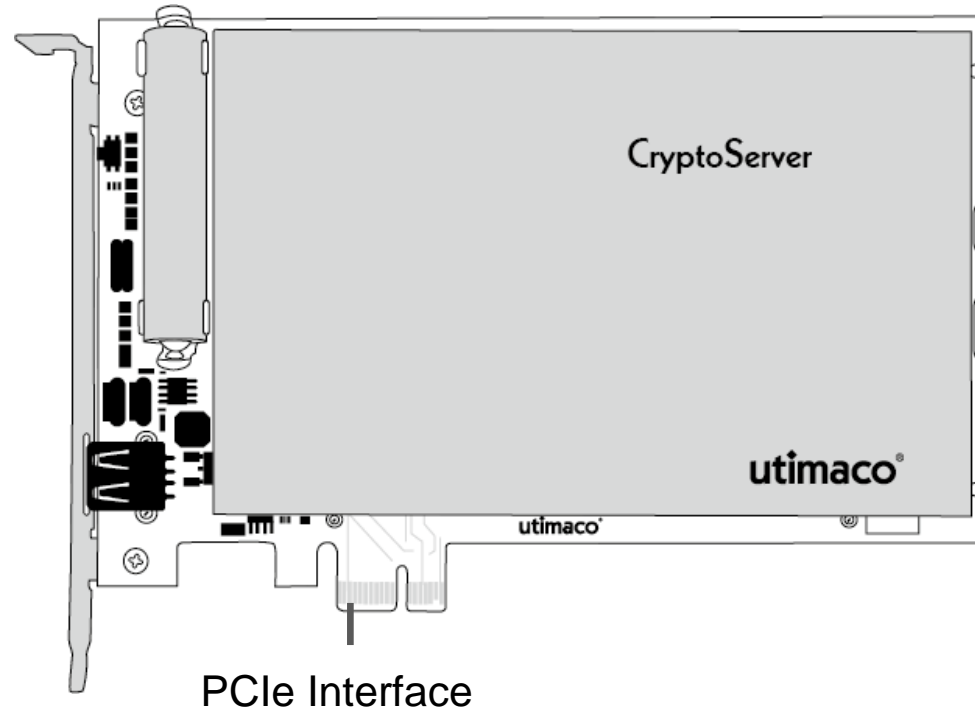
For detailed information on the full range of setup and configuration options, please read the [*CryptoServer Administration Manual*](#) and the [*CryptoServer PCIe Operating Manual CSe-Series*](#) or [*CryptoServer PCIe Operating Manual Se-Series Gen2*](#).

Before you start with the installation, read the safety instructions in the [*CryptoServer PCIe Operating Manual CSe-Series*](#) or [*CryptoServer PCIe Operating Manual Se-Series Gen2*](#) and examine the CryptoServer PCIe card for obvious signs of damage.

CryptoServer PCIe Card Se-Series Gen2



CryptoServer PCIe Card CSe-Series



Install the CryptoServer PCIe Card



Hold the CryptoServer PCIe card at its mounting plate and at the edges of the carrier board. Pressure on the encapsulated unit may damage the CryptoServer.

1. Turn off the computer and open the computer case.
2. Select the appropriate slot at the rear side of the computer:
 - CryptoServer CSe-Series/Se-Series Gen2 - a PCIe 3.0 lane compatible slot
3. Remove the corresponding slot bracket.
4. Carefully align the PCIe card with the PCIe slot of the computer and press directly down onto top middle of the Printed Circuit Board. Check to confirm that the board is properly seated before securing the mounting plate.
5. Close the computer case and turn on the computer.

Install the CryptoServer Driver (1/7)

Prerequisites

For example on a computer with a minimal RHEL 64-bit installation. See the operating manual for other Linux distributions.

- Source code of the CryptoServer driver or full CryptoServer product bundle
- The following packages are required: `kernel-devel`, `gcc.x86_64` and `make`
- root privileges are required.

Install the CryptoServer Driver (2/7)

Perform the following installation steps:

1. Check hardware: `lspci -d '*:c071'` and then look for `168a:c071`

2. Check OS/driver

Check if you are running in UEFI or in legacy (BIOS) mode:

```
ls /sys/firmware/efi
```

If `/sys/firmware/efi` exists, that means the system uses UEFI.

Check if SecureBoot is enabled:

```
mokutil --sb-state
```

If the output shows both UEFI and SecureBoot, the driver will only work if you are running Ubuntu 18 or higher. In all other cases, you will have to disable SecureBoot in your BIOS.

Install the CryptoServer Driver (3/7)

Perform the following installation steps:

3. Build and install the Driver under RHEL.

You find the source code files of the driver on the product CD in the `Software/Linux/Driver` directory.

Run the following command, adjusting the version number as necessary, to build and install the kernel module. The module will also be rebuilt on kernel updates (using DKMS):

```
sudo yum install ./cryptoserver-dkms-5.18.0-Linux.rpm  
kernel-devel
```

On the RHEL, the package will only work if you have the EPEL repository enabled. A check can be done using `yum repolist`.

The package installation will not automatically sign the module for SecureBoot, so SecureBoot needs to be disabled.

Install the CryptoServer Driver (4/7)

Perform the following installation steps:

4. Configure the driver.

By default, the driver will not enable the cHSM slots, nor the network interface. To do so, set up a `modprobe` configuration file to set `DeviceMask` and `DeviceFlags`, e.g.

```
/etc/modprobe.d/cryptoserver.conf
```

```
options cryptoserver DeviceMask=0xFFFFFFFF DeviceFlags=2
```

Reload the driver to let the changes take effect:

```
$ sudo rmmod cryptoserver
```

```
$ sudo modprobe cryptoserver
```

The '`$ sudo rmmod cryptoserver`' command may fail if the driver was not loaded.

Install the CryptoServer Driver (5/7)

Perform the following steps to verify the installation:

5. Copy the CryptoServer Administration Tool csadm from the product bundle to your local disk.

```
cp <Path to product  
bundle>/Software/Linux/Administration/csadm .
```

6. Make the csadm file executable.

```
chmod u+x csadm
```

7. Verify the connection to the CryptoServer.

```
csadm Dev=/dev/cs2.0 GetState
```

The 0 in cs2.0 indicates that you try to connect to the first found CryptoServer PCIe card.

Install the CryptoServer Driver (6/7)

Perform the following steps to verify the installation (continued):

8. Output example:

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 36.1 [C]
alarm     = OFF
bl_ver    = 5.00.0.5           (Model: Se-Series Gen2)
uid       = 6e000018 850bbe01 |          =*
adm1      = 53653530 20202020 43533434 34383739 | Se1500      CS600024
adm2      = 53656375 72697479 53657276 65720000 | SecurityServer
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

9. Make sure that the CryptoServer is in Operational Mode and no alarm has been triggered.

```
mode      = Operational Mode
...
alarm     = OFF
```

Install the CryptoServer Driver (7/7)

If there are problems to produce an output similar to the one above, perform the following steps:

10. Verify that the kernel module is running.

```
lsmod | grep cryptoserver
```

11. Verify that the device node has been created.

```
ls /dev/cs2.0
```

12. Verify for error messages from the driver.

```
dmesg | grep :cs
```

1. Generate a new authentication token (e.g. a protected keyfile):

```
csadm GenKey=<filepath\filename>,<keylength>,<key_owner>
```

Example:

```
csadm GenKey=/root/keys/rsa_key.key,2048,CryptoServer_Admin
```

2. Change the authentication token for the standard administrator ADMIN:

```
csadm Dev=<device> <Authentication> ChangeUser=<user>,<new_token>
```

Example:

```
csadm Dev=/dev/cs2.0 LogonSign=ADMIN,<...>/Software/Linux/Administration/key/ADMIN.key
```

```
ChangeUser=ADMIN,/root/keys/rsa_key.key
```

3. Generate a Master Backup Key (MBK) for the CryptoServer.



An MBK is a 32-byte AES key generated in an m-out-of-n scheme used for backup, encryption of external key storage or synchronization of HSMs in a cluster.

```
csadm Dev=<device> <Authentication> Key=<keyspec>  
MBKGenerateKey=<keytype>,<keylength>[<n>,<m>,<keyname>]
```

Example:

```
csadm Dev=/dev/cs2.0  
LogonSign=ADMIN,/root/keys/rsa_key.key#ask  
Key=/root/keys/mbk1.key#ask,/root/keys/mbk2.key#ask,/root/keys  
/mbk3.key#ask MBKGenerateKey=AES,32,3,2,DemoMBK
```

4. Import the MBK into the CryptoServer.

```
csadm Dev=/dev/cs2.0 <Authentication> Key=<keyspec> MBKImportKey=<slot_no>
```

Example:

```
csadm Dev=/dev/cs2.0 LogonSign=ADMIN,/root/keys/rsa_key.key#ask  
Key=/root/keys/mbk1.key#ask,/root/keys/mbk2.key#ask MBKImportKey=3
```

5. Check that the MBK is available in your CryptoServer.

```
csadm Dev=/dev/cs2.0 <Authentication> MBKListKeys
```

Example output:

slot	name	len	algo	type	k	generation	date	key	check	value

3	DemoMBK	32	AES	SHARE	2	2007/08/06	10:35:50	106B5E4E84031BDE		
								:95B959285F0C113C		

After you have finished performing the steps described in this document your CryptoServer is prepared to be fully integrated into your system infrastructure and to get operational.

Please find detailed information on the full range of setup and configuration options, as well as information about possible integration scenarios in the SecurityServer product bundle in the `Documentation` directory.


Recommendations for further reading:

[*CryptoServer Administration Manual*](#)

[*CryptoServer csadm Manual*](#)

[*CryptoServer PCIe Operating Manual CSe-Series*](#)

[*CryptoServer PCIe Operating Manual Se-Series Gen2*](#)



Utimaco IS GmbH
Germanusstr. 4
D-52080 Aachen, Germany
AMERICAS: +1-844-UTIMACO (+1 844-884-6226)
EMEA: +49 800-627-3081
APAC: +81 800-919-1301
<https://support.hsm.utimaco.com>
support@utimaco.com

Document number: M014-0002-en

Copyright © 2024 – Utimaco IS GmbH

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.