

CryptoServer PCIe

Quick Start Guide

Version 1.1.1

utimaco[®]

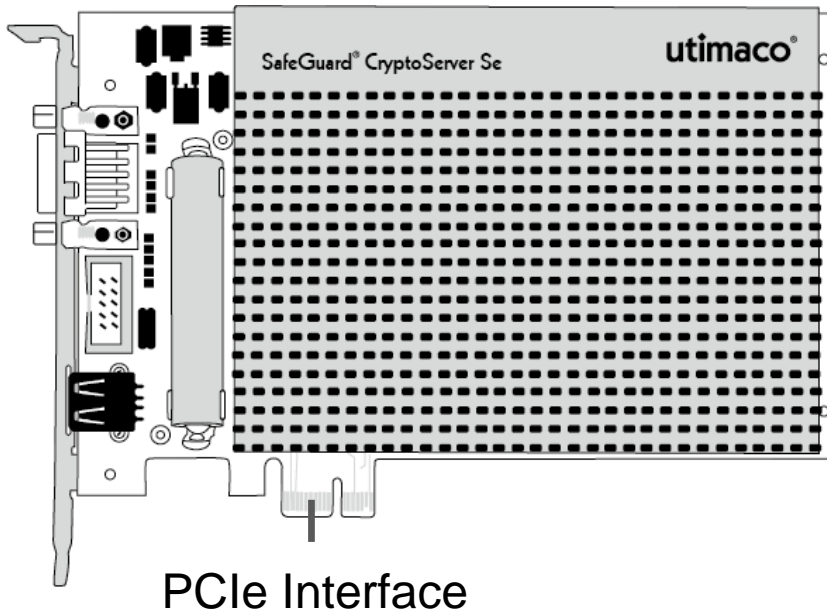
This document provides step-by-step instructions on how to bring the CryptoServer PCIe plug-in card into service, how to install the CryptoServer driver on a computer with minimal RHEL 7.0 installation and how to start administrating your CryptoServer. It doesn't cover all scenarios and is intended as a supplement to the product documentation provided on the SecurityServer product CD.

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

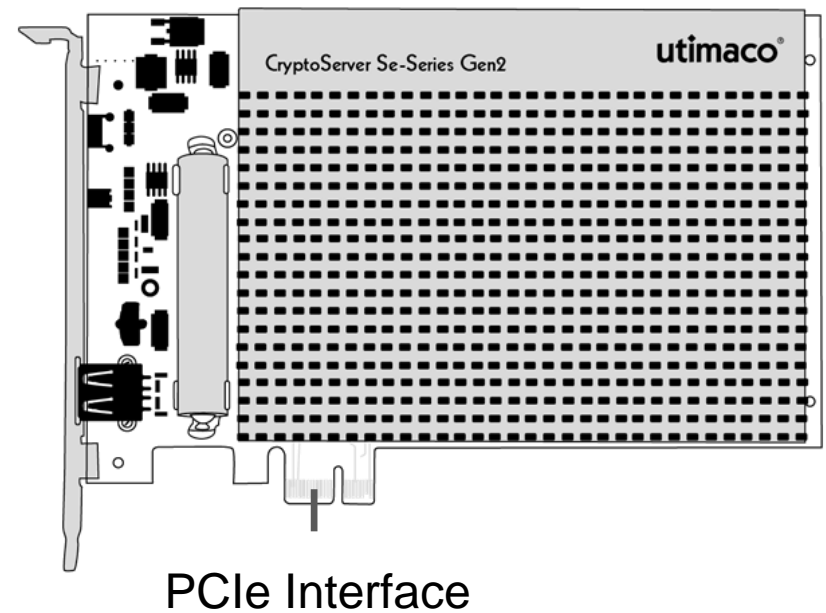
Before you start with the installation, read the safety instructions in the [CryptoServer PCIe Operating Manual CSe-Series](#), [CryptoServer PCIe Operating Manual Se-Series Gen2](#) or [CryptoServer PCIe Operating Manual Se-Series](#) and examine the CryptoServer PCIe plug-in card for obvious signs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

CryptoServer PCIe Plug-in Card Se-Series/Se-Series Gen2

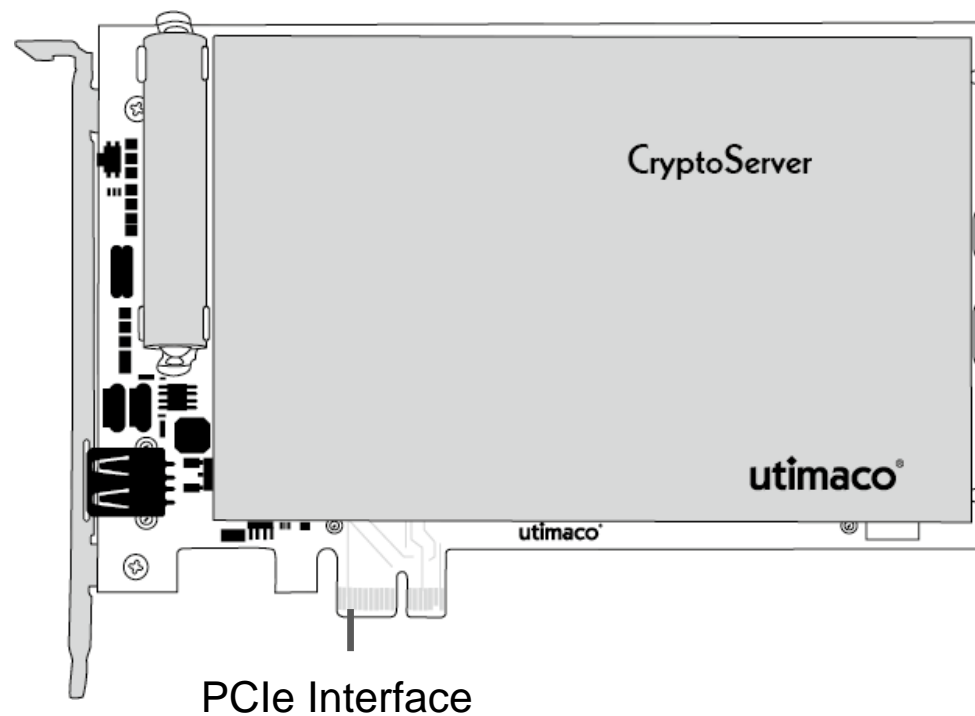
Se-Series



Se-Series Gen2



CryptoServer PCIe Plug-in Card CSe-Series



Install the CryptoServer PCI Plug-in Card



Hold the CryptoServer PCIe plug-in 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 Se-Series - a PCIe 1.1 lane compatible slot
 - 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 the board is properly seated before securing the mounting plate.
5. Close the computer case and turn on the computer.

Install the CryptoServer Driver (1/3)

For example on a computer with minimal RHEL 7.0 x64 installation.
Root privileges are required.

1. Install required additional packages

```
yum install kernel-devel  
yum install gcc.x86_64
```

2. Copy the CryptoServer driver directory from the product CD
.../Product CD/Software/Linux/Driver/ to a local directory.

3. Locate the directory containing the kernel source.

```
ls -la /usr/src/kernels/
```

4. Edit the `make.sh` script (e.g. with the `vi` editor)

```
KERNEL_SOURCE=/usr/src/kernels/<kernel source name>
```

Install the CryptoServer Driver (2/3)

5. Execute the `make.sh` script:

```
./make.sh
```

The kernel object `cs2.ko` is generated.

6. Copy `cs2.ko` to your module tree:

```
cp cs2.ko /lib/modules/<kernel source name>/kernel/drivers/pci
```

7. Check for dependencies between kernel modules:

```
depmod -a
```

8. Create the device node and set the needed file permissions:

```
mknod /dev/cs2 c 244 0
```

```
modprobe cs2
```

Install the CryptoServer Driver (3/3)

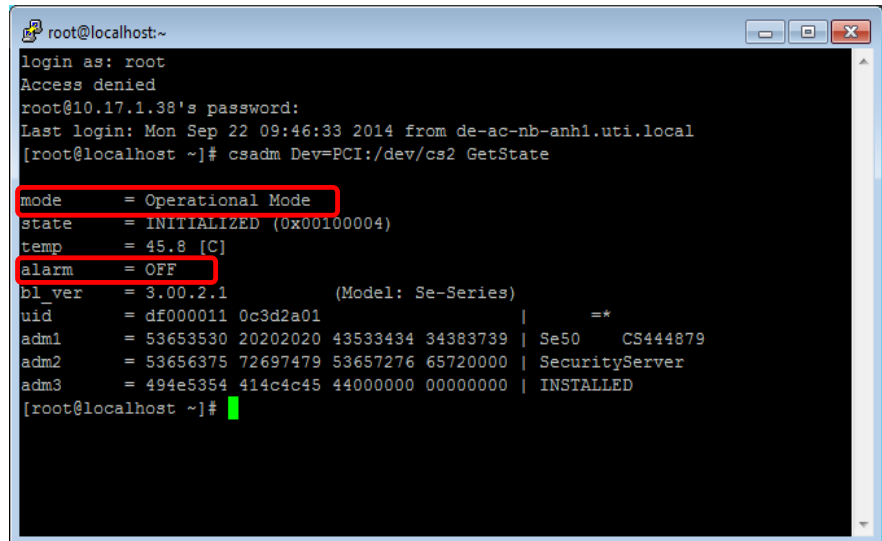
9. Copy the CryptoServer Administration Tool csadm from the product CD
...Product CD/Software/Linux/x86-64/Administration to
your bin directory, e.g.:

```
cp <...>/Software/Linux/Driver/csadm
```

10. Check the connection to CryptoServer:

```
csadm Dev=PCI:/dev/cs2 GetState
```

Make sure the CryptoServer is in
Operational Mode
(mode = Operational Mode)
and no alarm is triggered
(alarm = OFF).



```
root@localhost:~  
login as: root  
Access denied  
root@10.17.1.38's password:  
Last login: Mon Sep 22 09:46:33 2014 from de-ac-nb-anh1.uti.local  
[root@localhost ~]# csadm Dev=PCI:/dev/cs2 GetState  
mode      = Operational Mode  
state     = INITIALIZED (0x00100004)  
temp      = 45.8 [C]  
alarm     = OFF  
bl_ver    = 3.00.2.1          (Model: Se-Series)  
uid       = df000011 0c3d2a01 |      =*  
adm1      = 53653530 20202020 43533434 34383739 | Se50   CS444879  
adm2      = 53656375 72697479 53657276 65720000 | SecurityServer  
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED  
[root@localhost ~]#
```


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

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

Example:

```
csadm NewPassword=ask 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=PCI:/dev/cs2
```

```
LogonSign=ADMIN,<...>/Software/All_Supported_Operating_Systems/Administration/keys/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=PCI:/dev/cs2  
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.

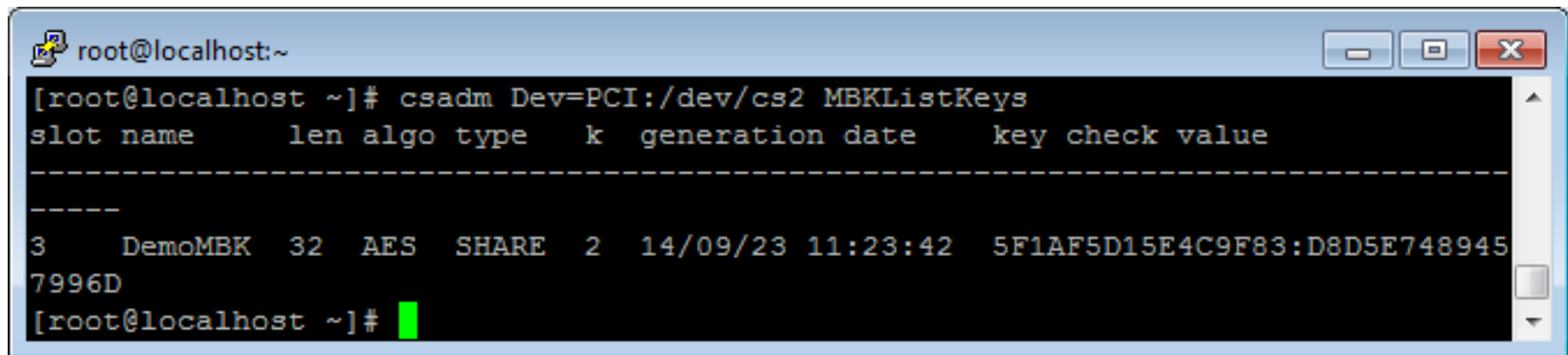
```
csadm Dev=PCI:/dev/cs2 <Authentication> Key=<keyspec> MBKImportKey=<slot_no>
```

Example:

```
csadm Dev=PCI:/dev/cs2 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=PCI:/dev/cs2 MBKListKeys
```



```
root@localhost:~  
[root@localhost ~]# csadm Dev=PCI:/dev/cs2 MBKListKeys  
slot name      len algo type    k  generation date    key check value  
-----  
3      DemoMBK  32  AES  SHARE  2   14/09/23 11:23:42  5F1AF5D15E4C9F83:D8D5E748945  
7996D  
[root@localhost ~]#
```

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 on the SecurityServer product CD in the `Documentation` directory. Recommendations for further reading:

[CryptoServer Manual for System Administrators](#)

[CryptoServer csadm Manual for System Administrators](#)

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

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

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



Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Germany

Tel +49 241 1696 200

Fax +49 241 1696 199

Email hsm@utimaco.com

Document number: M014-0002-en

Copyright © 2016 – 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.