

# CryptoServer PCIe

Quick Start Guide for Windows



## Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet e-mail	<a href="https://support.hsm.utimaco.com/">https://support.hsm.utimaco.com/</a> <a href="mailto:support@utimaco.com">support@utimaco.com</a>
Document Version	1.0.14
Product Version	6.0.0
Date	2024-10-24
Document No.	2020-0039
Status	<b>PUBLISHED</b>

All rights reserved	<p>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.</p> <p>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. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>
---------------------	--

# Table of Contents

<b>1</b>	<b>Introduction to CryptoServer .....</b>	<b>4</b>
<b>2</b>	<b>Getting to Know .....</b>	<b>5</b>
2.1	CryptoServer PCIe Card Se-Series Gen2.....	5
2.2	CryptoServer PCIe Card CSe-Series.....	5
<b>3</b>	<b>Getting Started .....</b>	<b>6</b>
3.1	Installing the CryptoServer PCIe Card .....	6
3.2	Installing the CryptoServer Driver.....	6
3.2.1	Verify the installation .....	7
3.2.2	If you have problems producing an output like the one above, try the following: .....	8
<b>4</b>	<b>Initial Administration Steps .....</b>	<b>9</b>
<b>5</b>	<b>Further Reading.....</b>	<b>11</b>

# 1 Introduction to CryptoServer

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 64-bit Windows 10 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/>



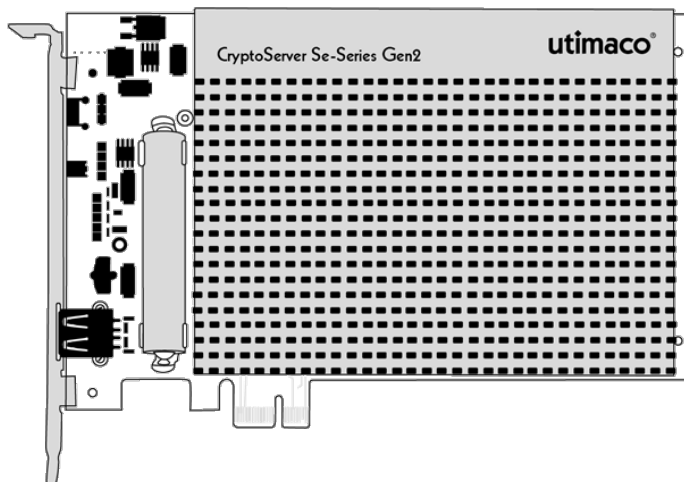
You have to be registered for this download portal and access to a download area, e.g., „SecurityServer Se Gen2“, must have been granted.

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.

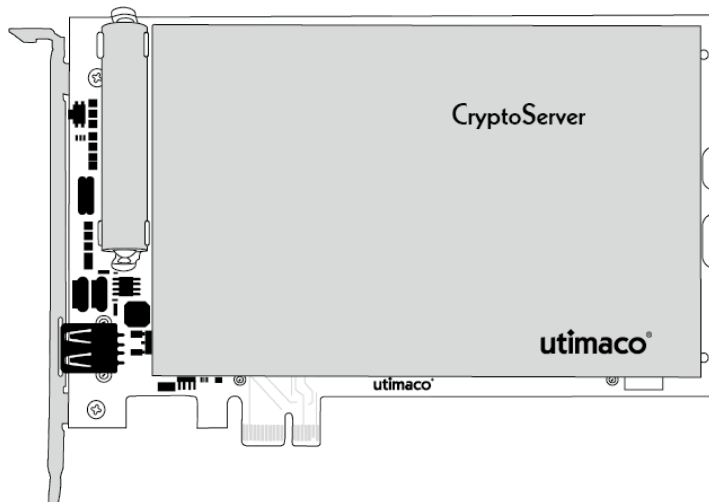
Before you start with the installation, read the safety instructions in the CryptoServer PCIe Operating Manual CSe-Series or CryptoServer PCIe Operating Manual Se-Series Gen2 and examine the CryptoServer PCIe card for obvious signs of damage.

## 2 Getting to Know

### 2.1 CryptoServer PCIe Card Se-Series Gen2



### 2.2 CryptoServer PCIe Card CSe-Series



## 3 Getting Started

### 3.1 Installing 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 the 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

### 3.2 Installing the CryptoServer Driver

#### Prerequisites:

For example on a computer with a 64-bit Windows 10 installation.

To install or upgrade the CryptoServer driver, you need the following files. For Windows 10 64-bit you can find them on the product CD in `Software\Windows\Driver\bin.`

- `CryptoServer.sys` (driver program)
- `CryptoServer.inf` (installation script)
- `cryptoserver.cat` (catalog file)

Do the following:

1. Insert the product CD into the CD/DVD drive of the computer.
2. Open the **Run** dialog by pressing the Windows key and the R key.
3. Enter `devmgmt.msc` into and select **OK**. The Windows **Device Manager** opens.
4. Double-click **Network and Computing Encryption/Decryption Controller** under **Other devices**.
5. Click **Update driver**.
6. Click **Browse my computer for driver software**.
7. Click **Browse**.
8. Click **OK**.
9. Click **Next**. The driver installation starts.
10. Click **Install this driver software anyway** or **Install**.
11. You will see a message that the driver has been installed successfully.
12. Click **Close**.
13. Open the Windows **Device Manager**.



The CryptoServer Se-Series Gen2 appears as the **CryptoServer Se-Series Gen2** device under **Cryptographic Devices**.

### 3.2.1 Verify the installation

1. Select **Run** from the Windows **Start** menu.
2. Enter `cmd`.
3. Click **OK** to open the command line window.
4. Enter the following command sequence to start the csadm administration tool from the product CD to determine the status of the CryptoServer Se Gen2. This assumes that the CryptoServer PCIe card is in the first slot.

```
D:
cd Software\Windows\Administration
set CRYPTOSERVER=PCI:0
csadm GetState
```

5. Output example:

```
mode = Operational Mode
state = INITIALIZED (0x00100004)
temp = 36.1 [C]
alarm = OFF
bl_ver = 5.00.5.5 (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
```

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

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

### 3.2.2 If you have problems producing an output like the one above, try the following:

1. If you cannot communicate with the CryptoServer Se-Series Gen2, check that the PCIe card has been mounted correctly. Also check in Windows Device Manager whether the driver has been installed correctly. Then repeat the functional test.
2. If you still cannot communicate with the CryptoServer Se-Series Gen2, contact either the reseller who supplied this CryptoServer Se-Series Gen2 or the Utimaco IS GmbH Customer Service team.
3. If you use several CryptoServer PCIe cards or the card is in a different slot, replace `PCI:0` in the above command sequence by `PCI:1` or `PCI:2` etc. for each additional card and perform this command sequence again.



## 4 Initial Administration Steps

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=PCI:0 LogonSign=ADMIN,<...>/Software/Windows/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=PCI: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=PCI:0 <Authentication> Key=<keyspec> MBKImportKey=<slot_no>
```

Example:

```
csadm Dev=PCI: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=PCI:0 <Authentication> MBKListKeys
```

Example:

```
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
```

## 5 Further Reading

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 Administration Manual
- CryptoServer csadm Manual
- CryptoServer CAT Manual
- CryptoServer PCIe Operating Manual CSe-Series
- CryptoServer PCIe Operating Manual Se-Series Gen2