

CryptoServer PCIe

Se-Series Gen2

Operating Manual

utimaco[®]

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	https://support.hsm.utimaco.com
Email	support@utimaco.com
Document version	1.2.17
Date	2024-10-24
Status	Final
Document No.	M015-0001-en
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.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>

Table of Contents

1	Introduction	5
1.1	About this Manual	5
1.1.1	Target Audience for this Manual	5
1.1.2	Contents of this Manual	5
1.1.3	Document Conventions	5
1.2	Other Manuals	6
1.3	Import and Export Regulations.....	8
1.4	Damage in Transit	8
1.5	Deliverables	8
2	General Safety Advice	9
2.1	Moving and Storing	9
2.2	Battery	10
2.3	Safely Transporting the CryptoServer	10
2.4	Environmental Temperature.....	12
3	Components of CryptoServer Se Gen2 (PCIe)	14
4	Unpacking and Handling.....	15
4.1	General Notes	16
4.2	Installing the CryptoServer Se Gen2	16
4.3	Removing the CryptoServer Se Gen2	17
5	Installation of the CryptoServer Driver Software.....	18
5.1	Installation on Windows Operating Systems.....	18
5.1.1	Installing the Driver on Windows	18
5.1.2	Performing a Functional Test.....	21
5.1.3	Updating the Driver.....	21
5.1.4	Uninstalling the Driver	22
5.2	Installation on Linux Operating Systems	22
5.2.1	Installing the Driver on Linux.....	22
5.2.2	Performing a Functional Test.....	25
5.2.3	Updating the Driver.....	27
5.2.4	Uninstalling the Driver	28
6	Replacing the Battery	29
7	Disposing of the CryptoServer Se Gen2	34
8	Technical Data.....	35
9	Contact Address for Support Queries	36
	References	37

1 Introduction

Thank you for purchasing our CryptoServer Se-Series Gen2 security system (referred to below as CryptoServer Se Gen2). We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or comments.

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.

1.1 About this Manual

In this manual you will find all the necessary information for using the hardware of the CryptoServer Se Gen2 as well as essential security instructions that are to be followed in order to ensure that the device can be operated safely.

1.1.1 Target Audience for this Manual

This manual is intended for system administrators who bring the CryptoServer Se Gen2 into service and administer it.

1.1.2 Contents of this Manual

Chapter 2 provides safety instructions that should be read carefully, before unpacking the CryptoServer Se Gen2 and bringing it into operation.

Chapter 3 shows the different components of the CryptoServer Se Gen2.

Chapter 4 contains some general notes about how to safely unpack and handle the CryptoServer Se Gen2, as well as general description of the procedure for installation and uninstallation of the CryptoServer Se Gen2 PCIe plug-in card.

Chapter 5 describes how to install the CryptoServer Se Gen2 driver on the host computer, update, test and remove it under Windows and Linux operating systems.

Chapter 6 provides instructions on how to replace the battery of the CryptoServer Se Gen2.

Chapter 7 gives information about what needs to be taken into account when disposing of the CryptoServer Se Gen2.

Chapter 8 is an overview of the essential technical data of the CryptoServer Se Gen2.

Chapter 9 provides the manufacturer's contact data in case you have questions on CryptoServer Se Gen2 or problems occurred while operating the CryptoServer Se Gen2.

1.1.3 Document Conventions

We use the following conventions in this manual:

Bold	Items of the Graphical User Interface (GUI), e.g., menu options
Monospaced	File names, folder and directory names, commands, file outputs,

programming code samples

Italic

References and important terms

We have used icons to highlight the most important notes and information.



Here you find important safety information that should be followed.



Here you find additional notes or supplementary information.

1.2 Other Manuals

The CryptoServer is supplied as a PCI-Express (PCIe) plug-in card in the following series:

- CryptoServer CSe-Series
- CryptoServer Se-Series
- CryptoServer Se-Series Gen2

The CryptoServer LAN (appliance) is supplied in the following series:

- CryptoServer LAN CSe-Series
- CryptoServer LAN Se-Series
- CryptoServer LAN Se-Series Gen2

We provide the following manuals on the product CD for the CryptoServer PCIe plug-in cards CSe-, Se-Series and Se-Series Gen2 and for the CryptoServer LAN (appliance) CSe-, Se-Series and Se-Series Gen2:

Quick Start Guides

You will find these Manuals in the main folder of the SecurityServer product CD. They are available only in English, do not cover all possible scenarios, and are intended as a supplement to the product documentation provided on the SecurityServer product CD.

- *CryptoServer LAN V5 - Quick Start Guide*

If you are looking for step-by-step instructions on how to bring the CryptoServer LAN into service, how to prepare a computer (Windows) for the CryptoServer administration and how to start administrating your CryptoServer with the Java-based GUI CryptoServer Administration Tool (CAT), read this document.

- *CryptoServer PCIe - Quick Start Guide for Linux*

If you are looking for 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 with the CryptoServer Command-line Administration Tool (csadm), read this document.

- *CryptoServer PCIe - Quick Start Guide for Windows*

If you are looking for step-by-step instructions on how to bring the CryptoServer PCIe card into service, how to install the CryptoServer driver on a Windows computer and how to start administrating your CryptoServer with the CryptoServer Command-line Administration Tool (csadm), read this document.

Manuals for System Administrators

You will find these manuals on the product CD in the following folder:

...Documentation\Administration Guides\

- *CryptoServer – Administration Manual*

If you need to administer a CryptoServer PCIe card or a CryptoServer LAN using the CryptoServer Administration Tool (CAT), read this manual. Furthermore, this manual provides a detailed description of the CryptoServer functions, required for the correct and effective operation of the product.

- *CryptoServer LAN V5 – Administration Manual*

If you need to administer a CryptoServer LAN (appliance), read this manual. Since a CryptoServer PCIe card is mounted into the CryptoServer LAN, please read the *CryptoServer – Administration Manual*, as well.

- *CryptoServer - Troubleshooting*

If problems occur while you are using a CryptoServer PCIe card or a CryptoServer LAN (appliance), read this manual.

- *CryptoServer - PKCS#11 P11CAT – Manual*

If you need to administer the PKCS#11 R3 interface with the PKCS#11 CryptoServer Administration Tool (P11CAT), read this manual.

- *CryptoServer - csadm Manual*

If you need to administer a CryptoServer PCIe card or a CryptoServer LAN using the CryptoServer Command-line Administration Tool (csadm), read this manual (only English version available).

Operating Manuals

You will find these manuals on the product CD in the following folder:

...Documentation\Operating Manuals\ . They contain all the necessary information for using the hardware of the CryptoServer PCIe plug-in card respectively the CryptoServer LAN (appliance).

1.3 Import and Export Regulations



The export and use of CryptoServer Se Gen2 outside Germany is subject to the legal foreign trade regulations of the Federal Republic of Germany and requires the appropriate authorization.

The import of CryptoServer Se Gen2 is subject to the legal requirements or other regulations that apply in the particular destination (import license).

Please contact your own national import authorities for more detailed information.

1.4 Damage in Transit

By purchasing CryptoServer Se Gen2 you have acquired a device that has been carefully tested and packed for delivery. Nevertheless, damage may occur during transport or improper temporary storage.

If you discover that the transport boxes are damaged when they arrive, please immediately contact your reseller or Utimaco IS GmbH (the address and telephone number are given in Chapter 9). Please have the delivery note and the device's serial number ready.

1.5 Deliverables

The CryptoServer Se Gen2 deliverables include:

- one CryptoServer Se Gen2 PCI Express plug-in card
- one *CryptoServer PCIe Se-Series Gen2 Operating Manual* (this Manual)

You can also use smartcards to administer the CryptoServer Se Gen2. These smartcards, and also the appropriate PIN pad can be purchased from Utimaco IS GmbH.

You cannot use PIN pads and smartcards that were not purchased from Utimaco IS GmbH to administer the CryptoServer Se Gen2.

2 General Safety Advice



Please follow all the warnings, safety notes and instructions given on the device or in this introduction. If you fail to do so, Utimaco IS GmbH will not accept any responsibility for any resulting damage caused.

The hardware security module CryptoServer Se Gen2 is fitted with a sensor which will delete all the data from the device if it is physically tampered with, or if the environmental temperature rises above, or falls below, the permitted operating temperature range.



Please read the safety instructions below carefully, before unpacking the device and bringing it into operation, to ensure that the device can be operated safely, and to prevent the CryptoServer Se Gen2 sensors from deleting data by mistake. Always keep these instructions handy, in a safe place.

Do not attempt to repair the CryptoServer Se Gen2 in any way.

2.1 Moving and Storing

When moving and storing the device, follow these instructions:

- The CryptoServer Se Gen2 should only be moved and stored in its original packaging.
- Although there is no motion detector on the CryptoServer PCIe card that could initiate the deletion of data, do not subject the device to impacts and vibrations or any other physical events that may damage the packaging.
- You must make sure that the CryptoServer Se Gen2 is always stored at temperatures between -10 °C and +55 °C (+14 °F and +131 °F).
- If the device is to be stored for a longer time period, ensure that the battery replacement time is not exceeded. For details, see Section 2.2, "Battery".
- Keep this manual together with your CryptoServer Se Gen2 so that it is handy if you need to reinstall the system.
- The PCIe connector is fragile, and can be damaged or even broken during movement and transport by force and acceleration of the computer chassis, where the CryptoServer is mounted in.
- There is a point of mechanical stress on the printed circuit board (PCB) near the PCIe bracket, which can be damaged.
- The maximum permissible deflection of the CryptoServer's PCB across its surface during movement and transport is restricted to 2 mm.

For these reasons careful attention is required during transport, movement and storage of the CryptoServer PCIe cards all series. Read additionally Section 2.3, "Safely Transporting the CryptoServer". We strongly recommend removing the CryptoServer PCIe card from the computer prior to any planned transport or movement. All cryptographic keys stored on the PCIe card remain securely maintained during the transport or movement since the CryptoServer is continuously supplied with power by the carrier battery.

2.2 Battery

One 3 V lithium battery (carrier battery) ensures that the CryptoServer Se Gen2 sensors and the erase circuit are always able to function correctly, that is, as long as the CryptoServer is not mounted in a computer or even if the computer, where it is mounted in, is switched off. This battery can power the CryptoServer for at least 6 months, and is already in use when the device is supplied.



This battery is not rechargeable.

If the CryptoServer Se Gen2 is operated in a computer that is not itself switched on, you must change the battery at regular intervals. If you do not do so, an alarm might be triggered and all the data on the device may be lost.

2.3 Safely Transporting the CryptoServer

This section describes which steps have to be performed to remove a CryptoServer PCIe card from a computer, transport it to another location and install it there in another computer.

Prerequisites

- Ensure that the requirements in Section 2.1, "Moving and Storing", are fulfilled.
- Prepare the new location of the CryptoServer PCIe card according to Section 4.1, "General Notes".

To ensure the safe transport of the CryptoServer PCIe card over long or short distances from the old location to the new location, proceed as follows:

Check the state of the carrier battery with the `csadm GetBattState` command or the CryptoServer Administration Tool (CAT).

- Example on a Windows operating system:

```
csadm Dev=PCI:0 GetBattState
```

- Example on a Linux operating system:

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

- Using CAT.

Click **Show > Battery State**.

Verify the output for the carrier battery.

The carrier battery ensures that the CryptoServer sensors and the erase circuit are always able to function correctly when the CryptoServer is not installed in a computer. Otherwise, an alarm might be triggered and all the data on the device may be lost.

- If the carrier battery power is displayed as **ok**, for example,
Carrier Battery: ok (3.068 V),
continue with step 0.
- If the carrier battery power is displayed as **low**, for example,
Carrier Battery: low (2.650 V),
continue with step 0.

The external battery is relevant only for the CryptoServer LAN.

Replace the carrier battery by a new one (3 V, Lithium, FDK CR 12600 SE-T1 with soldering tags, or similar type). You find step-by-step instructions on how to do that in Chapter 6, "Replacing the Battery", of this document. This battery ensures the power supply of the CryptoServer Se Gen2 for at least 6 months.

If you have replaced the carrier battery, continue with step 0 on page 12. Otherwise, continue with the next step.

As a preparation for backing up databases described below, determine the Master Backup Key (MBK) that is used in MBK slot 3. To determine this MBK, you can either perform the `csadm MBKListKeys` command according to Section "MBKListKeys" in [CSADMIN] or use CAT according to Section "Retrieving MBK Information" in [CSMSADM].

Note down the name of this MBK.



This MBK is used by the `csadm BackupDatabase` command to protect the backup file to be generated.

It is important to note down which MBK has been used because for a successful restoring of this backup file at a later date it is necessary that the same MBK is in MBK slot 3. Otherwise, for example, after the execution of a `csadm MBKImportKey` command or after an MBK rollover, the backup file is inaccessible. See Section "Master Backup Key Rollover" in [CSADMIN] for details.

Verify that all shares of this MBK are available as keyfiles or on smartcards. To verify MBK shares on a smartcard, either perform the `csadm MBKCardInfo` command according to Section "MBKCardInfo" in [CSADMIN] or use CAT according to Section "Retrieving MBK Information" in [CSMSADM].

Back up the following databases.

- User database (`user.db`)

- Cryptographic key database (CXIKEY.db)
- Audit log signature key (auditkey.db), if available

To do so, you can either perform the `csadm BackupDatabase` command according to Section "BackupDatabase" in [CSADMIN] or use CAT according to Section "Backing up Databases" in [CSMSADM].

Example:

```
csadm LogonSign=ADMIN,:cs2:cjo:USB0 BackupDatabase=CXIKEY.db BackupDatabase=user.db
BackupDatabase=auditkey.db
```

Remove the CryptoServer PCIe card from the computer. Follow the instructions for removing PCIe cards as specified in the operating manual for your computer as well as the instructions in Section 4.3, "Removing the CryptoServer Se Gen2", of this document.

Put the CryptoServer PCIe card into an antistatic wrapping and in the original packaging. If you need an original packaging or/and antistatic wrapping, contact the manufacturer Utimaco IS GmbH.

Again, ensure that the requirements in Section 2.1, "Moving and Storing", are fulfilled.

After reaching destination, put the computer, where the CryptoServer PCIe card should be mounted in, to the required position, and then mount the CryptoServer PCIe card. Follow the instructions for mounting PCIe cards as specified in the operating manual for your computer as well as the instructions in Section 4.2, "Installing the CryptoServer Se Gen2", in the current document.

2.4 Environmental Temperature

The CryptoServer Se Gen2 should only be operated and stored in a particular temperature range.

- You must make sure that the CryptoServer Se Gen2 is always stored at temperatures between -10 °C and +55 °C (+14 °F to +131 °F).
- You must make sure that the CryptoServer Se Gen2 is always operated at temperatures between +10 °C and +45 °C (+50 °F to +113 °F).



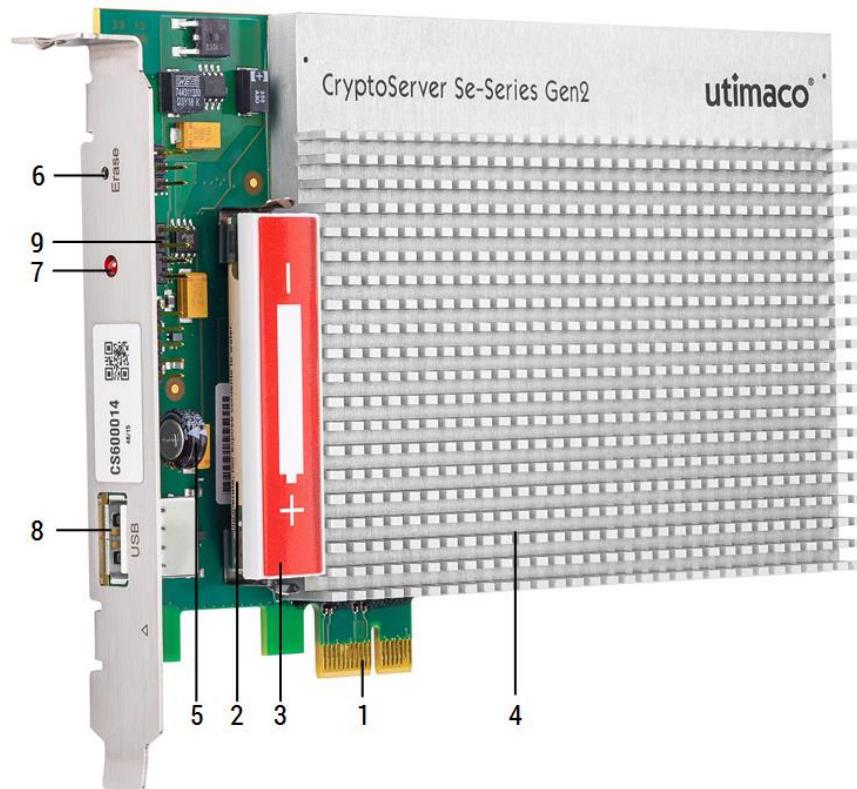
If the environmental temperature is out of the permitted range, there is a risk that the device sensor will delete all the data on it.

For security reasons, the CryptoServer Se Gen2 PCIe card implements a mechanism that actively protects the device from being used under extreme temperatures. For this purpose, the CryptoServer Se Gen2 PCIe card implements a temperature sensor that is located inside the CryptoServer Se Gen2 PCIe card and that permanently monitors the temperature to trigger an immediate action in case that the allowed range is exceeded. For the permitted temperature range of the temperature sensor, see Section "Temperature Monitoring" in [CSMSADM]. This section describes in detail at which temperatures the CryptoServer Se Gen2 is shut down or even an alarm is triggered, and all sensitive data is deleted. There is therefore a risk that the CryptoServer Se Gen2 is shut down and deletes all sensitive data

because a too low or too high environmental temperature indirectly brings the inside temperature out of the permitted range

3 Components of CryptoServer Se Gen2 (PCIe)

The CryptoServer Se Gen2 consists of the following components:



- 1 PCI Express bus (PCIe x1) of the PCIe plug-in card
- 2 Battery
To supply power to the sensors and quenching system when the computer is switched off
- 3 Battery protection cap
- 4 Encapsulated processor
This mechanical protection prevents cryptographic data from being manipulated or extracted
- 5 Capacitor
Continues supplying power for approximately five minutes whilst a battery is being replaced
- 6 Erase pushbutton
Pushbutton for performing External Erase
- 7 LED flash light
Flashes up red to indicate the activation of the Erase pushbutton
- 8 USB port (external)
USB 2.0 port for peripheral devices such as a PIN pad
- 9 USB port (internal)
Port strip for additional USB 2.0 connection

4 Unpacking and Handling

The CryptoServer Se Gen2 is supplied with several encryption keys already stored on it. You cannot operate the device unless these keys are present. For this reason, take great care when unpacking and then installing the device.

The CryptoServer Se Gen2 is also already fitted with a battery when it is supplied. This battery is already in operation. Therefore, all the individual contact points and components are supplied with power.



The CryptoServer Se Gen2 is packaged in a special antistatic wrapping. Please retain this wrapping in case you need to store or transport the device.

The CryptoServer Se Gen2 must always be stored in this specific anti-static wrapping. This is because many other types of anti-static wrap are more conducting and may cause a short circuit on the contact points that supply power.



When unpacking and installing the device, follow all the standard guidelines for working with electrical devices and take all the applicable protective measures.

In particular, you must note the following points.



Never place the bottom of the circuit board on a surface that can conduct electricity (for example, the metal cover of a computer), as this can cause a short-circuit.

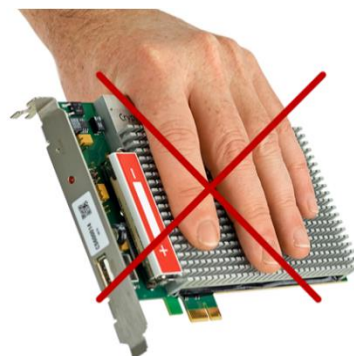
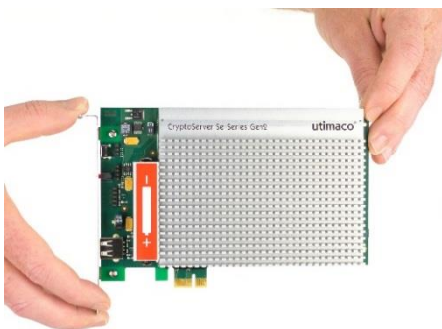
Take care that the circuit board never touches a metallic object (such as a screwdriver or wedding ring).

Never touch the contacts on the backside of the circuit board.



Do not touch any contacts on the card. Handle the CryptoServer Se Gen2 only at its mounting plate and the edges of the carrier board (see left side of figure below).

Do not apply any pressure on the encapsulated unit, and do not touch any contacts on the backside of the carrier board (see right side of figure below).



*Correct**Wrong*

4.1 General Notes

The CryptoServer Se Gen2 is fitted with a system of sensors that can tell whether it is being operated within a permitted temperature range.



During normal operations, the internal temperature of the CryptoServer Se Gen2 must not exceed 62 °C (143 °F). If it does, the device will switch off automatically. Consequently, you must ensure that the CryptoServer Se Gen2 is cooled to below this temperature. To ensure that the internal temperature is not exceeded, the environmental temperature should not be more than 45 °C (113 °F).

For this reason, it is important you note the following installation instructions:

- The computer in which you want to mount the CryptoServer Se Gen2 must be sited in a cool, well ventilated place.
- Do not place it near sources of heat or in direct sunlight.
- You must ensure that the expansion slot in which CryptoServer Se Gen2 is mounted lies in the computer's ventilation airstream.
- The CryptoServer Se Gen2 should only be inserted below other plug-in cards that radiate heat.
- Ensure that you keep one expansion slot free between all other plug-in cards, or other devices, and the CryptoServer Se Gen2.



If you cannot implement this configuration, we strongly recommend you mount a PCIe slot cooling fan directly beside the CryptoServer Se Gen2 device.

4.2 Installing the CryptoServer Se Gen2

Follow the instructions for installing PCIe cards as specified in the operating manual for your computer. This is only a general description of the procedure:

1. Switch off the computer.

Unplug all cables.

Open the computer case.

Select a free PCIe expansion slot and remove the corresponding slot cover on the rear face of the computer.

Insert the CryptoServer Se Gen2 PCIe card in the computer's PCIe expansion slot. Make sure the card fits securely.

Close the computer case.

Reconnect the cables.

Switch the computer on again.

4.3 Removing the CryptoServer Se Gen2

You will need to remove the CryptoServer Se Gen2 to change its carrier battery or to store or transport it.



Follow the instructions for removing PCIe cards as specified in the operating manual for your computer.

1. Switch off the computer.



Please note that the heat sink of the CryptoServer Se remains very hot for quite a while after you have switched off the computer. Please allow the heat sink to cool down first before you remove the CryptoServer Se Gen2.

Unplug all cables.

Open the computer case.

Remove the CryptoServer Se Gen2 carefully from the PCIe slot. You must never use a tool (for example, screwdriver) to lever the card out of the slot.

Close the computer case.

Reconnect all cables.

5 Installation of the CryptoServer Driver Software

You can find the list of all currently supported operating systems in the document CS_PD_SecurityServer_SupportedPlatforms.pdf on the product CD in the folder ...\\Documentation\\Product Details.

The following sections describe how to install the CryptoServer Se Gen2 driver in the host computer, update it, and then remove it, under a number of different operating systems.

5.1 Installation on Windows Operating Systems

To install or upgrade the CryptoServer driver, you need these files:

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



*You can find the files on the product CD in the following directory:
Software\\Windows\\Driver\\bin*

5.1.1 Installing the Driver on Windows



You should have local Administrator rights for the host computer (Windows), where the CryptoServer Se Gen2 driver shall be installed on.



The driver supports a maximum of 32 CryptoServer PCIe cards.

Prerequisites

To run the GUI tools, your Java installation needs to support unlimited crypto. If your system does not have a JRE, download one from <http://openjdk.java.net/Next> install the corresponding Java security policy files, for example UnlimitedJCEPolicyJDK11.zip from the openjdk.java.net website. Extract them and copy the *.jar files to your /lib/security directory.

Procedure

To install the CryptoServer driver on a computer with a Windows operating system, proceed as follows:

1. In the highest folder level of the product bundle, click the file **SecurityServer-<version number>.msi**.



*If necessary, you will be prompted to install the Microsoft runtime environment (VCRedist). Click **OK** to confirm the corresponding dialog box.*

2. In the installation wizard, click **Next**.
3. In the **Select Installation Folder** dialog, use the **Browse...** button to select a different directory for installing the software or confirm the default installation directory.
4. Click **Next**.

The **Choose Setup Type** dialog box opens.

Typical

The CryptoServer administration tools (CAT, csadm etc.) and the CryptoServer documentation are installed.

Custom

This installation type lets you specify the features to be installed.

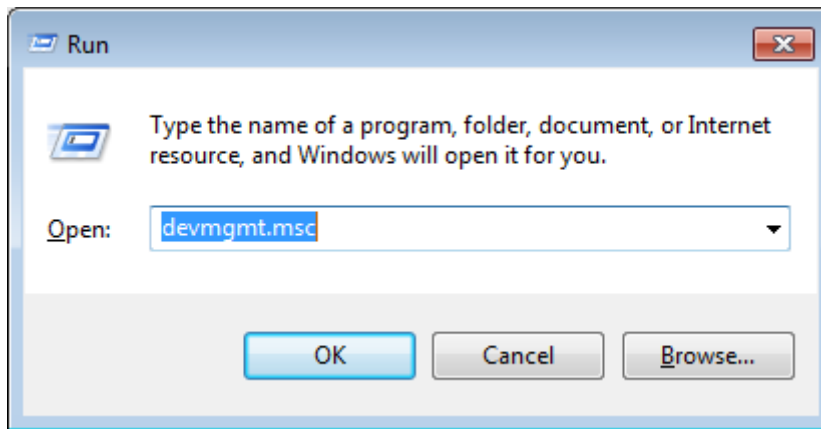
Complete

This corresponds to selecting all items of the custom installation except for PCIe driver and PIN Pad driver.

Select **Custom**.

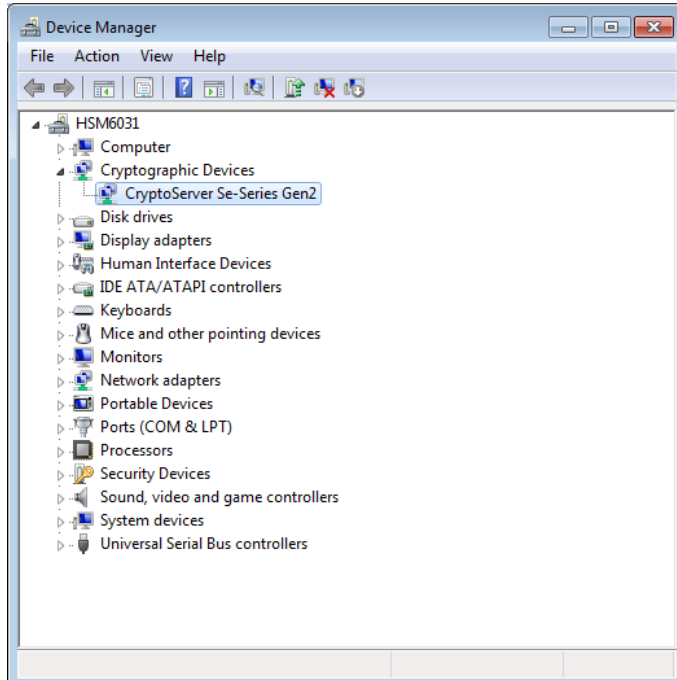
5. The **Select the features to be installed** dialog box opens. By default, **Administration** and **Documentation** are selected.
6. Clear all items that should remain unchanged (not be installed/updated). They are indicated by a red X.
7. Click the small black triangle next to **Drivers > CryptoServer** and select **Will be installed on local hard drive**.
8. Click **Next**.
9. In the **Ready to Install** dialog box, click **Install**.
10. Click **Finish** to complete the software installation.
11. Start the device manager.

- a) Open the **Run** dialog by pressing the  key and then simultaneously pressing the R key.



- b) Enter `devmgmt.msc` into the text field and press the ENTER key.
The Windows device manager opens.

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



5.1.2 Performing a Functional Test

If you want to check if the driver has been installed correctly and that the CryptoServer Se Gen2 is functioning as it should, please follow these steps:

1. Use the Windows **Start** menu to select the **Run** option.
2. Enter `cmd` in the window that now opens.
3. Then click **OK** to open the command line window.

Input 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 your CD/DVD drive is the D: drive and that the CryptoServer PCIe card is in the first slot.

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

If the driver has been installed correctly and the CryptoServer Se Gen2 is functioning as it should, you should see output that is similar to the following:

```
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  CS60000024
adm2    = 53656375 72697479 53657276 65720000 | SecurityServer
adm3    = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

If you cannot communicate with the CryptoServer Se Gen2, check that the PCIe card has been mounted correctly. Also check in the Windows Device Manager to see whether the driver has been installed correctly. After that, repeat the functional test.

If you still cannot communicate with the CryptoServer Se Gen2, contact either the reseller who supplied this CryptoServer Se Gen2 or the Utimaco IS GmbH Customer Service team.

If you use several CryptoServer PCIe cards or the card is in another 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.

5.1.3 Updating the Driver

If you want to update the driver later on, proceed as follows:

1. Open the Device Manager.

Click with the right-hand mouse button on **CryptoServer Se-Series Gen2**, and select the context menu option **Update Driver Software....**

Select the option **Browse my computer for driver software**.

Click on **Browse...** .

The remaining steps you must follow to select and install the new driver are the same as those for installing the driver for the first time as described in Chapter 5.1.

5.1.4 Uninstalling the Driver



You must uninstall the driver from your computer before you remove the CryptoServer Se. It is not possible to uninstall the driver after you have removed the CryptoServer Se from the computer.

If you want to uninstall the driver, please follow the steps below.

1. Open the Device Manager.

Click with the right-hand mouse button on **CryptoServer Se-Series Gen2**, and select the context menu option **Uninstall**.

In the next window, click **OK** to confirm that you want to uninstall the driver.

Also select the option for deleting the driver software from your computer.

The CryptoServer Se Gen2 driver will now be uninstalled and removed from your computer.

After you close the wizard, the **CryptoServer Se-Series Gen2** is also deleted from the Device Manager display.

Shut down the Windows operating system before removing the CryptoServer Se Gen2 plug-in card.

5.2 Installation on Linux Operating Systems

Due to the architecture of the Linux kernel, it is unfortunately not possible to provide a driver that is ready for installation.

For this reason, the CryptoServer driver for Linux is supplied as source code on the product CD and must be compiled on the target system.

5.2.1 Installing the Driver on Linux

5.2.1.1 Prerequisites

To compile the CryptoServer driver on a Linux operating system, the following prerequisites must be available:

- The source code of the CryptoServer driver must be available.

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

The driver supports a maximum of 8 CryptoServer PCIe cards. This number can be changed in the source code of the driver.

- Each major Linux distribution has a package for headers, often called "kernel-devel". Some distributions use other names, for example, "linux-headers-amd64" for a 64-bit Debian. Check the documentation of your distribution. Ensure that this package is installed.
- Ensure that gcc is installed.
- Ensure that make is installed.
- root privileges on the computer are required for performing the CryptoServer driver installation on a Linux operating system.

5.2.1.2 Check Hardware

Before beginning with the driver installation, a hardware check must be performed.

Check that the card is detected on your PC by running: `lspci -d '*:c071'` and then look for 168a:c071

```
$ lspci -d '*:c071'  
01:00.0 Network and computing encryption device: Device 168a:c071
```

5.2.1.3 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.

5.2.1.4 Build and Install the Driver under Ubuntu/Debian

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

1. Run the following commands, 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 apt install ./cryptoserver-dkms_5.18.0_all.deb
```

2. After a reboot, you will find yourself in the MOK utility. Choose enroll key and re-enter the previously chosen password.



A reboot is recommended in this case to ensure the driver loads automatically.

5.2.1.5 Build and Install the Driver under CentOS/Fedora/openSUSE/SLES/RHEL



For SLES 12, do not perform the following steps, but the steps described further below.

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

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

```
# centos/rhel
$ sudo yum install ./cryptoserver-dkms-5.18.0-Linux.rpm kernel-devel
# fedora
$ sudo dnf install ./cryptoserver-dkms-5.18.0-Linux.rpm kernel-devel
# opensuse/sles
$ sudo zypper install ./cryptoserver-dkms-5.18.0-Linux.rpm
```

For SLES 12, perform the following steps instead:

1. Create a new temp directory.

```
mkdir temp
```

2. Move the cryptoserver-dkms-5.19.0-Linux.rpm file into this temp directory, adjusting the version number as necessary.

```
mv cryptoserver-dkms-5.19.0-Linux.rpm temp/.
```

3. Go to this temp directory.

```
cd temp
```

4. Perform the following commands, adjusting the version number as necessary.

```
rpm2cpio cryptoserver-dkms-5.19.0-Linux.rpm | cpio -idmv
cd usr/src/cryptoserver-5.19.0/
```



```
make  
make install
```

5. Change the value of `allow_unsupported_modules` to 1 in the `/etc/modprobe.d/10-unsupported-modules.conf` file.
6. Create the `/etc/modules-load.d/cryptoserver.conf` file with the line `cryptoserver` as content.
7. Create the `/etc/modprobe.d/70-cryptoserver.conf` file with the line `options cryptoserver DeviceMask=0xFFFFFFFF` as content.
8. Go to the directory containing the `temp` directory you created above.
9. Remove the `temp` directory you created above. Do not remove the `/tmp` directory.

```
rm -rf temp
```

10. Reboot the computer.

```
reboot
```

On the CentOS/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.

5.2.1.6 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.

5.2.2 Performing a Functional Test

To verify that the driver has been installed correctly and that the CryptoServer Se Gen2 is working properly, follow these steps:

1. Copy the CryptoServer Administration Tool `csadm` from the product CD to your local disk.

Example:

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

2. Make the csadm file executable.

```
chmod u+x csadm
```

3. Verify the connection to the CryptoServer.

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

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

If the driver has been installed correctly, and the CryptoServer Se Gen2 is working properly, you see an

```
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
```

Make sure that the following lines are shown.

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

They indicate that the CryptoServer is in Operational Mode and that no alarm has been triggered.

If there are problems to produce an output similar to the one above, perform the following substeps.

- a) Verify that the kernel module is running.

```
lsmod | grep cryptoserver
```

Example output:

```
Cryptoserver 90112 0
```

- b) Verify that the device node has been created.

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

Example output:

```
crw-rw-rw- 1 root root 240, 0 Dez 19 16:17 /dev/cs2.0
```

- c) Verify for error messages.

```
dmesg | grep :cs
```

- d) If you cannot communicate with the CryptoServer Se Gen2, verify that the PCIe card has been mounted correctly and verify if the driver has been installed correctly. After that, repeat the functional test.

If you still cannot communicate with the CryptoServer Se Gen2, contact either the reseller who supplied this CryptoServer Se Gen2 or the Utimaco IS GmbH Customer Service team. See Chapter 9, "Contact Address for Support Queries", for details.

- e) If you use several CryptoServer PCIe cards or the card is in the second, third etc. found PCIe slot, replace `/dev/cs2.0` in the above command by `/dev/cs2.1` or `/dev/cs2.2` etc. for each additional card and perform this command again.

5.2.3 Updating the Driver

5.2.3.1 Updating the Driver from SecurityServer Release before 4.30

If you want to upgrade the CryptoServer driver from a SecurityServer release before 4.30, perform the following steps as a root/super user.

1. Unload the kernel module.

```
modprobe -r cs2
```

Determine the kernel version using this command:

```
uname -r
```

Delete the `cs2.ko` kernel module, with this command:

```
rm /lib/modules/<kernel version>/extra/cs2.ko
```

Delete the `cs2a` device file with this command:

```
rm /dev/cs2a
```

Delete the udev rule automatically creating the device node. This command may fail if you do not have installed the udev rule.

```
rm /lib/udev/rules.d/10-cryptoserver.rules
```

Perform the following substeps depending on the Linux distribution you use.

- SLES

Remove the `cs2` line from the `/etc/modules` file.

- RHEL

Remove the `modprobe cs2` line from the `/etc/rc.modules` file.

Reboot the computer.

Follow the steps in Section 5.2.1, "Installing the Driver",

Follow the steps in Section 5.2.2, "Performing a Functional Test".

5.2.3.2 Updating the Driver from a SecurityServer Release 4.30

To upgrade the CryptoServer driver from a SecurityServer Release 4.30, proceed as follows:

1. For SLES only: Remove the `cryptoserver` line from the `/etc/modules` file.

For RHEL only: Remove the `modprobe cryptoserver` line from the `/etc/rc.modules` file.

Follow the steps in Section 5.2.1, "Installing the Driver",

Follow the steps in Section 5.2.2, "Performing a Functional Test".

5.2.3 Updating the Driver from a SecurityServer Release 4.31 or later

To upgrade the CryptoServer driver from a SecurityServer Release 4.31 or later, follow the steps in Section 5.2.1, "Installing the Driver", and Section 5.2.2, "Performing a Functional Test".

5.2.4 Uninstalling the Driver

Perform the following commands as a root/super user to uninstall the driver.

1. Unload the kernel module.

```
modprobe -r cryptoserver
```

Determine the kernel version using this command:

```
uname -r
```

Delete the `cryptoserver.ko` kernel module, with this command:

```
rm /lib/modules/<kernel version>/extra/cryptoserver.ko
```

Disable auto-loading of the kernel module. To do so for Linux distributions running `systemd` (RHEL 8 and later and SLES 12 and later), perform the following command.

```
rm /etc/modules-load.d/cryptoserver.conf
```

For other Linux distributions, consult the documentation.

If there are no other external kernel modules, you can change the value of the

`allow_unsupported_modules` variable to 0 in the `/etc/modprobe.d/10-unsupported-modules.conf` file.

Shut down the computer before removing the CryptoServer Se Gen2.

6 Replacing the Battery

A battery (carrier battery) ensures the sensor system and the quenching circuit can function even when the CryptoServer Se Gen2 is switched off.

If the CryptoServer Se Gen2 is running in a computer, its power is supplied via the PCIe interface. In this case the battery is not required. However, if a battery has already been partially discharged, this will not recharge it.

In those situations, when the CryptoServer Se Gen2 is not supplied with power via the PCIe interface, for example when it is being stored or if the computer is switched-off, it will be powered by the battery. The battery can supply the CryptoServer Se Gen2 with power for at least 6 months.



This battery is not rechargeable.

Depending on how frequently the CryptoServer Se Gen2 is in operation, the battery must be replaced at specific intervals. If the battery is not replaced at the right time, an alarm will be triggered and all the data on the CryptoServer Se Gen2 will be deleted.

For this reason, you should check the battery status regularly. To do this, run the **GetBattState** command in the csadm administration tool.

```
csadm Dev=PCI:0 GetBattState
```

GetBattState output example:

Carrier Battery: low (2.540 V)

External Battery: absence

If the status of the carrier battery is shown as **LOW**, you must replace it as soon as possible. The external battery is only relevant for the CryptoServer LAN.



Read the instructions carefully before you change the battery.

1. Before replacing the battery, make sure you have the correct type of battery. We recommend you use only FDK CR 12600 SE-T1 batteries with soldering tags or a similar type.



Using the wrong batteries may cause an explosion. Utimaco IS GmbH accepts no responsibility for damage caused by any batteries other than those recommended by Utimaco IS GmbH.

Ensure you dispose of spent batteries in accordance with the manufacturer's instructions and in an environmentally responsible manner.

Make sure the battery contacts are clean and grease-free.



Clean both battery contacts and the soldering tags with alcohol.

When performing the following steps, avoid touching the contacts with your fingers.

As a preparation for backing up databases described below, determine the Master Backup Key (MBK) that is used in MBK slot 3. To determine this MBK, you can either perform the `csadm MBKListKeys` command according to Section "MBKListKeys" in [CSADMIN] or use CAT according to Section "Retrieving MBK Information" in [CSMSADM].

Note down the name of this MBK.



This MBK is used by the `csadm BackupDatabase` command to protect the backup file to be generated.

It is important to note down which MBK has been used because for a successful restoring of this backup file at a later date it is necessary that the same MBK is in MBK slot 3. Otherwise, for example, after the execution of a `csadm MBKImportKey` command or after an MBK rollover, the backup file is inaccessible. See Section "Master Backup Key Rollover" in [CSADMIN] for details.

Verify that all shares of this MBK are available as keyfiles or on smartcards. To verify MBK shares on a smartcard, either perform the `csadm MBKCardInfo` command according to Section "MBKCardInfo" in [CSADMIN] or use CAT according to Section "Retrieving MBK Information" in [CSMSADM].

Back up the following databases.

- ▣ User database (`user.db`)
- ▣ Cryptographic key database (`CXIKEY.db`)
- ▣ HSM Authentication Key (`authkey.db`), if available
- ▣ Audit log signature key (`auditkey.db`), if available

To do so, you can either perform the `csadm BackupDatabase` command according to Section "BackupDatabase" in [CSADMIN] or use CAT according to Section "Backing up Databases" in [CSMSADM].

Example:

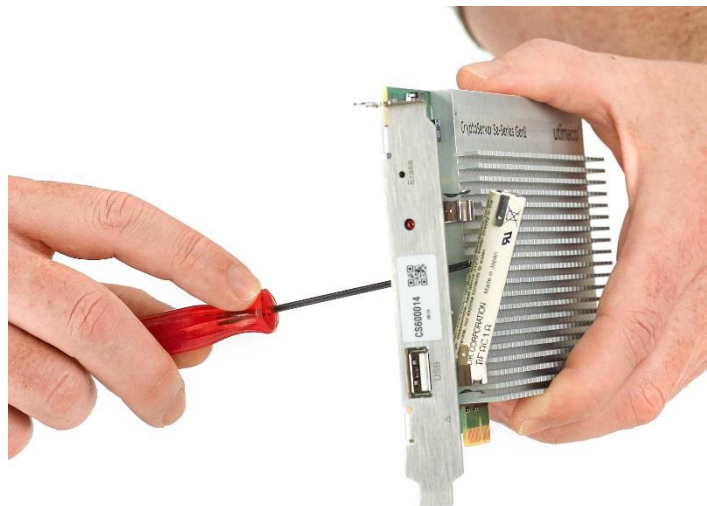
```
csadm LogonSign=ADMIN,:cs2:cjo:USB0 BackupDatabase=CXIKEY.db BackupDatabase=user.db  
BackupDatabase=authkey.db BackupDatabase=auditkey.db
```

Turn off the computer.

Remove the CryptoServer Se Gen2 from the computer.

Consider that you have a maximum of 5 minutes for the actual battery replacement in the next two steps. For this period of time, it is guaranteed that a capacitor supplies the PCIe card with electric current and that the data on the PCIe card is not deleted. After a maximum of 30 minutes without a carrier battery, the data on the PCIe card is deleted in any case.

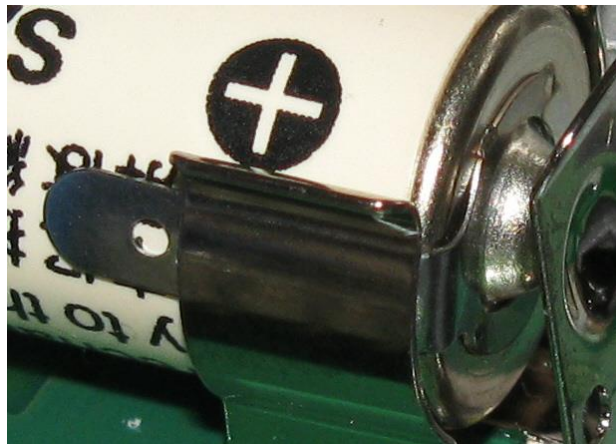
On the reverse of the battery clips you see a hole in the board. Insert a thin tool (screwdriver) through the hole to remove the battery from its mounting clips (see the Figure below).



Change the battery.



Make sure the polarity is correct (see the label on the CryptoServer Se Gen2). If the polarity is incorrect, the data on the device will be deleted. When removing the battery for replacement, pay specific attention to the polarity, and compare the physical installation against the direction of the label on the battery cover. After installing the replacement battery, ensure that the cover is replaced with the polarity label correctly oriented. Make sure that the soldering tags on the battery are in contact with the lateral mountings for the battery (see the Figure below).



You have a maximum of 5 minutes in which to replace the battery. During this period, a capacitor ensures the CryptoServer Se Gen2 continues to be supplied with power. If you do not insert a new battery within a maximum of 30 minutes, an alarm is triggered and all sensitive data on the CryptoServer Se Gen2 is deleted.

Reinstall the CryptoServer Se Gen2.

Make a note of the next battery replacement date.

Turn on the computer.

Check the status of the CryptoServer Se Gen2 by using the CryptoServer administration tool you chose – csadm or CAT.

Example with the csadm command **GetState**:

csadm PCI:0 GetState

In case the battery replacement took you more than five minutes, the output of the csadm command **GetState** shows

- ▣ that an alarm has been triggered:

alarm = ON

- ▣ and the cause for the alarm:

sens = 02bf

- Alarm has occurred
- Power failed

This means that the sensor controller remained without power for a long time.

Example output for **GetState**:

```
mode    = Maintenance Mode
state   = INITIALIZED (0x020aff84)
temp    = 36.1 [C]
```


alarm = ON

sens = 02ff

- Alarm has occurred
- Power failed

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

Reset the alarm by using the CryptoServer administration tool you chose – csadm or CAT.

Example with the csadm command **ResetAlarm**:

```
csadm Dev=PCI:0 LogonSign=ADMIN,:cs2:cjo:USB0 ResetAlarm
```

Set the time and date of the CryptoServer Se Gen2 by using the CryptoServer administration tool you chose – csadm or CAT.

Example with the csadm command **SetTime**:

```
csadm Dev=PCI:0 LogonSign=ADMIN,:cs2:cjo:USB0 SetTime=GMT
```

Now, your CryptoServer Se Gen2 is ready for use again.

7 Disposing of the CryptoServer Se Gen2

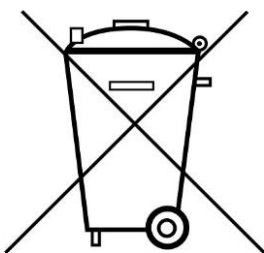
To dispose of your CryptoServer Se Gen2, perform the following steps.

1. Perform an External Erase to securely delete all sensitive data from your CryptoServer Se Gen2. Refer to [CSMSADM] for details.

Of course, you also have the option of returning the CryptoServer Se Gen2 that you no longer require to us, Utimaco IS GmbH, as the manufacturer. Below you will find a description of how to dispose of the CryptoServer Se Gen2 and the battery in an environmentally friendly way.

If you want to dispose of the CryptoServer Se Gen2 yourself, note that in the CryptoServer Se Gen2 carrier you will find a battery which must be disposed of in an environmentally friendly way.

Remove the battery from the CryptoServer Se Gen2 and note the following general information about rechargeable and non-rechargeable batteries (in accordance with the German Notice Requirement According to §18 BattG (the law concerning Batteries)).



You are not permitted to throw away rechargeable or used batteries in the normal household waste.

Consumers are obliged to bring batteries to a suitable municipal or commercial collection point.

Rechargeable and used batteries can contain harmful materials or heavy metals that can damage the environment and health.

Batteries are reused. They contain important raw materials such as iron, zinc, manganese or nickel.

Regardless of whether you have performed an External Erase or not, the following applies: If you remove the CryptoServer PCIe card from the computer and remove any battery from this plug-in card, the sensitive data on this plug-in card is deleted automatically in any case after a maximum of 30 minutes.

You can either dispose of the battery of the CryptoServer Se Gen2 at a suitable municipal or commercial collection point, or send it to us, Utimaco IS GmbH, as the manufacturer.

8 Technical Data

Dimensions	PCI Express (PCIe) plug-in card: Length: 167.65 mm ("half" length) Height: 111.15 mm ("full" height)
Weight	400 g
Battery	3 V, Lithium, Ø 12 mm, L = 600 mm, FDK CR 12600 SE-T1 with soldering tags, or similar type
Ports	PCIe x1 2 USB 2.0
Environmental temperature	Operation: +10 °C to +45 °C (+50 °F to +113 °F) Storage: -10 °C to +55 °C (+14 °F to +131 °F)
Humidity	10 % to 95% relative humidity, non-condensing
MTBF	360.000 hours (as specified in MIL-HDBK-217)
RoHS compliance	Yes
WEEE	National register for waste electric equipment (EAR) DE65203472
Conformity	Interference emission in accordance with EN 55022 Class B Influence of interference in accordance with EN 61000-6-2 (industry) Equipment safety in accordance with EN/IEC 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 FCC 47 CFR Ch. 1 Part 15 Class B

9 Contact Address for Support Queries

If an error occurs while operating the CryptoServer, read [CSTrSh] to solve it.

If the error still occurs, prepare diagnostic information in a .txt file on your computer as described in [CSTrSh].

If you have any further questions on CryptoServer, feel free to contact us.

You can reach us from Monday to Friday 09.00 a.m. to 05.00 p.m., apart from German public holidays and other customs days.

Utimaco IS GmbH

Germanusstr. 4

52080 Aachen

Germany

■ RMA query

If you need to send the CryptoServer back to the Utimaco IS GmbH, i.e., open a new RMA case, 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>

■ For other support queries, use the following contact data:

▣ By mail (preferred contact method)

support@utimaco.com

Attach the diagnostic information to your e-mail.

▣ By 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.

References

<i>Reference</i>	<i>Title/Company</i>	<i>Document No.</i>
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH.	2009-0003
[CSMSADM]	CryptoServer – Administration Manual/Utimaco IS GmbH.	M010-0001-en
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH.	M011-0008-en