
# CryptoServer PCIe

CSe-Series

Operating Manual

utimaco®

# Imprint


| | |
|---|---|
| Copyright 2017 | Utimaco IS GmbH<br>Germanusstr. 4<br>D-52080 Aachen<br>Germany |
| Phone | +49 (0)241 / 1696-200 |
| Fax | +49 (0)241 / 1696-199 |
| Internet | http://hsm.utimaco.com |
| e-mail | hsm@utimaco.com |
| Document Version | 1.1.7 |
| Date | 2017-02-09 |
| Status | Final |
| Document No. | M013-0002-en |

# Table of Contents

# 1 Introduction

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

## 1.1 About this Manual

In this operating manual you will find all the necessary information for using the hardware of the CryptoServer 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 CSe plug-in card 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 CSe and bringing it into operation.

*Chapter 3* shows the different components of the CryptoServer CSe.

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

*Chapter 5* describes how to install the CryptoServer CSe 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 CSe.

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

*Chapter 8* is an overview of CryptoServer CSe's essential technical data.

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

### 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 CSe-, Se- and Se-Series Gen2 plug-in cards and for the CryptoServer LAN (appliance) CSe-, Se- 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 - 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 7) 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*
  If you are looking for 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 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 - Manual for System Administrators*
  If you need to administer a CryptoServer PCIe plug-in 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 - Manual for System Administrators*
  If you need to administer a CryptoServer LAN (appliance), read this manual. Since a CryptoServer plug-in card is integrated into the CryptoServer LAN, please read the *CryptoServer - Manual for System Administrators*, as well.
- *CryptoServer LAN/CryptoServer - Troubleshooting*
  If problems occur while you are using a CryptoServer PCIe plug-in card or a CryptoServer LAN (appliance), read this manual.
- *CryptoServer LAN/CryptoServer*
  *PKCS#11 CryptoServer Administration Tool – Manual for System Administrators*
  If you need to administer the PKCS#11 R2 interface with the PKCS#11 CryptoServer Administration Tool (P11CAT), read this manual.
- *CryptoServer LAN/CryptoServer*
  *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*
  If you need to administer a CryptoServer PCIe plug-in 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 CSe 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 CSe 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 CSe 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 of this manual). Please have the delivery note and the device's serial number ready

## 1.5 Deliverables

The CryptoServer CSe deliverables include:

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

You can also use smartcards to administer the CryptoServer CSe. 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 CSe.

# 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 CSe 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 CSe sensors from deleting data by mistake.*
*Always keep these instructions handy, in a safe place.*

Do not attempt to repair the CryptoServer CSe in any way.

## 2.1 Moving and Storing

When moving and storing the device, follow these instructions:

- The CryptoServer CSe should only be moved and stored in its original packaging.
- 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 CSe 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, please ensure that the battery replacement time is not exceeded.
- Keep this Manual together with your CryptoServer CSe 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 CryptoSever CSe is installed 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 plug-in cards all series. We strongly recommend to remove the CryptoServer PCIe plug-in card from the computer prior to any planned transport or movement. All cryptographic keys stored on the plug-in card remain securely maintained during the transport or movement since the CryptoServer is continuously supplied with power by a battery.

## 2.2 Battery

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

*This battery is not rechargeable.*
*If the CryptoServer CSe 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

To ensure the safe transport of the CryptoServer plug-in card proceed as follows:

1. Check the battery state with the csadm command `GetBattState`.
   - Example on a Windows operating system:

     ```
     C:\>csadm Dev=PCI:0 GetBattState
     ```

   - Example on a Linux operating system:

     ```
     C:\>csadm Dev=/dev/cs2 GetBattState
     ```

   If the residual battery power is displayed as `ok`, for example,

   `Carrier Battery: ok (3.068 V)`,
   continue with step 3.

   If the residual battery power is displayed as `low`, for example,
   `Carrier Battery: low (2.650 V)`,
   continue with step 2.
2. Replace the battery by a new one (3 V, Lithium, FDK CR 12600 SE-T1 with soldering tags, or similar type). You will find step-by-step instructions on how to do that in chapter 6 of

the current document. Please note that this battery ensures the power supply of the CryptoServer CSe for at least six months.

3. Remove the CryptoServer plug-in card from the computer. Follow the instructions for removing PCIe plug-in cards as specified in the operating manual for your computer as well as the instructions in chapter 4.3 of the current document.
4. Put the CryptoServer plug-in card into an antistatic wrapping and in the original packaging. If you need an original packaging or/and antistatic wrapping, please contact the manufacturer Utimaco IS GmbH.
5. After reaching destination, put the computer, where the CryptoServer plug-in card should be installed in, to the required position, and then install the CryptoServer plug-in card. Follow the instructions for installing PCIe plug-in cards as specified in the operating manual for your computer as well as the instructions in chapter 4.2 of the current document.

## 2.4 Environmental Temperature

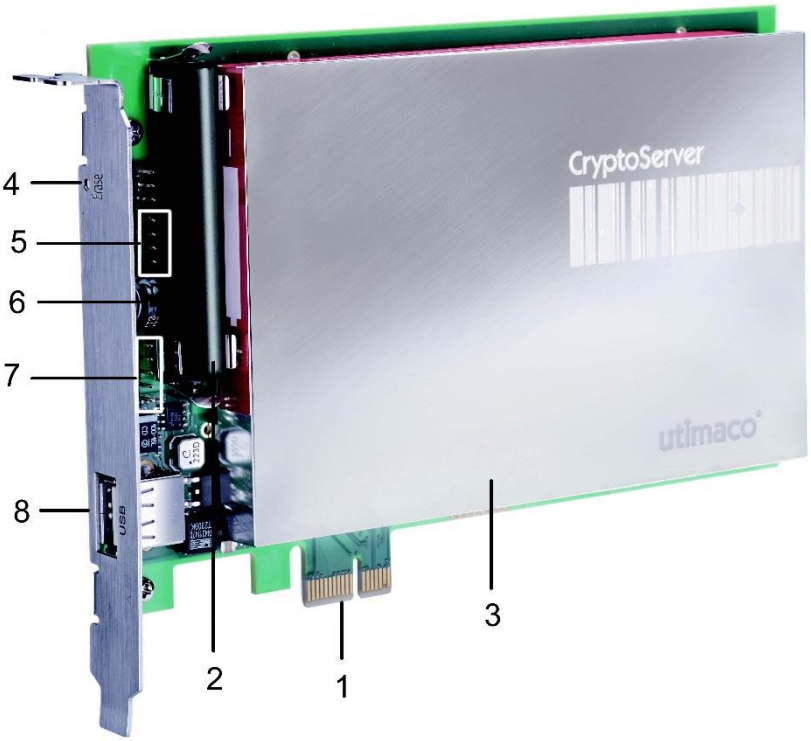
CryptoServer CSe must only be operated and stored in a particular temperature range.

- You must make sure that the CryptoServer CSe is always stored at temperatures between -10 °C and +55 °C (+14 °F to +131 °F).
- You must make sure that the CryptoServer CSe is always operated at temperatures between +10 °C and +35 °C (+50 °F to +95 °F).

*If the environmental temperature drops out of the permitted range, the device sensor will delete all the data on it.*

# 3 Components of the CryptoServer CSe (PCIe)

The CryptoServer CSe consists of the following components:




1 PCI Express bus (PCIe x1) of the CSe plug-in card

2 Battery
Supplies power to the sensors and quenching system when the computer is switched off

3 Encapsulated processor
The mechanical protection and the sensory prevent cryptographic data from being manipulated or extracted.

4 Erase pushbutton

5 Connector for an external battery, e.g., the external battery of CryptoServer LAN

6 Capacitor
Continues supplying power for approximately five minutes whilst the carrier battery is being replaced

7 USB connector (internal)
USB connector for additional USB 1.1 connection

8 USB port (external):
USB 1.1 port for peripheral devices such as a PIN pad

# 4 Unpacking and Handling

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

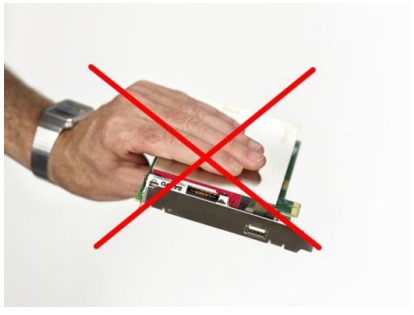
*The CryptoServer CSe is packaged in a special anti-static wrapping. Please retain this wrapping in case you need to store or transport the device.*
*The CryptoServer CSe must always be stored in this specific anti-static wrapping. This is because many other types of anti-static wrap are more conducting 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 CSe 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 CSe 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 CSe must not exceed 62 °C (143 °F). If it does, the device will switch off automatically. Consequently, you must ensure that the CryptoServer CSe is cooled to below this temperature.*
*To ensure that the internal temperature is not exceeded, the environmental temperature should not be more than 35 °C (95 °F).*

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

- The computer in which you want to install the CryptoServer CSe 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 CSe is installed lies in the computer's ventilation airstream.
- The CryptoServer CSe 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 CryptoServer CSe devices.

*If you cannot implement this configuration, we strongly recommend you install a PCIe slot cooling fan directly beside the CryptoServer CSe device.*

## 4.2 Installing the CryptoServer CSe

Follow the instructions for installing PCIe plug-in 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 the cables and open the computer casing.
2. Select a free PCIe expansion slot and remove the corresponding slot cover on the rear face of the computer.
3. Insert the CryptoServer CSe plug-in card in the computer's PCIe expansion slot. Make sure the card fits securely.
4. Close the case, reconnect the cables and then switch the computer on again.

## 4.3 Removing the CryptoServer CSe

You will need to remove the CryptoServer CSe to change its battery or to store or transport it.

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

1. Switch off the computer, unplug all the cables and open the computer casing.
2. Remove the CryptoServer CSe carefully from the PCIe slot. You must never use a tool (for example, screwdriver) to lever the card out of the slot.
3. Close the computer case and reconnect all the cables.

*Please note that the heat sink of the CryptoServer CSe 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 CSe.*

# 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 CSe 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

After you have installed the CryptoServer CSe, the next time you restart the host computer, the Windows operating system will recognize the new plug-in card and start the hardware installation wizard. The installation wizard guides you through the procedure for selecting and installing the driver.

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

- `CryptoServer.sys` (driver program)
- `CryptoServer.inf` (installation script for Windows 32-bit) or `CryptoServer_x64.inf` (installation script for Windows 64-bit)
- `cryptoserver.cat` (catalog file)

*You can find the files on the product CD in the following directory:*
*For 32-bit Windows operating system `Software\Windows\x86-32\Driver`.*
*For 64-bit Windows operating system `Software\Windows\x86-64\Driver`.*

### 5.1.1 Installing the Driver

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

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

1. Select the installation from the product CD supplied with the device.
2. Select one of the following directories on the product CD:

- For a 32 bit Windows operating system
  …\Software\Windows\x86-32\Driver
- For a 64 bit Windows operating system
  …\Software\Windows\x86-64\Driver

3. Click OK to confirm your selection.
4. Click Next.
   The driver installation starts. You will see a message that the driver has been signed by Utimaco IS GmbH.
5. Click on Installation.
   This installs the driver. You will then see a message saying that the driver has been installed successfully.
6. Click Close to close the installation wizard.
7. Open the Windows Device Manager. The CryptoServer CSe appears as the CryptoServer CSe-Series 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 CSe is functioning as it should, please follow these steps:

1. Use the Windows Start menu to select the Run option. Enter `cmd` in the window that now opens.
2. Click OK to open the command line window.
3. Input the following command sequence to start the csadm administration tool from the product CD to determine the status of the CryptoServer CSe. This assumes that your CD/DVD drive is the D: drive, and that you are using a 32-bit Windows operating system.
   `D:`

```
cd Software\Windows\x86-32\Administration
set CRYPTOSERVER=PCI:0
csadm GetState
```

If you are using a 64-bit Windows operating system please replace in the example above the path `Software\Windows\x86-32\Administration` by the path `Software\Windows\x86-64\Administration.`

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

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 39.8 [C]
alarm     = OFF
bl_ver    = 4.00.1.3          (Model: CSe-Series)
hw_ver    = 4.00.3.0
uid       = b0000011 0c310101                    |      1
adm1      = 43536531 30202020 43533539 30303032 | CSe10   CS590002
adm2      = 5554494d 41434f20 43533539 30303032 | UTIMACO CS590002
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

If you cannot communicate with the CryptoServer CSe, check that the PCIe plug-in card has been installed correctly and 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 CSe, please contact either the reseller who supplied this CryptoServer CSe or the Utimaco IS GmbH Customer Service team.

### 5.1.3 Updating the Driver

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

1. Open the Device Manager by using the Windows-Start menu > Control Panel > System > Device Manager.
2. Click with the right-hand mouse button on CryptoServer CSe-Series and select the context menu option Update Driver Software....
3. Select the option Browse my computer for driver software.
4. 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 of this manual.

### 5.1.4 Uninstalling the Driver

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

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

1. Open the Device Manager by using the Windows-Start menu > Control Panel > System > Device Manager.
2. Click with the right-hand mouse button on CryptoServer CSe-Series and select the context menu option Uninstall.
3. In the next window, click OK to confirm that you want to uninstall the driver.
4. Also select the option for deleting the driver software from your computer.
   The CryptoServer CSe driver will now be uninstalled and removed from your computer.
   After you close the wizard, the device CryptoServer CSe-Series is also deleted from the Device Manager display.
5. Shut down the Windows operating system before removing the CryptoServer CSe 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 Compiling/Installing the Driver

To compile the CryptoServer driver on a Linux operating system the following files are required:

- Source code of the CryptoServer driver
- Complete source code tree of the Linux kernel you are using

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

*To compile and install the driver for the Linux kernel please read and follow the instructions in the README file on the product CD in the* `…/Software/Linux/Driver` *directory.*

*You should have root permissions for performing the CryptoServer driver compilation/installation on a Linux operating system.*

### 5.2.2 Performing a Functional Test

To check that the driver has been installed correctly and that the CryptoServer CSe is working properly, follow these steps:

1. Open a command shell.
2. Change to your home directory with the `cd` command.
3. Go to the mount point for your CD-/DVD-ROM.
   The system may already have created it for you:
   `cd /media/cdrom or cd /media/cdrom0`

   If not, create it yourself:

   `mkdir /media/cdrom`
4. Input the following command sequence to start the csadm administration tool from the product CD to determine the status of the CryptoServer CSe. In the following example we assume that you are using a 32-bit Linux operating system.

   ```
   cd Software/Linux/x86_32/Administration
   export CRYPTOSERVER=/dev/cs2
   ./csadm GetState
   ```

   If you are using a 64 bit Linux operating system please replace the path
   `cd Software/Linux/x86_32/Administration` in the example above by the path
   `cd Software/Linux/x86_64/Administration`.

   If the driver has been installed correctly, and the CryptoServer CSe is working properly, you should see output that is similar to the following:

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 39.8 [C]
alarm     = OFF
bl_ver    = 4.00.1.3          (Model: CSe-Series)
hw_ver    = 4.00.3.0
uid       = b0000011 0c310101                    |      1
adm1      = 43536531 30202020 43533539 30303032 | CSe10   CS590002
adm2      = 5554494d 41434f20 43533539 30303032 | UTIMACO CS590002
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

If you cannot communicate with the CryptoServer CSe check that the PCIe plug-in card has been installed correctly and check if the driver has been installed correctly. After that, repeat the functional test.

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

### 5.2.3 Updating the Driver

If you want to upgrade the driver, proceed as follows:

1. Compile the new source code files into a kernel module called `cs2.ko`
2. Copy it into the following directory:
   `/lib/modules/<kernel version>/kernel/drivers/pci`.
3. Restart the system.

### 5.2.4 Uninstalling the Driver

Perform the following commands to uninstall the driver:

1. Unload the Kernel modul using the following command:
   `modprobe –r cs2`
2. Determine the Kernel Version using the following command:
   `uname -r`
3. Delete the `cs2.ko` kernel module, with this command:

   `rm /lib/modules/<kernel version>/kernel/drivers/pci/cs2.ko`
4. Delete the `cs2` device file, with this command:

   `rm /dev/cs2` or
   `rm /lib/udev/devices/cs2`
5. Delete the line `cs2` from the file `/etc/modules`.
6. Shut down the Linux operating system before removing the plug-in card.

# 6 Replacing the Battery

A battery ensures the sensor system and the quenching circuit can function even when the CryptoServer CSe is switched off.

If the CryptoServer CSe 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 CSe 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 CSe with power for at least six months.

*This battery is not rechargeable.*
*Depending on how frequently the CryptoServer CSe 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 CSe 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.

*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 12600SE-T1 batteries with soldering tags.

*Using the wrong batteries may cause an explosion. Utimaco IS GmbH accepts no responsibility for damage caused by any batteries other than those supplied by Utimaco IS GmbH.*
*Please ensure you dispose of spent batteries in accordance with the manufacturer's instructions and in an environmentally responsible manner.*

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

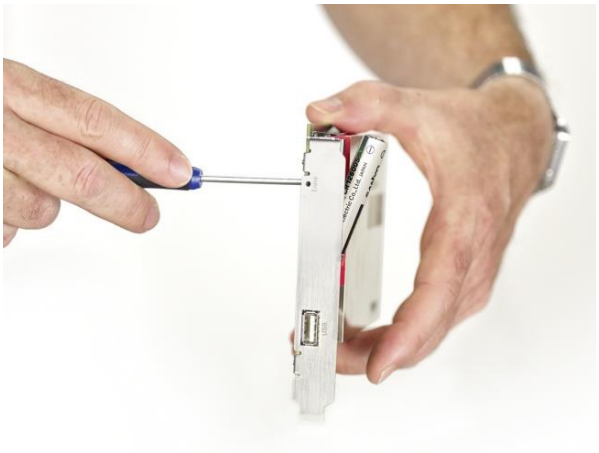
*Clean both battery contacts and the soldering tags with alcohol.*
*When performing the following steps, avoid touching the contacts with your fingers.*

3. Prepare a backup of your data, e.g., key and user databases, by using the CryptoServer administration tool you chose – csadm or CAT. Please read the *CryptoServer PCIe - Quick Start Guide* and the *CryptoServer - Manual for System Administrators* for further details.

*You find detailed information about the Installation of the csadm administration tool and the csadm commands in the "CryptoServer LAN/CryptoServer CryptoServer Command-line Administration Tool (csadm) Manual for System Administrators".*

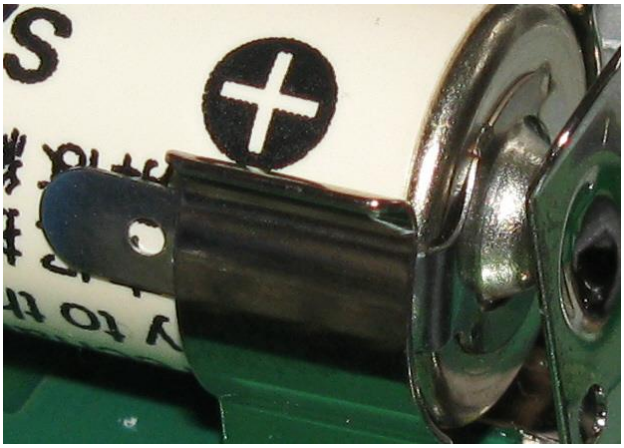
*You find detailed information about the installation and usage of the CryptoServer Administration Tool (CAT) in the "CryptoServer - Manual for System Administrators".*

4. Turn off the computer.
5. Remove the CryptoServer CSe from the computer.
6. On the reverse of the battery clips you will 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).



7. Change the battery.

*Make sure the polarity is correct (see the label on the CryptoServer CSe). If the polarity is incorrect, the data on the device will be deleted.*
*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 five minutes in which to replace the battery. During this period, a capacitor ensures the CryptoServer CSe 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 CSe is deleted.*

8. Reinstall the CryptoServer CSe.
9. Make a note of the next battery replacement date.
10. Turn on the computer.
11. Check the status of the CryptoServer CSe 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 sensory controller remained without power for long time.

Example output for `GetState`:

```
mode      = Maintenance Mode
state     = INITIALIZED (0x00100004)
temp      = 39.8 [C]
alarm     = ON
sens      = 02bf
          - Alarm has occurred
          - Power failed
bl_ver    = 4.00.1.3          (Model: CSe-Series)
hw_ver    = 4.00.3.0
uid       = b0000011 0c310101                   |      1
adm1      = 43536531 30202020 43533539 30303032 | CSe10   CS590002
adm2      = 5554494d 41434f20 43533539 30303032 | UTIMACO CS590002
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

12. 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:cyb:USB0 ResetAlarm
    ```

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

    Example with the csadm command `SetTime`:

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

Now, your CryptoServer CSe is ready for use again.

# 7 Disposing of the CryptoServer CSe

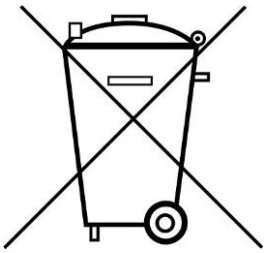
To dispose of your CryptoServer CSe, perform the following steps.

1. Perform an External Erase to securely delete all sensitive data from your CryptoServer. Refer to the *CryptoServer - Manual for System Administrators* manual for details.

   Of course, you also have the option of returning the CryptoServer CSe 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 CSe and the battery in an environmentally friendly way.

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

2. Remove the battery from the CryptoServer CSe 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 plug-in 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 CryptoServer CSe's battery 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:<br>Length: 167.65 mm ("half" length)<br>Height: 111.15 mm ("full" height) |
| Operating power | 3.3 V (PCIe bus specification) |
| Weight | 375 g |
| Battery | 3 V, Lithium, Ø 12 mm, L = 600 mm,<br>FDK CR 12600 SE-T1 with soldering tags, or similar type |
| Ports | PCIe x1<br>2 USB 1.1 |
| Environmental temperature | Operation: +10 °C to +35 °C (+50 °F to +95 °F)<br>Storage: -10 °C to +55 °C (+14 °F to +131 °F) |
| Humidity | 10 % to 95% relative humidity, non-condensing |
| MTBF | 350.000 hours (as specified in MIL-HDBK-217) |
| RoHS compliance | Yes |
| WEEE | National register for waste electric equipment (EAR)<br>DE39805015 |
| Conformity | Interference emission in accordance with EN 55022 Class B<br>Influence of interference in accordance with EN 61000-6-2 (industry)<br>Equipment safety in accordance with<br>IEC 60950-1:2001/EN 60950-1:2001 (CB scheme)<br>FCC 47 CFR Ch. 1 Part 15 Class B |

# 9 Contact Address for Support Queries

Please feel free to contact us if an error occurs while operating the CryptoServer CSe-Series plug-in card, or if you have any further questions on CryptoServer CSe.

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen
Germany

You can reach us from Monday to Friday 09.00 a.m. to 05.00 p.m., apart from public holidays and other customs days, under the following phone/fax number and e-mail address:

Phone: +49 (0) 241 1696-153
Fax: +49 (0) 241 1696-58153
e-mail: support-cs@utimaco.com

If you need to send the CryptoServer CSe-Series plug-in card back to the manufacturer, we request that you first send us an e-mail containing a short description of the problem, to this email address:

rma-cs@utimaco.com