

The Data Security Company

Utimaco SafeWare

www.utimaco.com

SafeGuard[®] CryptoServer PCI

Installation & Operating Manual

utimaco[®]
s a f e w a r e
a member of the Sophos Group

Print

Copyright 2009

Utimaco Safeware AG
A member of the Sophos Group
Germanusstr. 4
52080 Aachen

Phone +49 (0)241 / 1696-200

Fax +49 (0)241 / 1696-199

Internet www.utimaco.de

e-mail support-cs@utimaco.de

Document Version 1.7.3

Date 09-01-27

Status Released

Author Dieter Bong

All rights reserved 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 AG or be processed, reproduced or distributed using electronic systems.

The company Utimaco AG reserves the right to modify or amend the documentation at any time without prior notice. Utimaco AG assumes no liability for typographical errors and damages incurred due to them.

Table of Contents

1	Introduction	5
1.1	About this manual	5
1.2	Import- and export regulations	5
1.3	Transport damage.....	6
1.4	Deliverables	6
2	General safety advice	7
2.1	Moving and storing.....	7
2.2	Environmental temperature	8
2.3	Battery	8
3	Components of SafeGuard CryptoServer PCI	9
4	Unpacking and handling	10
4.1	General hints.....	11
4.2	Installation	11
4.3	Uninstallation.....	12
5	Driver installation	13
5.1	Windows XP / Server 2003 / Vista / Server 2008.....	13
5.1.1	Installing the PCI driver	13
5.1.2	Testing	14
5.1.3	Updating the PCI driver.....	15
5.1.4	Uninstalling the PCI driver.....	15
5.2	Linux-Kernel 2.4.....	16
5.2.1	Installing the PCI driver	16
5.2.2	Testing	17
5.2.3	Updating the PCI driver.....	18
5.2.4	Uninstalling the PCI driver.....	18
5.3	Linux Kernel 2.6	18
5.3.1	Installing the PCI driver	19
5.3.2	Testing	19
5.3.3	Updating the PCI driver.....	19
5.3.4	Uninstalling the PCI driver.....	20
5.4	Solaris	20
5.4.1	Installing the PCI driver	20
5.4.2	Testing	21
5.4.3	Updating the PCI driver.....	21

5.4.4	Uninstalling the PCI driver	22
6	Replacing the battery	23
7	Technical data.....	25

1 Introduction

Thank you very much for buying our security system, SafeGuard CryptoServer PCI. We hope that our product will meet your expectations. If you have any complaints or suggestions to improve it, please let us know.

1.1 About this manual

Utimaco Safeware AG reserves the right to modify or change this manual without prior notice. Utimaco Safeware AG is not liable for damage resulting from print or translation errors.

To make this manual easier to use, and to help you to refer to specific sections quickly, some passages in the manual have been marked with symbols.



These contain important safety information that you must follow.



These are additional notes or supplementary information.



This is an example

1.2 Import- and export regulations



The export and use of SafeGuard CryptoServer PCI outside the Federal Republic of Germany is subject to Germany's legal export regulations and requires an export license.

The import of SafeGuard CryptoServer PCI must comply with the legal or other regulations currently in force in the importing countries.

Please contact your national customs authorities for further information

1.3 Transport damage

By purchasing SafeGuard CryptoServer PCI 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 Safeware AG (the address and telephone number are given on page 2). Please have the delivery note and the device's serial number ready

1.4 Deliverables

SafeGuard CryptoServer PCI is delivered with:

- 1 SafeGuard CryptoServer PCI plug-in card
- 1 SafeGuard CryptoServer PCI Installations- & Betriebsanleitung (German)
- 1 SafeGuard CryptoServer PCI Installation & Operating Manual (this document)

Smartcards can optionally be used for the administration of SafeGuard CryptoServer PCI. Such smartcards are not part of the deliverables. You can order smartcards, and a pinpad needed for contacting these smartcards, at your reseller or at Utimaco Safeware AG.

2 General safety advice



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

The hardware security module SafeGuard CryptoServer PCI 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.



To ensure that the device can be operated safely, and to prevent the SafeGuard CryptoServer PCI sensors from deleting data by mistake, please read the safety instructions below carefully, before unpacking the device and bringing it into operation.

Always keep these instructions handy, in a safe place.

Do not perform any repair of SafeGuard CryptoServer PCI yourself.

2.1 Moving and storing

When moving and storing the device, please follow these instructions:

- SafeGuard CryptoServer PCI should only be moved and stored in its original packaging and antistatic foil.
- Do not subject the device to impacts and vibrations or any other physical events that may damage the packaging.
- Make sure that the ambient temperature for storage of the SafeGuard CryptoServer PCI is always in the range 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 (see section 6).
- Keep this Manual together with your SafeGuard CryptoServer PCI so that it is handy if you need to reinstall the device.

2.2 Environmental temperature

SafeGuard CryptoServer PCI must only be operated and stored in a particular temperature range:

- You must make sure that SafeGuard CryptoServer PCI is always stored at temperatures between -10° C and +55° C (+14° F and +131° F).
- The permitted temperature range for SafeGuard CryptoServer PCI when it is running is from +10° C to +35° C (+50° F to +95° F).



If the environmental temperature drops below, or exceeds, the permitted range, the device sensor will delete all the data on it. It is therefore essential that you also read the instructions about siting the device in section 2.1 and 4.1 below.

2.3 Battery

The SafeGuard CryptoServer PCI hardware security module has a 3V lithium battery. This battery powers the sensor and the quenching circuit when the computer is switched off. This battery can power SafeGuard CryptoServer PCI for at least 6 months.

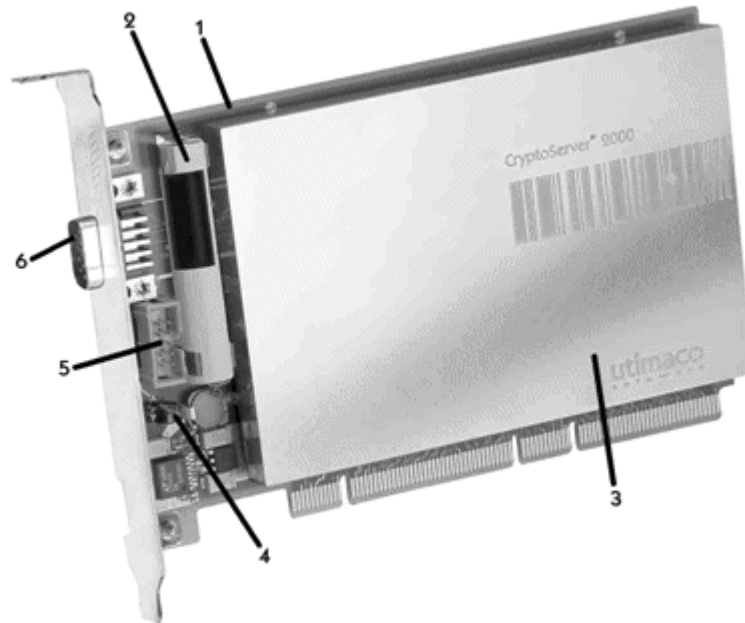


The battery must be replaced at regular intervals (see section 6). Otherwise all data inside the device may be deleted.

The battery is already in use at the time of delivery.

3 Components of SafeGuard CryptoServer PCI

The SafeGuard CryptoServer PCI plug-in card consists of the following components:



1. PCI carrier board:
32 Bit bus, 33/66 MHz.
2. Battery:
Supplies sensor and quenching circuit when computer is turned off.
3. Encapsulated processor:
Built-in sensor protects all cryptographic data from attacks and manipulation.
4. Capacitor:
Backs-up power supply during battery replacement for approx. 5 minutes.
5. Serial interface (internal):
Connection for internal smartcard reader or pinpad.
6. Serial interface (external):
Connection for peripheral devices, e.g. pinpad or terminal.

4 Unpacking and handling

SafeGuard CryptoServer PCI is equipped with a sensor that will delete all data inside the device in case of mechanical impact. A wrong manipulation during unpacking and installation can activate this sensor.

Ex works, SafeGuard CryptoServer PCI comes with cryptographic keys installed on it. The device can not be operated without them. Therefore, you should handle the SafeGuard CryptoServer PCI very carefully when unpacking and installing.

The SafeGuard CryptoServer PCI is equipped with a battery. This battery is already active during delivery, i.e. certain contacts and components of the PCI card are energized.



The SafeGuard CryptoServer PCI is packed in an antistatic foil. Keep the original package and antistatic foil for later transport or storage.

Other foils are often more conducting. Using such foils may cause short circuits between energized contacts and/or components. The SafeGuard CryptoServer PCI may therefore only be stored in its original antistatic foil.



Heed all relevant regulations for work on electrical equipment as well as all electrostatic protective measures during installation and uninstallation.

Take special care to follow the guidelines below.

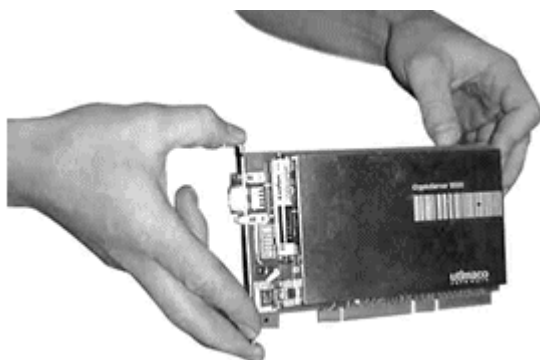


Never place the PCI card on a conducting surface (e.g. metal cover of a computer). This can cause a short circuit between energized contacts and/or components.

Take care to not touch the PCI card with any metal item (e.g. screwdriver or wedding ring). This can also cause a short circuit.

Do not touch any contacts on the card. Handle the SafeGuard CryptoServer PCI 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 hints

SafeGuard CryptoServer PCI is equipped with a sensor that detects whether it operates within the permissible temperature range (see 'Technical data' on page 25).



The internal temperature of SafeGuard CryptoServer PCI during operation may not exceed 55°C (131°F), since the device will otherwise automatically shut down.

This requires adequate cooling for SafeGuard CryptoServer PCI.

Therefore, heed the following installation hints:

- Select a cool and well ventilated site for the computer on which you want to operate the SafeGuard CryptoServer PCI.
- Avoid heat sources like heating's or direct sun light.
- Make sure that the plug-in card is located in the cooled air stream of the computer. Position the SafeGuard CryptoServer PCI only below heat-emitting PCI cards.
- Keep one slot free to heat-emitting PCI cards and to further SafeGuard CryptoServer PCI devices.



The implementation of a slot ventilator placed next to SafeGuard CryptoServer PCI is strongly recommended.

4.2 Installation

When installing SafeGuard CryptoServer PCI, heed all instructions on how to install PCI expansion cards given in the operating manual of your computer. The following steps only describe the general procedure:

- Turn off the computer, remove all cables and open the housing.
- Select a free PCI slot and remove the corresponding cover at the back of the computer.
- Insert the SafeGuard CryptoServer PCI card into a PCI slot of the computer. Make sure that the card locks properly.
- Close the housing, connect all cables and turn on the computer.

4.3 Uninstallation

In case of battery replacement, transport or storage, it may become necessary to uninstall the SafeGuard CryptoServer PCI.



When uninstalling, heed all instructions on how to uninstall PCI expansion cards given in the operating manual of your computer, as well as the instructions given in section 4.

- ◆ Turn off the computer, remove all cables and open the computer housing.
- ◆ Remove the SafeGuard CryptoServer PCI carefully out from the PCI slot. Do not lift out the card with some kind of object (e.g. screwdriver).
- ◆ Close the housing and reconnect all cables.

5 Driver installation

Driver for SafeGuard CryptoServer PCI are available for the following Operating Systems:

- Windows XP / Server 2003 / Vista / Server 2008, 32 bit and 64 bit Operating Systems
- Linux (Intel processor architecture, kernel versions 2.4 and 2.6)
- Sun Solaris 8 and higher / OpenSolaris (SPARC- and Intel-processor architecture)

The following sections describe the driver installation, test, update and uninstallation on the above mentioned Operating Systems.

5.1 Windows XP / Server 2003 / Vista / Server 2008

You need the following files to install or update the SafeGuard CryptoServer PCI driver:

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



For 32 bit Windows Operating Systems, these files can be found on the product CD in directory „Driver\Windows\wdm_x86_32“.

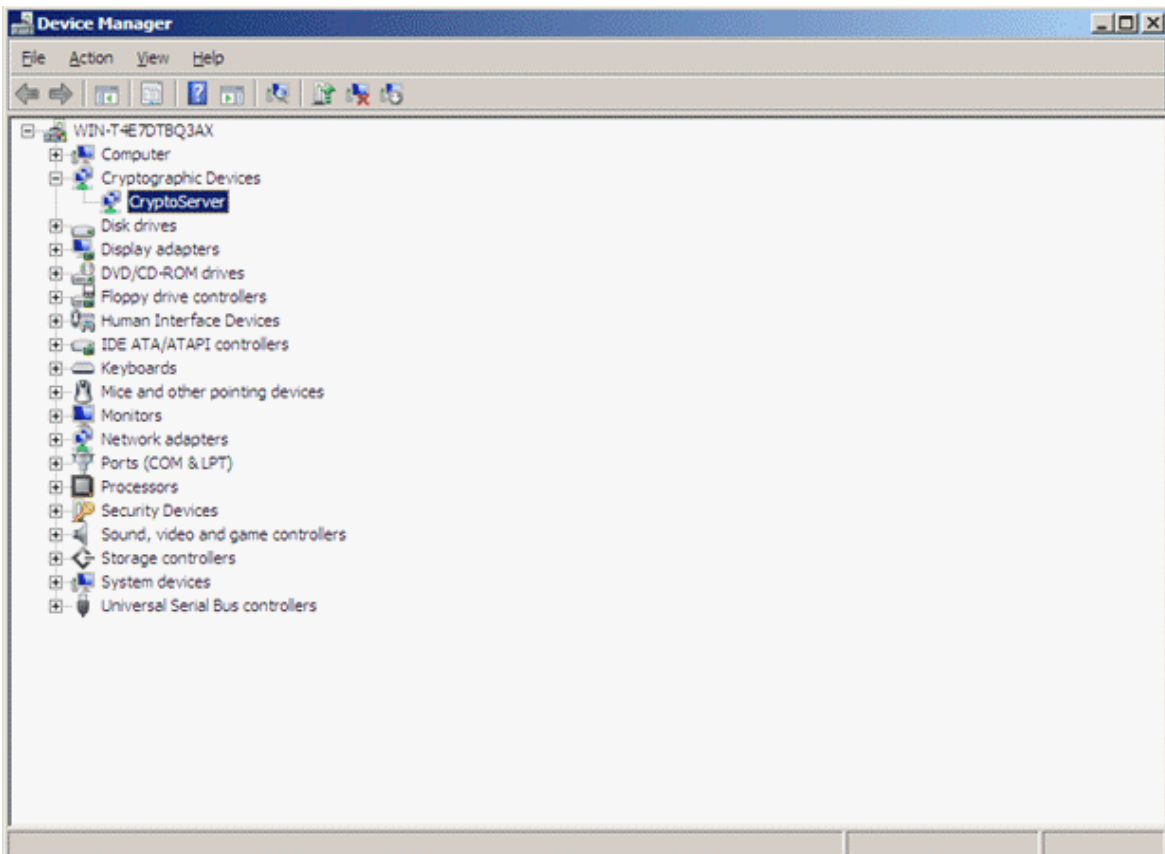
For 64 bit Windows Operating Systems, these files can be found on the product CD in directory „Driver\Windows\wdm_x86_64“.

5.1.1 Installing the PCI driver

Take the following steps for installation. Notice that the sequence of windows may slightly differ from below description depending on the exact Windows system.

- When first booting after SafeGuard CryptoServer PCI installation, Windows will detect the new PCI expansion card and launch the “Found New Hardware” wizard that will guide you through the installation.
- Do not search the Internet („Windows Update“) for a driver, but select to install the driver from the product CD.
- Choose the directory on the product CD „Driver\Windows\wdm_x86_32“ (when operating on a 32 bit Windows system) respectively „Driver\Windows\wdm_x86_64“ (when operating on a 64 bit Windows system).
- Drivers with a release date before January 1st, 2008 are not digitally signed. When installing such driver you will be notified that the driver is not digitally signed. Ignore this message and choose to install the driver anyway.
- Drivers with a release date after January 1st, 2008 are digitally signed. When installing such driver you will be notified that the driver is signed by Utimaco Safeware AG. Press <Install> to start driver installation.

- The driver is now being installed. Finally the successful installation will be reported, and you can close the hardware installation wizard.
- Open the Device Manager. SafeGuard CryptoServer PCI is shown as device „CryptoServer“ in device class „Cryptographic Devices“.



5.1.2 Testing

For testing the correct installation of the driver and functionality of the SafeGuard CryptoServer PCI, proceed as follows:

- From the Windows Start menu choose the option „Run“ and enter the command „cmd“. Launch the command shell by pressing <OK>.
- Execute the following sequence of commands to launch the administration program „csadm“ from the product CD and check the status of SafeGuard CryptoServer PCI. It is assumed here that your CD/DVD drive is identified by the drive letter „D:“.

```
D:
cd Software\Administration
cd csadm\Windows_x86_32
set CRYPTOSERVER=PCI:0
csadm getstate
```

You should receive an output similar to the following when the PCI driver was installed successfully and SafeGuard CryptoServer PCI is functional

```
CryptoServer is in Operational Mode
```

```
state      = 00000005 OPERATIONAL
temp       = 44,5 C°
alarm      = OFF
bl_ver     = 01000400
hw_ver     = 01000200
UID        = d8000008 c2cafe01 |
adm1       = 5554494d 41434f20 43533030 34373131 | UTIMACO CS004711
adm2       = 43727970 746f5365 72766572 00000000 | CryptoServer
adm3       = ffffffff ffffffff ffffffff ffffffff |
```

Should this not be the case, check again that the PCI card has been installed correctly. Do also consult the Windows Device Manager and check whether the PCI driver for the device „CryptoServer“ is correctly installed, and repeat the functional test.

In case you keep having problems, contact your reseller or the Utimaco support.

5.1.3 Updating the PCI driver

To update the driver, open the Windows Device Manager and select the device „CryptoServer“.

Choose the action “Update Driver Software...” from the menu „Action“ or from the context menu (right mouse click).

The further steps to select and install the new driver are the same as during the first driver installation (see section 5.1.1).

5.1.4 Uninstalling the PCI driver



Make sure to first uninstall the PCI driver before removing the SafeGuard CryptoServer PCI from your computer.

Uninstallation of the SafeGuard CryptoServer PCI driver is not anymore possible after removing the SafeGuard CryptoServer PCI from your computer!

Proceed as follows for uninstalling the PCI driver:

- ➔ Open the Windows Device Manager and select the device „CryptoServer“. Choose the action “Uninstall“ from the menu „Action“ or from the context menu (right mouse click).

- In the next window, press <OK> to confirm that you want to uninstall the PCI driver from your computer. Also choose the option to delete the driver software from your computer.
- The SafeGuard CryptoServer PCI driver is now being uninstalled and deleted from your computer. After termination of the uninstallation wizard, the device „CryptoServer“ is removed from the Device Manager list of devices.

To uninstall the SafeGuard CryptoServer PCI card, shut down the computer and uninstall the PCI card as described in section 4.3

5.2 Linux-Kernel 2.4

You need the following files to install or update the SafeGuard CryptoServer PCI driver:

- cs2.o



You need administrator privileges to install the PCI driver.

- Copy the kernel module 'cs2.o' into the directory '/lib/modules/2.4.n/misc' ('n' being the kernel patch level).
- Create a device file for SafeGuard CryptoServer PCI and assign the appropriate rights for his file:

```
mknod /dev/cs2 c 244 0
chmod 666 /dev/cs2
```

- Insert the following line in your '/etc/modules.conf' file:

```
alias char-major-244 cs2
```

5.2.1 Installing the PCI driver

Proceed as follows to install the PCI driver.



You need administrator privileges to install the PCI driver.

- Copy the kernel module 'cs2.o' into the directory '/lib/modules/2.4.n/misc' ('n' being the kernel patch level).
- Create a device file for SafeGuard CryptoServer PCI and assign the appropriate rights for his file:

```
mknod /dev/cs2 c 244 0
chmod 666 /dev/cs2
```

- Insert the following line in your `/etc/modules.conf` file:

```
alias char-major-244 cs2
```

5.2.2 Testing

Proceed as follows to test the correct installation of the driver and functionality of the SafeGuard CryptoServer PCI:

- Open a command shell, mount the CD/DVD drive with the product CD, and change to the root directory of the product CD.
- Execute the following sequence of commands to launch the administration program „csadm“ from the product CD and check the status of SafeGuard CryptoServer PCI.

```
cd Software/Administration
cd csdam/Linux_x86_32
export CRYPTOSERVER=/dev/cs2
csadm getstate
```

You should receive an output similar to the following when the PCI driver was installed successfully and SafeGuard CryptoServer PCI is functional:

```
CryptoServer is in Operational Mode
```

```
state      = 00000005 OPERATIONAL
temp       = 44,5 C°
alarm      = OFF
bl_ver     = 01000400
hw_ver     = 01000200
UID        = d8000008 c2cafe01 |
adm1       = 5554494d 41434f20 43533030 34373131 | UTIMACO CS004711
adm2       = 43727970 746f5365 72766572 00000000 | CryptoServer
adm3       = ffffffff ffffffff ffffffff ffffffff |
```

Should this not be the case, check again that the PCI card has been installed correctly. Do also consult the Windows Device Manager and check whether the PCI driver for the device „CryptoServer“ is correctly installed, and repeat the functional test.

In case you keep having problems, contact your reseller or the Utimaco support.

5.2.3 Updating the PCI driver

To update the PCI driver, copy the kernel module 'cs2.o' into the directory '/lib/modules/2.4.n/misc' ('n' being the kernel patch level). Perform a system reboot to load the new driver.

5.2.4 Uninstalling the PCI driver



Make sure to first uninstall the PCI driver before removing the SafeGuard CryptoServer PCI from your computer.

Perform the following commands to uninstall the PCI driver:

- Delete the kernel module 'cs2.o' and the device file '/dev/cs2'.

```
rm /lib/modules/2.4.n/misc/cs2.0 ('n' being the kernel patch
level)
rm /dev/cs2
```

- Remove the line 'alias char-major-244 cs2' from your '/etc/modules.conf' file.

To uninstall the SafeGuard CryptoServer PCI card, shut down the computer and uninstall the PCI card as described in section 4.3

5.3 Linux Kernel 2.6

Due to the architecture of the Linux 2.6 kernel it is unfortunately not possible to provide a ready-to-install driver.

For this reason, the source code of the SafeGuard CryptoServer PCI driver is being shipped on the product CD. For the compilation of the PCI driver on the target system you need the following files:

- Source code of the SafeGuard CryptoServer PCI driver
- Complete source code of your Linux 2.6 kernel



The source code of the SafeGuard CryptoServer PCI driver can be found on the product CD in directory „Driver\Linux\kernel_2.6“.

5.3.1 Installing the PCI driver



Compiling the driver and the Linux kernel requires special know-how.

Read the instructions in the kernel documentation under 'Documentation/kbuild/modules.txt' or ask your Linux guru.



You need administrator privileges to install the PCI driver.



- Compile the driver as kernel object 'cs2.ko'.
- Copy the kernel object 'cs2.ko' into the directory '/lib/modules/<kernel-version>/kernel/drivers/pci'.
- Create a device file for SafeGuard CryptoServer PCI:

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

- With newer Linux versions that use sysfs and udev, the directory '/dev' is a temporary file system. In this case the device file must not be created in directory '/dev' but in directory '/lib/udev/devices':

```
mknod /lib/udev/devices/cs2 c 244 0
```

- Set appropriate rights for the device file:

```
chmod 666 /dev/cs2 respectively  
chmod 666 /lib/udev/devices/cs2
```

Insert a line „cs2“ into the file '/etc/modules' to make sure that the driver is loaded with every system boot.

Either reboot the system, or manually load the driver with the following commands:

```
depmod -a -q  
modprobe cs2
```

5.3.2 Testing

Perform the test as described in section 5.2.2 to test the correct driver installation and functionality of the SafeGuard CryptoServer PCI.

5.3.3 Updating the PCI driver

To update the PCI driver, compile the new driver sources into a kernel module 'cs2.ko' and copy this kernel module into the directory '/lib/modules/<kernel-version>/kernel/drivers/pci'. Perform a system reboot to activate the new driver.

5.3.4 Uninstalling the PCI driver



Make sure to first uninstall the PCI driver before removing the SafeGuard CryptoServer PCI from your computer.

Perform the following commands to uninstall the PCI driver:

- Delete the kernel module 'cs2.ko'.

```
rm /lib/modules/<kernel-version>/kernel/drivers/pci/cs2.ko
```

- Delete the device file 'cs2'.

```
rm /dev/cs2 respectively  
rm /lib/udev/devices/cs2
```

- Delete the device file from the system.

```
rmmod cs2
```

To uninstall the SafeGuard CryptoServer PCI card, shut down the computer and uninstall the PCI card as described in section 4.3

5.4 Solaris

The SafeGuard CryptoServer PCI driver for Solaris is delivered as pre-compiled driver for Sparc processors (64 bit) and Intel processor architecture (32 bit).



The driver can be found on the product CD in directory „Driver\Solaris\sun4u“ (for Sparc processors) respectively “Driver\Solaris\i64pc” (for Intel processor architecture).

The installation script for the driver can be found on the product CD in directory „Driver\Solaris“.

5.4.1 Installing the PCI driver

Perform the following steps to install the PCI driver:

- Execute the shell script „Install.sh“ from the product CD, specifying the command line option „-i“ or „—install“. The shell script will copy the driver to the appropriate system directory, create a device file and load the driver.

5.4.2 Testing

Proceed as follows to test the correct installation of the driver and functionality of the SafeGuard CryptoServer PCI:

- Open a command shell, mount the CD/DVD drive with the product CD, and change to the root directory of the product CD.
- Execute the following sequence of commands to launch the administration program „csadm“ from the product CD and check the status of SafeGuard CryptoServer PCI.

```
cd Software/Administration
cd csdam/Solaris_sparc
export CRYPTOSEVER=/dev/cs2
csadm getstate
```

You should receive an output similar to the following when the PCI driver was installed successfully and SafeGuard CryptoServer PCI is functional:

```
CryptoServer is in Operational Mode
```

```
state      = 00000005 OPERATIONAL
temp       = 44,5 C°
alarm      = OFF
bl_ver     = 01000400
hw_ver     = 01000200
UID        = d8000008 c2cafe01 |
adm1       = 5554494d 41434f20 43533030 34373131 | UTIMACO CS004711
adm2       = 43727970 746f5365 72766572 00000000 | CryptoServer
adm3       = ffffffff ffffffff ffffffff ffffffff |
```

Should this not be the case, check again that the PCI card has been installed correctly. Do also consult the Windows Device Manager and check whether the PCI driver for the device „CryptoServer“ is correctly installed, and repeat the functional test.

In case you keep having problems, contact your reseller or the Utimaco support.

5.4.3 Updating the PCI driver

Perform the following steps to update the PCI driver:

- Execute the shell script „Install.sh“ from the product CD, specifying the command line option „-u“ or „—uninstall“. The shell script will uninstall the current driver.
- Execute the shell script „Install.sh“ from the product CD, specifying the command line option „-i“ or „—install“. The shell script will copy the new driver to the appropriate system directory and load the new driver.

5.4.4 Uninstalling the PCI driver



Make sure to first uninstall the PCI driver before removing the SafeGuard CryptoServer PCI from your computer.

Perform the following steps to uninstall the PCI driver:

- Execute the shell script „Install.sh“ from the product CD, specifying the command line option „-u“ or „—uninstall“. The shell script will uninstall the current driver.

To uninstall the SafeGuard CryptoServer PCI card, shut down the computer and uninstall the PCI card as described in section 4.3.

6 Replacing the battery

A battery ensures that the sensor and the quenching circuit are always working even when the SafeGuard CryptoServer PCI is not powered.

The SafeGuard CryptoServer PCI is powered via the PCI interface when being operated inside a computer. In this case the battery is not strained, but a partly discharged battery is not being recharged either.

When not being powered via its PCI interface (e.g. during storage or when the computer is powered off) the battery ensures powering of the SafeGuard CryptoServer PCI. The battery ensures the powering for at least 6 months, often even more than a year.



Depending on the operational time of the SafeGuard CryptoServer PCI the battery must be replaced in regular intervals.

In case that the battery is not replaced early enough, all data inside the SafeGuard CryptoServer PCI will be deleted!

Therefore the battery state has to be checked regularly. This can be done by executing the GetInfo command of the administration tool “csadm” (see “SafeGuard CryptoServer – Administration Guide“).



Make sure to carefully read the following directions before changing the battery. Heed all handling instructions described in section 4

- Before replacing the battery, make sure you have the right spare battery at hand (see ‘Technical data’ on page 25).



Replacing the battery by an incorrect type means risking an explosion! Utimaco Safeware AG is not liable for damage caused by incorrect battery types!

Dispose used batteries according to instructions!

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



Clean both battery contacts with alcohol. After that avoid touching the contacts with your fingers.

- Uninstall the SafeGuard CryptoServer PCI from your computer (see section 4.3).

- On the rear side of the battery clamps you will find two holes in the card. Plug a small screwdriver through one of these holes in order to remove the battery from the clamps (see figure below).



- Replace the battery.



*Observe the correct polarity (see sticker on the CryptoServer).
If the polarity is wrong, all data inside the device will be deleted!*



*You have a maximum of 5 minutes available to replace the battery. During this period, a capacitor maintains the power supply of the CryptoServer.
If you do not have inserted the new battery within this period, all data inside the CryptoServer will be deleted.*

- Reinstall the SafeGuard CryptoServer PCI (see section 4.2).
- Note the date for the next battery replacement.

7 Technical data

Dimensions	PCI plug in card: length: 167 mm ("half" length) height: 107 mm ("half" height)
Operating power	4,5 - 5,5 volts (PCI bus specification)
Power requirements	≤ 5 W
Battery	3 V, Lithium, Ø 12 mm, length 600 mm, Sanyo CR 12 600 SE or identical type, e.g. VARTA CR2NP
External interfaces	<ul style="list-style-type: none"> ■ PCI (32 bit, 33/66 MHz) ■ 2 serial V.24 interfaces
Environmental temperature	<ul style="list-style-type: none"> ■ In operation: +10° C to +35° C / +50° F to +95° F ■ In warehouse: -10° C to +55° C / +14° F to +131° F
Humidity	10 to 85 % relative humidity, non-condensing
MTBF	350,000 hours (in acc. with MIL-HDBK-217)
RoHS compliance	Yes
WEEE	Elektro-Altgeräte-Register DE39805015
Compliance	<ul style="list-style-type: none"> ■ Interference emission in accordance with EN 55022 Class B ■ Interference immunity in accordance with EN 61000-6-2 (Industrial environment) ■ Equipment safety in accordance with IEC 60950-1:2001 / EN 60950-1:2001 (CB scheme) ■ FCC 47 CFR Ch. 1 Part 15 Class B