Utimaco Safeware

www.utimaco.com

The Data Security Company

SafeGuard® CryptoServer LAN

Installation & Operating Manual

utimaco®
safeware
a member of the Sophos Group

Imprint

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	2.2.3
Date	01/19/2009
Status	Released
Author	Dieter Bong

Table of Contents

1 Introduction

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

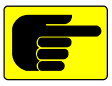
1.1 About this Operating Manual

Utimaco Safeware AG reserves the right to modify or change this Operating 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.

Important security advice that should always be followed.

Additional information.



Example.

1.2 Import and export regulations

The export and use of SafeGuard CryptoServer LAN outside the Federal Republic of Germany is subject to Germany's legal export regulations and requires an export license.
The import of SafeGuard CryptoServer LAN 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 LAN 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 LAN is delivered with:

- 1 SafeGuard CryptoServer LAN 19 inch appliance
- 1 power cable
- 1 PS/2 Y adapter for the mouse and keyboard, 1x6-pin mini DIN plug, 2x6-pin mini DIN socket, length 0.2m
- 1 SafeGuard CryptoServer LAN Installations- & Betriebsanleitung (German)
- 1 SafeGuard CryptoServer LAN Installation & Operating Manual (this manual)

The delivery may also include a pinpad and several smartcards, which are used to administer your SafeGuard CryptoServer LAN, depending on which product package you purchased.

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.

SafeGuard CryptoServer LAN has a hardware security module: SafeGuard CryptoServer PCI. This 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.

2.1 Moving and storing

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

- Before moving SafeGuard CryptoServer LAN, please ensure that the power supply cable has been pulled out of the socket and that all other connection cables have been removed from the other devices.
- SafeGuard CryptoServer LAN 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.
- If the device is to be stored for a longer time period, please ensure that the battery replacement time is not exceeded (see section 3).
- Keep this Manual together with your SafeGuard CryptoServer LAN so that it is handy if you need to reinstall the device.

2.2 Environmental temperature

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

- You must make sure that SafeGuard CryptoServer LAN is always stored at temperatures between -10° C and +55° C (+14° F and 131° F).
- The permitted temperature range for SafeGuard CryptoServer LAN when it is running is from +10° C to +30° C (+50° F to + 86° 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 2.3 below.

2.3 Siting the device

2.3.1 19 inch cabinet

Brackets are attached to either side of the device so that SafeGuard CryptoServer LAN can be installed in a 19 inch cabinet.

- Before it is installed in a 19 inch cabinet, SafeGuard CryptoServer LAN must be placed on rails that are strong enough to bear its weight. You must ensure that the device is evenly balanced and is placed squarely on the rails to ensure that it is stable. To ensure the weight is evenly distributed, do not stack too many devices on each set of rails. Find out what weight load the rails will bear.
- To install SafeGuard CryptoServer LAN in a 19 inch cabinet, simply attach the securing brackets to the cabinet.
- The temperature inside the 19 inch cabinet may be higher than the temperature outside the cabinet. This is particularly true if several devices are installed in the same cabinet. Please ensure that the temperature inside the 19 inch cabinet does not exceed the maximum permitted environmental temperature (see section 2.2).
- Take care that, when you install the device in a 19 inch cabinet, the ventilation slots are kept free to ensure that air circulates enough.

2.3.2 Desktop

If you do not want to install SafeGuard CryptoServer LAN in a 19 inch cabinet, please follow these instructions:

- Place the device on a secure, stable surface. Avoid impacts and blows to the device.
- Never operate SafeGuard CryptoServer LAN close to water or other liquids. Never spill liquid on the device.
- Do not place objects, articles of clothing or papers on the device itself.
- Protect SafeGuard CryptoServer LAN against humid or dusty environments, vibrations, extreme temperature variations and direct sunlight. Do not place the device next to heating units, air conditioning units, etc.
- Ensure that the maximum permitted environmental temperature is not exceeded (see section 2.2).
- Ensure adequate ventilation. Never install the device in a cabinet or similar object in which the circulation of air is impeded. The ventilation slots on the device must never be covered.
- Do not connect the device to sockets that are switchable or have timers.
- Avoid connecting the device to electrical circuits to which other power-hungry devices (such as motors, air conditioning units, photocopiers, etc.) are connected. This would put the device at risk of sudden power fluctuations.

2.4 Mains (grid) power supply and power supply cable

SafeGuard CryptoServer LAN is available with either alternating current (AC) or direct current (DC) power supply:

- SafeGuard CryptoServer LAN with alternating current power supply can be connected to mains (grid) voltage of 100 to 240V (AC).
- SafeGuard CryptoServer LAN with direct current power supply can be connected to mains (grid) voltage of -24 to -72V (DC).

Check the power voltage. Connecting SafeGuard CryptoServer LAN to the incorrect power voltage may destroy the device

- Check the electrical connection to the power circuit to ensure it will not be overloaded. Take note of the device performance data in section 6 in this Manual.
- Ensure that the device's electrical connection is properly earthed. If you connect several devices together, their total power consumption may exceed the total safe limit.
- Handle the power supply cable carefully. Always disconnect it by pulling on the plug, not on the cable itself. Pulling on the cable loosens the contacts and can cause problems.

- Protect the power supply cable against physical damage. Never place furniture or other heavy objects on the power supply cable and do not drop any sharp-edged or heavy objects on it.
- Do not tie knots in the power supply cable.

2.5 Opening the device

SafeGuard CryptoServer LAN must only be opened by the employees of Utimaco Safeware AG or certified sales partners.

If SafeGuard CryptoServer LAN is opened by someone else, instead of an employee of Utimaco Safeware AG or a certified sales partner, Utimaco Safeware AG accepts no warrenty for any damage caused by opening the device.
However, if there is an urgent need to open the device, it is essential that the power supply plug is removed from the socket before the device is opened.

To ensure that SafeGuard CryptoServer LAN cannot be opened without anyone noticing, there are three security seals on the device itself. The following information is given on these seals:

Breaking the seal invalidates the warrenty!
A broken seal represents a security risk!
Please inform the security operator.

- To avoid the risk of electrical shocks or fires, do not attempt to tamper with any components inside the device.
- Do not attempt to repair SafeGuard CryptoServer LAN in any way.
- If water, wires or other parts penetrate the device by accident, immediately disconnect the power supply cable and inform your dealer or Utimaco Safeware AG. If you continue using the device in this condition, you risk causing a fire or suffering an electrical shock.
- Do not insert any objects into the openings in the SafeGuard CryptoServer LAN casing because they may hit live components and cause a short circuit. This may result in a fire or a life-threatening electrical shock.
- Incorrect or improper use may seriously damage SafeGuard CryptoServer LAN.

2.6 Batteries

SafeGuard CryptoServer LAN contains two batteries. These ensure that no security-critical information is lost or deleted on the hardware security module when the device is switched off, or if operation is interrupted due to a power failure. Both batteries have a combined life of at least 2.5 years.

Using the wrong batteries may cause an explosion! Utimaco Safeware AG accepts no responsibility for damage caused by using any other batteries except the ones supplied by Utimaco Safeware AG!

2.6.1 Batteries in the battery compartment

The battery compartment behind the SafeGuard CryptoServer LAN's front flap contains one 3.6V lithium battery (size D) which is directly connected to the SafeGuard CryptoServer PCI hardware security module (see figure in section 3.3). This battery can power SafeGuard CryptoServer PCI for at least 2 years if the device is not connected to a mains (grid) power supply with the power supply cable.

This battery is already in use when the device is supplied.

Check the status of this battery at regular intervals. When the battery reaches a critically low power level, it must be replaced.

Section 4 describes how to check the battery status and replace it as required.

Customers are permitted to change these batteries.

2.6.2 Battery in the hardware security module

The SafeGuard CryptoServer PCI hardware security module has a 3V lithium battery. This battery powers the sensor and the quenching circuit when SafeGuard CryptoServer LAN is switched off and the battery in the battery compartment does not have enough power to supply the hardware security module. This battery can power SafeGuard CryptoServer PCI for at least 6 months.

The battery in the hardware security module must only be replaced by an employee of Utimaco Safeware AG or one of its certified sales partners!

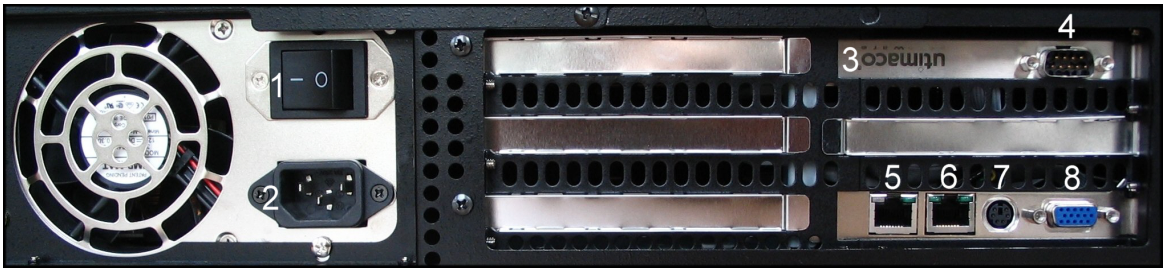
2.7 Cleaning

- Clean SafeGuard CryptoServer LAN with a soft, clean cloth dampened with a mild soapy solution. Then dry the device with a clean dry cloth.
- If the device has become wet, wipe it with a clean, dry, soft cloth.
- Never use benzene, solvents, alcohol or other aggressive substances to clean the device.

3 Installation

Before installing SafeGuard CryptoServer LAN, check whether all its parts are present. These include the parts described in section 1.4.

3.1 Sockets and ports on the rear face



1	Power supply switch (switches power on/off)
2	100-240V power supply socket
3	SafeGuard CryptoServer PCI hardware security module
4	External serial port on SafeGuard CryptoServer PCI for connecting peripheral devices such as a pin pad or log terminal
5	Ethernet connection 10/100/1000 (RJ45)
6	Ethernet connection 10/100 (RJ45)
7	Mouse and keyboard socket. The keyboard can only be used with a PS2/Y adapter.
8	VGA connector (screen)

*For SafeGuard CryptoServer LAN with direct current power supply, the power supply socket **2** has a different shape than shown above.*

3.2 Connections and operating elements on the front face

1	Display
2	PS2 power supply for pinpads. Can also be used as a keyboard connector (without PS2/Y adapter).
3	Serial port for SafeGuard CryptoServer LAN administration
4	Internal serial port for SafeGuard CryptoServer PCI.
5	Internal serial port for the second SafeGuard CryptoServer PCI (if present)
6	Light to show when the device is in operation
7, 8	Buttons for SafeGuard CryptoServer LAN menu control
9	Two USB 2.0 ports
10	Reset button
11	On/off switch
12	Floppy drive
13	Battery compartment

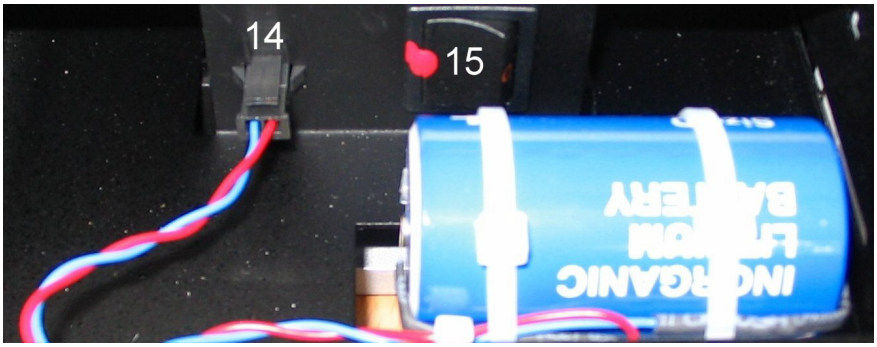
*The connections and operating elements **9** to **13** are located behind the front door on the right side of the front face.*

3.3 Connections and operating elements in the battery compartment

The battery compartment (**13**) can be pulled out to access the inner connections and operating elements.

Inside the battery compartment there is a plug **(14)** for the size D 3.6V lithium battery used by SafeGuard CryptoServer LAN (see section 2.6.1) to provide power to the sensor system and the quenching switch for when the device is switched off.

Behind this battery you will find a sealed delete switch (**15**).



If you press this switch (15) you will trigger the deletion procedure in the SafeGuard CryptoServer PCI hardware security module and all the security-critical information will be deleted.
The maintenance tasks then required to restore your system are not covered by the guarantee provided by Utimaco Safeware AG.

3.4 Using the menu control buttons

There are six menu control keys.

Key	Meaning
EXIT	Quits the menu level or menu item currently displayed
OK	This selects the menu level or confirms the menu item
1	Up (also known as the ↑ direction key)
2	Right (also known as the → direction key)
3	Down (also known as the ↓ direction key)
4	Left (also known as the ← direction key)

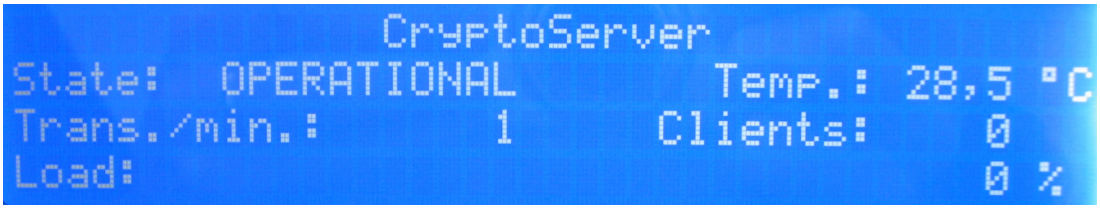
3.5 Installation

To install the device and bring it into operation, follow these steps:

- Install SafeGuard CryptoServer LAN in a 19 inch cabinet or put it in the place where you want to install it. When selecting this location, please bear in mind the notes in section 2.3.
- Connect the power supply socket **2** on the rear face of SafeGuard CryptoServer LAN to a 100 to 240 Volt power supply using the power supply cable supplied with the device.
- Connect the Ethernet port **5** on the rear face of the SafeGuard CryptoServer LAN to your network with a twisted pair cable (RJ45).
- Switch on the power switch **1** on the rear face of the SafeGuard CryptoServer LAN.
- Press the on/off switch **11** on the front of the device to switch on the SafeGuard CryptoServer LAN.

After a few seconds you will hear a short signal tone and see the first messages on the display panel **1** on the front of the device.

After approximately 30 seconds, SafeGuard CryptoServer LAN will be ready for use. You will see this status information on the display panel:



If the state shown is not "OPERATIONAL", please refer to the section on diagnosing errors in the "SafeGuard CryptoServer LAN User Manual".

The remaining configuration steps are described in the "SafeGuard CryptoServer LAN User Manual".

4 Maintenance

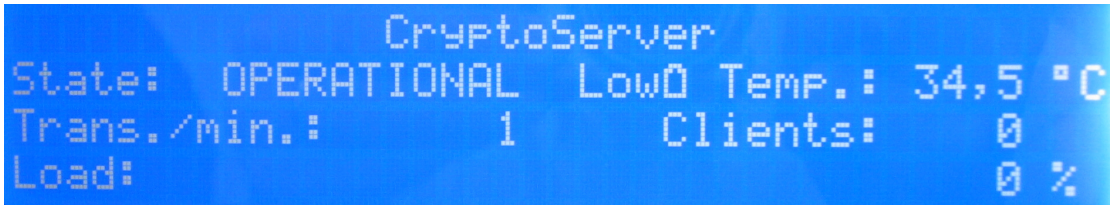
The only maintenance task that a customer is permitted to perform on the SafeGuard CryptoServer LAN is to check the power level of the battery in the battery compartment. When the battery reaches a critically low power level, it must be replaced.

Apart from this no maintenance tasks should be carried out on the SafeGuard CryptoServer LAN. However, if other maintenance work must be performed, such as replacing the second battery, which is directly connected to the SafeGuard CryptoServer PCI hardware security module, these tasks must only be carried out by an employee of Utimaco Safeware AG or a certified sales partner.

If you should open SafeGuard CryptoServer LAN for any other maintenance work, all warranty claims against Utimaco Safeware AG become null and void!

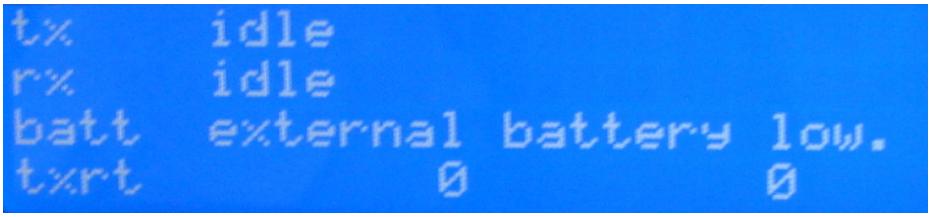
4.1 Checking the battery status

If the power level of the battery in the battery compartment and/or the battery on the hardware security module sinks below a critical level, a message appears on the SafeGuard CryptoServer LAN display panel: Between the state and temperature display you will then see the word "Low" and a battery icon.



To find out which of these batteries has reached this critical power level:

- Click OK.
- Select the "CryptoServer Administration" menu item and click OK.
- Use the ↓ direction key to go to the "Generic commands" menu item and then click OK.
- Use the ↓ direction key to go to the "Show driver info" menu item and then click OK.
- Use the ↓ direction key to scroll down in the display until you reach the line that starts with "batt".



If the message "batt …?" appears in this line it means that the system could not find out the battery status because the hardware security module's register is currently being accessed by someone else.
In this case, press the EXIT button and then repeat the "Show driver info" command.

If the message "batt external battery failed" appears in this line, it means that the power level of the battery in the battery compartment has sunk to a critical level.

- You must now replace this battery as described in section 4.2

If the message "batt carrier battery failed" appears in this line it means the power level of the battery on the hardware security module has sunk to a critical level.

- In this case, contact Utimaco Safeware AG or a certified sales partner and have them replace this battery.

If the message "batt carrier battery failed. external battery failed." appears in this line it means the power level in both batteries is at a critical level.

- You must now immediately, and whilst the device is in operation, replace the battery in the battery compartment as described in section 4.2. Then contact Utimaco Safeware AG or a certified sales partner and have them replace the battery on the hardware security module.

4.2 Replacing a battery

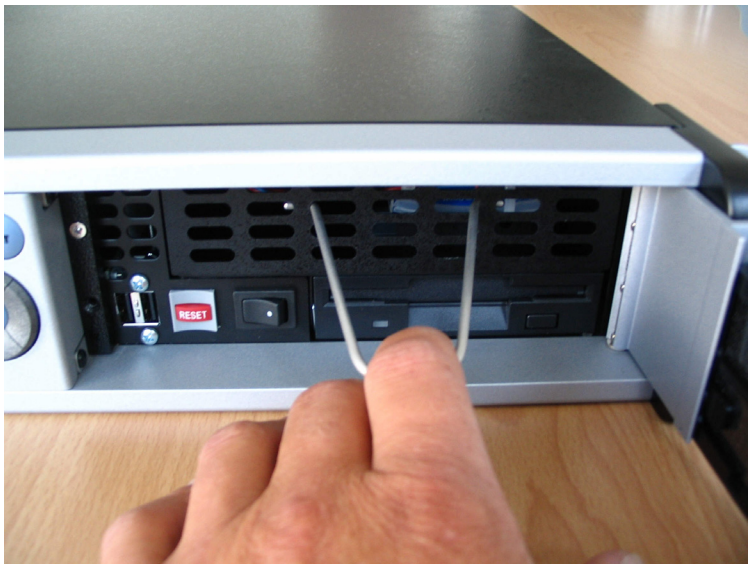
To replace the battery in the battery compartment you will need a battery replacement kit which you can purchase from Utimaco Safeware AG, and a wire cutter.

Using the wrong batteries may cause an explosion!
Utimaco Safeware AG accepts no responsibility for damage caused by using any other batteries except the ones supplied by Utimaco Safeware AG!
Please ensure you dispose of spent batteries in accordance with the manufacturer's instructions and in an environmentally responsible manner!

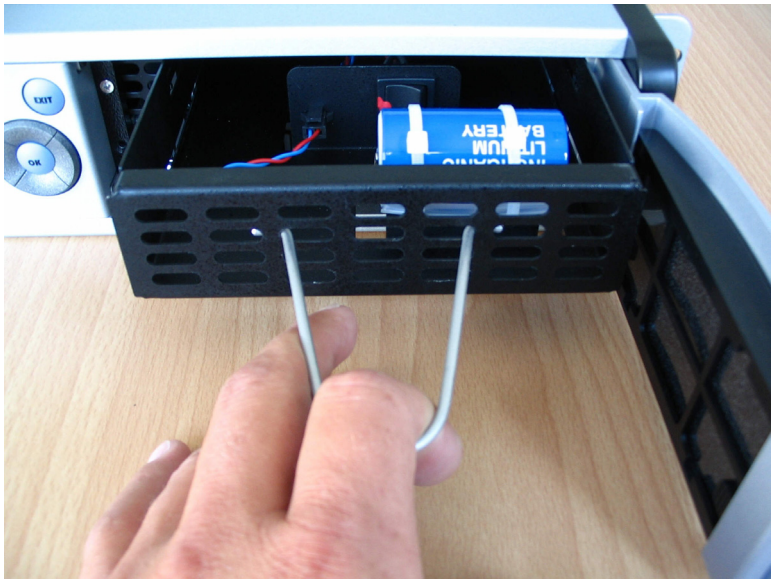
The battery replacement kit includes a 3.6 Volt lithium battery (with a connection plug) a cable holder and a metal hook that you use to open the battery compartment.

You should replace the battery whilst the device is running normally so that SafeGuard CryptoServer LAN will continue to be supplied with power.

- Open the flap on the front of SafeGuard CryptoServer LAN.
- Insert the ends of the hook in the holes in the battery compartment as shown in the next picture.

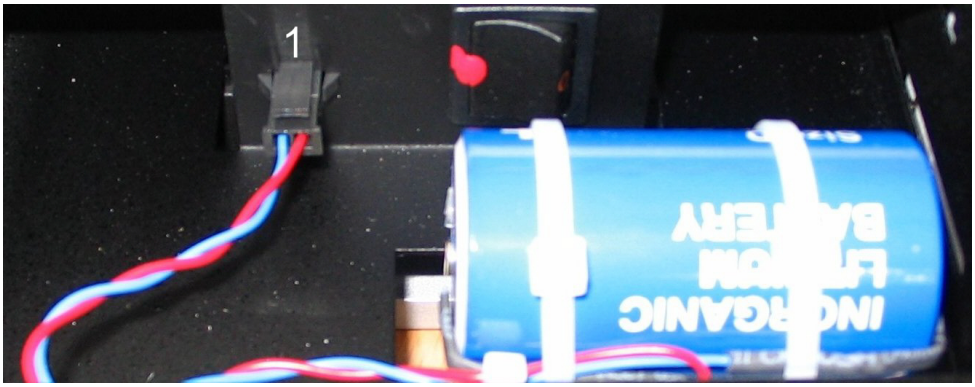


- Now carefully pull out the battery compartment.

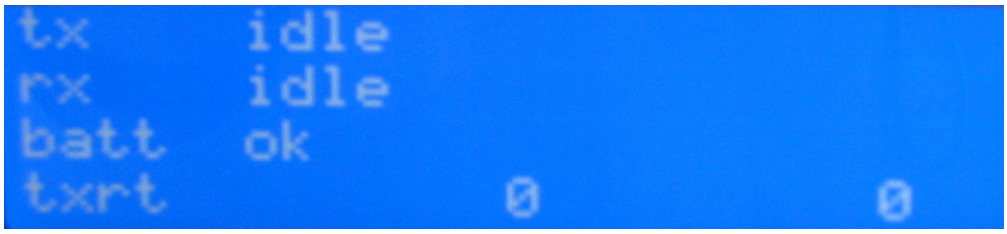


During the next steps, take great care not to touch the delete switch on the back wall of the battery compartment!

- Disconnect power supply plug **1** from the back wall of the battery compartment.



- Carefully disconnect the cable holder from the battery using the wire cutter.
- Remove the cable holder and then take the battery out of the compartment.
- Now place the new battery in the battery compartment. Guide the new cable holder through the two holes in the battery compartment again and pull it gently to secure it.
- Push power supply plug **1** for the new battery into the socket on the back wall of the battery compartment.
- Close the battery compartment.
- As the battery status message on the SafeGuard CryptoServer LAN display panel is now updated very often, check the status of the new battery with the "Show driver Info" command as described in section 4.1. The battery status will now appear as "batt ok".



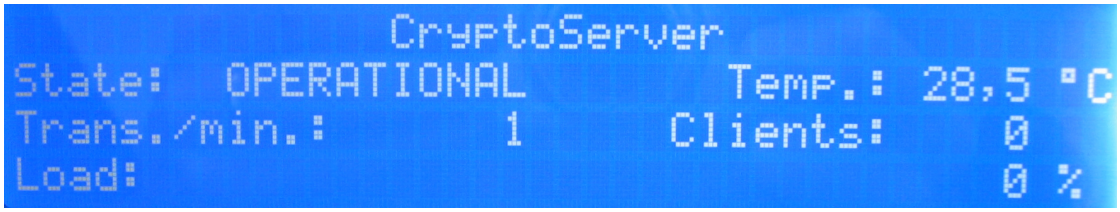
However, if the message is still "batt external battery failed.", check that the new battery has been connected correctly.

After a while, the message "Low" and the battery icon will disappear from the SafeGuard CryptoServer LAN display panel.

5 Switching off the device

Before you switch off SafeGuard CryptoServer LAN, please close down all the applications that access it.

The following status message in the display panel is the reference point for the next steps. If you are currently working in a particular menu level or an input screen, quit this by pressing the **EXIT** button. You may need to do this several times.



Then use the menu control to switch off SafeGuard CryptoServer LAN as follows:

- Click **OK.**
- Select the "CryptoServer Administration" menu item and click **OK**.
- Use the ↓ direction key to go to the "Shut down" menu item and then click **OK**.
- Use direction key ← to select "Yes" and then click **OK**. This shuts down the device.

When the device is switched off, the message in the display panel disappears. If you want to switch off SafeGuard CryptoServer LAN completely, switch off the power supply switch **2** on the rear face of the device.

The SafeGuard CryptoServer LAN should be kept running constantly to prevent the batteries from being used.
If a system is not running over a long period, the batteries will be used up. After a while this can result in the hardware security module not being supplied with power any more, and all data will be deleted. The resulting maintenance tasks are not covered by Utimaco Safeware AG's guarantees.
On the other hand, a brief break in the power supply (if the device is being moved around etc.) places no serious demands on the batteries and consequently there is no danger of data and setting etc. being deleted.

6 Technical Data

Dimensions	Height	88 m (2 heigths units)	
	Width	446 mm excluding attachment bracket (19 inch)	
	Depth	510 mm excluding handles	
Weight	13 kg		
Operating power	AC power supply: 100~240 VAC, 47~63 Hertz AC		DC power supply: -36 ~ -72 VDC
Operating power load	AC power supply: max. 8A / 4A at 100V / 240V		DC power supply: max. 25A / 10A at -36V / -72V
Power requirement	AC power supply: max. 960 W (4A at 240V)		DC power supply: max. 900 W (25A at -36V)
Effective / apparent power	AC power supply: Typical 76 W / 82 VA		DC power supply: Typical 76 W / ----
Interfaces on the front face	1 x PS2	power supply socket for pin pad and/or keyboard	
	3 x DB9	1 serial port for SafeGuard CryptoServer LAN (labeled “COM”) 1 serial port for SafeGuard CryptoServer PCI (labeled “CS1”) 1 serial port not used (labeled “CS2”)	
	2 x USB	USB 2.0 ports	
Interfaces on the rear face	1 x PS2	combined mouse/keyboard port	
	1 x DB15HD	VGA connector (screen)	
	1 x RJ45	10/100/1000 MBit Ethernet	
	1 x RJ45	10/100 MBit Ethernet	
	1 x DB9	1 serial port for SafeGuard CryptoServer PCI	
Removable storage medium	Floppy drive	3½ inch, 1.44 Mb, DOS-formatted floppy disks	
Environmental temperature	in operation	+10° C to +30° C (+50° F to + 86° F)	
	in warehouse	-10° C to +55° C (+14° F to 131° F)	
Humidity	10 to 85% relative humidity, non-condensing		
MTBF	110,000 hours at 25°C (in acc. with MIL-HDBK-217)		
RoHS compliance	Yes		
WEEE	Elektro-Altgeräte-Register DE39805015		
Conformity	Interference emission in accordance with EN 55022 Class B, EN 61000-3-2, EN 61000-3-3 Interference immunity in accordance with EN 55024 Equipment safety in accordance with IEC 60950-1:2001/ EN 60950-1:2001 (CB scheme) FCC 47 CFR Ch. 1 Part 15 Class B UL		

7 EC Declaration of Conformity

EG-KONFORMITÄTSERKLÄRUNG

Für das folgend bezeichnete Erzeugnis

Produktkategorie: Informationstechnische Einrichtung
Produkttyp: Industrie-Computer

Produktname: MAYFLOWER-ID Utimaco CryptoServer LAN

wird hiermit bestätigt, dass es den Anforderungen entspricht, die in der Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten über die elektromagnetische Verträglichkeit (89/336/ EWG), die Niederspannungsrichtlinie (73/23EWG) und die CE-Kennzeichnung (93/23/EWG), festgelegt sind.

Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

DIN EN 55022, Rev.:2003-09 (IEC/CISPR 22:1997 + A1:2000 + A2:2002); EN 55022:1998 + Corrigendum Juli 2003 + A1:2000 + Corrigendum April 2003 + A2:2003 Klasse/Class B

DIN EN 55024, Rev.:2003-10 (IEC/CISPR 24:1997, Corrigendum +A1:2001 + A2:2002); EN 55024:1998 + A1:2001 + A2:2003

DIN EN 61000-4-2, Rev.:2001-12, (IEC 61000-4-2:1995 + A1:1998 + A2:2000); EN 61000-4-2:1995 + A1:1998 + A2:2001

DIN EN 61000-4-3, Rev.:2003-11 (IEC 61000- 4-3:2002 + A1:2002); EN 61000-4-3:2002 + A1:2002

DIN EN 61000-4-4, Rev.:2002-07, (IEC 61000-4-4:1995 +A1:2000 + A2:2001)

DIN EN 61000-4-5, Rev.:2001-12, (IEC 61000-4-5:1995 + A1:2000); EN 61000-4-5:1995 + A1:2001

DIN EN 61000-4-6, Rev.:2001-12, (IEC 61000-4-6:1996 + A1:2000); EN 61000-4-6:1996 + A1:2001

DIN EN 61000-4-8, Rev.:2001-12 (IEC 61000-4-8:1993 + A1:2000); EN 61000-4-8:1993 + A1:2001

DIN EN 61000-4-11, Rev.:2005-02 (IEC 61000-4-11:2004); EN 61000-4-11:2004

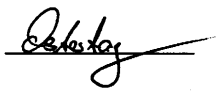
Zur Beurteilung des Erzeugnisses hinsichtlich der Gerätesicherheit wurden folgende Normen herangezogen:

DIN EN 60950: A11: 1997
DIN VDE 0805: 11/93
IEC 950: 1991 modifiziert

Diese Erklärung wird verantwortlich für den Hersteller

InoNet Computer GmbH
Bajuwarenring 19
D-82041 Oberhaching

abgegeben durch Ralph Ostertag
Geschäftsführer



Oberhaching, den 14.07.2005

Systemdokumentation MAYFLOWER-ID - 1 -