CryptoServer LAN V4

Operating Manual

utimaco®

Imprint

Copyright 2017	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen 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	1.2.3
Date	2017-02-08
Status	Final
Document No.	M012-0002-en

Table of Contents

1 Introduction

Thank you for purchasing our CryptoServer LAN V4 security system (referred to below also as CryptoServer LAN). We hope you are satisfied with our product. Please do not hesitate to contact us if you have any questions 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 LAN 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 LAN with an integrated CryptoServer CSe- or Se-Series Gen2 into service and administer it.

1.1.2 Contents of This Manual

After the introduction this manual is divided up as follows:

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

Chapter 3 shows the different ports, interfaces and operating elements on the front and rear side of the CryptoServer LAN, and provides a general description of the procedure for bringing the CryptoServer LAN into service.

Chapter4 contains the maintenance tasks that a customer is permitted to perform on the CryptoServer LAN, i.e., to check the power level of the batteries (carrier battery and external battery) and, if necessary, to change the external battery in the battery compartment, as well as to remove/swap a power supply module.

Chapter 5 provides instructions on how to switch off the CryptoServer LAN.

Chapter 6 gives information about what needs to be taken into account when disposing of the CryptoServer LAN.

Chapter 7 is an overview of the essential technical data of the CryptoServer LAN with AC power supply.

Chapter 8 is an overview of the essential technical data of the CryptoServer LAN with DC power supply.

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

1.1.3 Document Conventions

We use the following conventions in this manual:

Convention	*Usage*	*Example*
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file `example.conf` in the `/exmp/demo/` directory.
Italic	References and important terms	See Chapter 3, "Sample Chapter" in the *CryptoServer LAN/CryptoServer CryptoServer Command-line Administration Tool -csadm -Manual for System Administrators*.

Table 1: Document conventions

We use special 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 Gen2

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

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

We provide the following manuals on the product CD for the CryptoServer PCIe CSe- and Se-Series Gen2 plug-in cards and for the CryptoServer LAN (appliance) CSe- 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\`. From version 4.01.0 of the SecurityServer product CD they are only provided in English.

- *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.

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 LAN outside Germany is subject to the legal foreign trade regulations of the Federal Republic of Germany and require the appropriate authorization.
The import of CryptoServer LAN is subject to the legal requirements or other regulations that apply in the particular destination (import license)
Please contact your own national customs authorities for more detailed information.

1.4 Damage in Transit

By purchasing the 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 (the e-mail address and telephone number are given in

Chapter 9 of this manual). Please have the delivery note and the serial number of the device at hand.

1.5 Deliverables

The CryptoServer LAN deliverables include:

- one CryptoServer LAN V4
- two power supply cables
- one *CryptoServer LAN V4 Operating Manual* (this manual)
- one PIN pad
- ten smartcards for administering the CryptoServer LAN V4

2 General Safety Instructions

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

The CryptoServer LAN includes a CryptoServer CSe- or Se-Series Gen2. If the predefined limit values for its internal temperature are exceeded (or not reached), an alarm will be triggered and all the data on the CryptoServer will be deleted.

Before unpacking the device and bringing it into operation, please read the safety instructions below carefully to ensure that the device can be operated safely. 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 the CryptoServer LAN, ensure that the power supply cables have been pulled out of the sockets and that all other connection cables have been unplugged from the other devices.
- CryptoServer LAN should only be moved and stored in its original packaging.
- You must make sure that CryptoServer LAN is always stored at temperatures between -10 °C and +55 °C (+14 °F to +131 °F).
- 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, ensure that the battery replacement time is not exceeded.
- Keep this manual together with your CryptoServer LAN so that it is handy if you need to reinstall the system.

2.2 Environmental Temperature

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

- You must make sure that CryptoServer LAN is always stored at temperatures between -10 °C and +55 °C (+14 °F to +131 °F).
- You must make sure that CryptoServer LAN with an integrated CryptoServer Se-Series Gen2 PCIe plug-in card is always operated at temperatures between +10 °C and +50 °C (+50 °F to +122 °F).
- You must make sure that CryptoServer LAN with an integrated CryptoServer CSe-Series PCIe plug-in card is always operated at temperatures between +10 °C and +40 °C (+50 °F to +104 °F).

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

2.3 19" Rack

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

- You can use slide rails for the installation of the CryptoServer LAN in a 19" rack which you can purchase from the manufacturer Utimaco.
- To install CryptoServer LAN in a 19" rack, simply attach the securing brackets to the 19" rack.
- The temperature inside the 19" rack may be higher than the temperature outside the 19" rack. This is particularly true if several devices are installed in the same 19" rack. Please ensure that the temperature inside the 19" rack does not exceed the maximum permitted environmental temperature.
- Take care that, when you install the device in a 19" rack, the ventilation slots are kept free to ensure that air circulates enough.

2.4 Desktop

If you do not want to install CryptoServer LAN in a 19" rack, please follow these instructions:

- Place the device on a secure, stable surface. Avoid impacts and blows to the device.

- Never operate 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 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.
- 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.

This device has not been designed for use at a workstation within the user's field of vision. To avoid disturbing reflections, do not place this product at a workstation directly in the field of vision.

2.5 Power Supplies and Power Supply Cables

The CryptoServer LAN is equipped with two redundant power supplies. Please find further technical details in Chapter 7 and Chapter 8 of the current document.

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

Connect the two power cables to two different power circuits. This ensures that the CryptoServer LAN remains in operation continuously even if one of the power circuits fails.

- Check the electrical connections to the power circuits to ensure they will not be overloaded.
- 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 cables carefully. Always disconnect them by pulling on the plugs, not on the cables themselves. Pulling on the cables loosens the contacts and can cause problems.
- Protect the power supply cables against physical damage. Never place furniture or other heavy objects on the power supply cables and do not drop any sharp-edged or heavy objects on it.
- Do not tie knots in the power supply cables.

2.6 Opening the Device

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

If the CryptoServer LAN is opened by someone else, instead of an employee of Utimaco or a certified sales partner, Utimaco accepts no liability 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 plugs are removed from the sockets before the device is opened. Before opening the device please contact your reseller or directly us, the manufacturer Utimaco (please see Chapter 9 for contact details). Please have the delivery note and the serial number of the device at hand.

To ensure that CryptoServer LAN cannot be opened without anyone noticing, there are holographic security seals on the device itself.

- 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 CryptoServer LAN in any way.
- If water, wires or other parts penetrate the device by accident, immediately disconnect the power supply cables and inform your dealer or Utimaco IS GmbH. If you operate the device in this condition, you risk either causing a fire, or electrical shocks.
- Do not insert any objects into the openings in the 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 CryptoServer LAN.

2.7 Batteries

The CryptoServer LAN contains two batteries. These ensure that no security-critical information is lost or deleted in the CryptoServer when the device is switched off, or if operation is interrupted due to a power failure. The external battery is located in the battery compartment of the CryptoServer LAN. The carrier battery is placed on the CryptoServer plug-in card.

These batteries are not rechargeable.
Using the wrong batteries may cause an explosion! Utimaco IS GmbH accepts no liability for damage caused by using any other batteries except the ones supplied by Utimaco IS GmbH.

2.7.1 External Battery in the Battery Compartment

The external battery placed in the battery compartment behind the front door of the CryptoServer LAN is a 3.6 V lithium battery (size A) which is directly connected to the CryptoServer.

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

The external battery provides a guaranteed power supply for the CryptoServer for at least 1½ years if the device is not supplied with power via the power cables.
Check the status of this battery at regular intervals. When the battery reaches a critically low power level, it must be replaced.

Customers are permitted to change the external battery as described in Chapter 4.2 of this manual.

2.7.2 Carrier Battery of the CryptoServer

On the CryptoServer plug-in card which is integrated into the CryptoServer LAN there is a 3 V lithium battery – the carrier battery. It powers the sensor and the erase circuit when CryptoServer LAN is switched off and the external battery in the battery compartment does not have enough power to supply the CryptoServer.

The carrier battery can power the CryptoServer for at least six months.
The carrier battery must only be replaced by an employee of Utimaco or one of its certified sales partners.

2.8 Cleaning

- Clean 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, thinner, alcohol or other aggressive substances to clean the device.

3 Bringing into Service

Before you start up CryptoServer LAN, check whether all parts that belong to the delivery, as listed in Chapter 1.5 of this manual, are present.

3.1 Ports and Interfaces on the Rear Side (AC Power Supply)

The CryptoServer LAN V4 with AC power supply might be supplied with slightly different ports and interfaces on the rear side as shown in the following two figures, while the front panel remains the same as in Figure 7 resp. Figure 9.

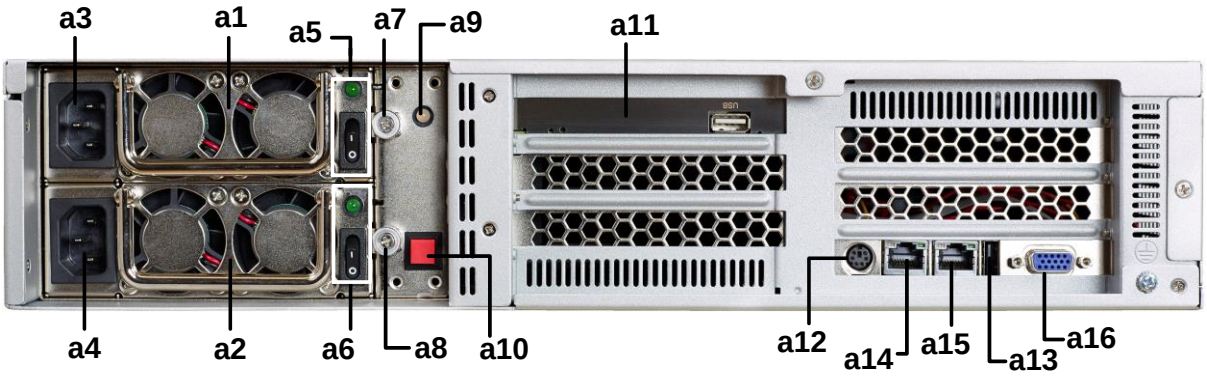


Figure 1: CryptoServer LAN V4 (AC) – Sockets and ports on the rear side (variant b)

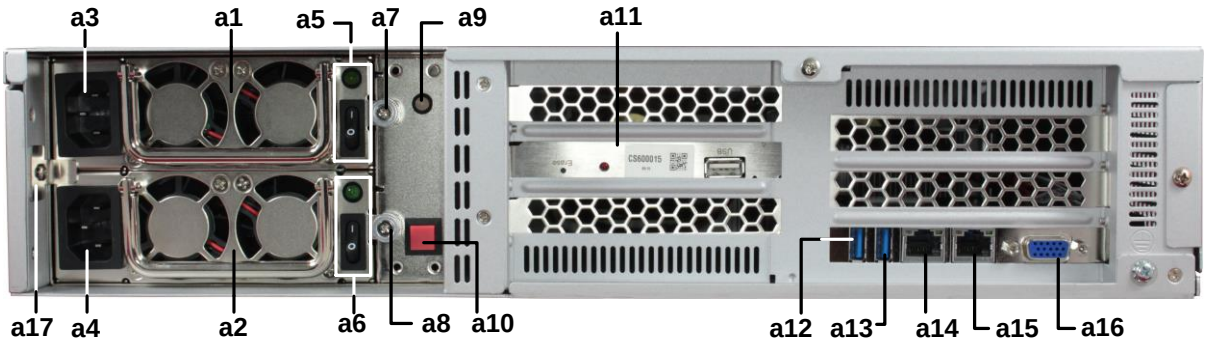


Figure 2: CryptoServer LAN V4 (AC) – Sockets and ports on the rear side (variant c)

Port/Interface	*Description*
	CryptoServer LAN V4 (Figure 1 and Figure 2)
a1, a2	Power supplies
a3, a4	Power supply sockets 90 V ~ 246 V (AC)
a5, a6	Power supply switches (switches power on/off) plus control light (green) above
a7, a8	Screws for attaching the power supplies
a9	Control light for the operation status of both power supplies: ■ green – normal operation ■ red – alarm status if a power supply fails or is switched off; A signal tone sounds.
a10	Mute key for the signal tone that sounds if a power supply fails or is switched off
a11	CryptoServer CSe-Series or Se-Series Gen2 plug-in card ■ CryptoServer CSe-Series plug-in card

Figure 3: CryptoServer CSe – Sockets and ports on the rear side

- ▣ A – Erase pushbutton
- ▣ B – USB 2.0 port of the CryptoServer CSe

■ CryptoServer Se-Series Gen2 plug-in card

Figure 4: CryptoServer Se-Series Gen2 – Sockets and ports on the rear side

- ▣ C – Erase pushbutton
- ▣ D – LED flash light – indicates the activation of the Erase push-button
- ▣ E – USB 2.0 port of the CryptoServer Se-Series Gen2

Port/Interface	*Description*
a14	**eth1** - Ethernet port 10/100/1000 (RJ45)
a15	**eth0** - Ethernet port 10/100/1000 (RJ45)
a16	VGA connector (screen)
	CryptoServer LAN V4 in Figure 1
a12	PS/2 power supply for a keyboard or mouse
a13	USB 2.0 port for the CryptoServer LAN
	CryptoServer LAN V4 in Figure 2
a12, a13	USB 2.0 ports for the CryptoServer LAN
a17	Guard bracket protecting both power supplies against inadvertent displacement during transport/movement.

Table 2: Ports and interfaces on the rear side of CryptoServer LAN V4 (AC)

3.2 Ports and Interfaces on the Rear Side (DC Power Supply)

The CryptoServer LAN V4 with DC power supply might be supplied with slightly different ports and interfaces on the rear side as shown in the following two figures, while the front panel remains the same as in Figure 7 resp. Figure 9.

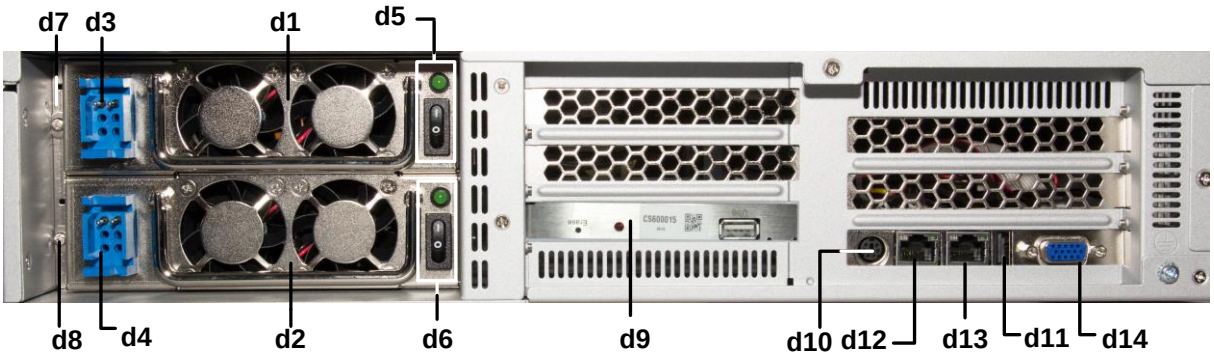


Figure 5: CryptoServer LAN V4 (DC) – Sockets and ports on the rear side (variant b)

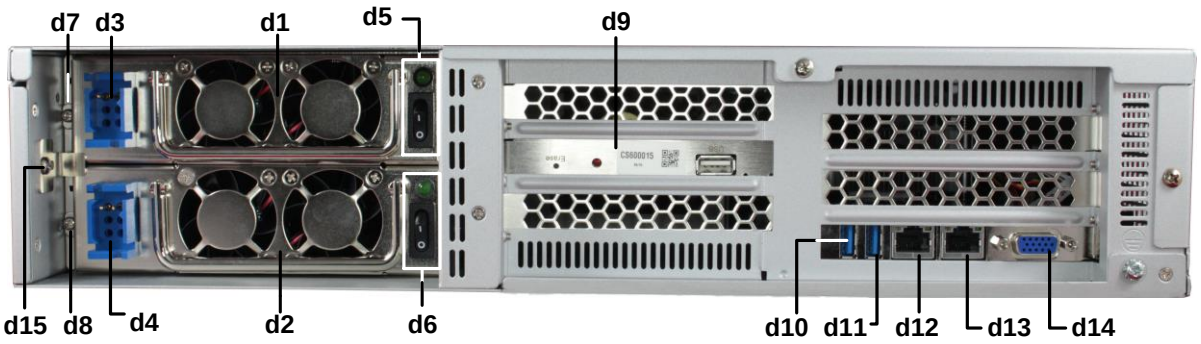


Figure 6: CryptoServer LAN V4 (DC) – Sockets and ports on the rear side (variant c)

Port/Interface	*Description*
	CryptoServer LAN V4 (Figure 5 and Figure 6)
d1, d2	Power supplies
d3, d4	Power supply sockets 42 V ~ 60 V DC
d5, d6	Power supply switches (switches power on/off) plus control light (green) above
d7, d8	Screws for attaching the power supplies
d9	CryptoServer plug-in card (CSe-Series or Se-Series Gen2)
d12	eth1 - Ethernet port 10/100/1000 (RJ45)
d13	eth0 - Ethernet port 10/100/1000 (RJ45)
d14	VGA connector (screen)
	CryptoServer LAN V4 in Figure 5
d10	PS/2 power supply for a keyboard or mouse
d11	USB 2.0 port for the CryptoServer LAN
	CryptoServer LAN V4 in Figure 6
d10, d11	USB 2.0 ports for the CryptoServer LAN
d15	Guard bracket protecting both power supplies against inadvertent displacement during transport/movement.

Table 3: Ports and interfaces on the rear side of CryptoServer LAN V4 (DC)

3.3 Ports and Operating Elements on the Front Panel

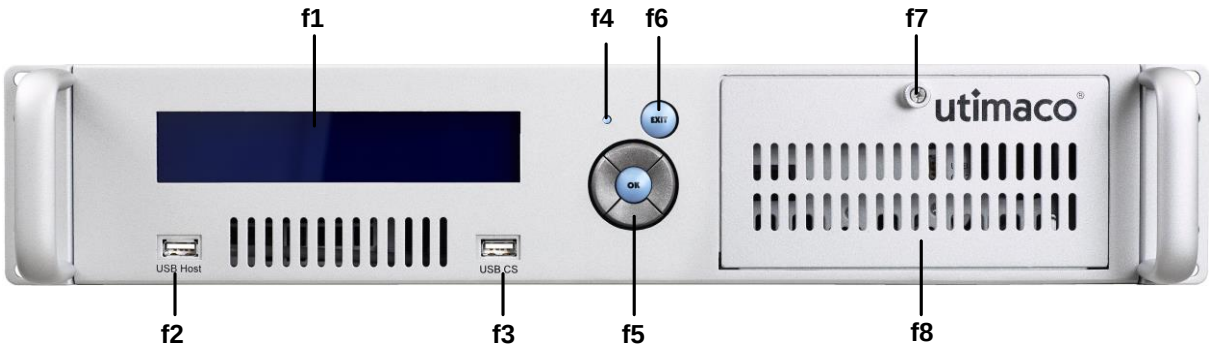


Figure 7: CryptoServer LAN V4 – Ports and operating elements on the front panel

Port/ Op. element	*Description*
f1	Display
f2	USB Host USB 2.0 port of the CryptoServer LAN. Generally, this port is used for connecting the delivered PIN pad.
f3	USB CS USB 2.0 port of the CryptoServer used for the CryptoServer administration
f4	Control light to show when the device is in operation
f5, f6	Buttons for CryptoServer LAN menu control
f7	Screw for opening the front door of the CryptoServer LAN
f8	Front door of the CryptoServer LAN

Table 4: Ports and operating elements on the front panel of the CryptoServer LAN V4

3.3.1 Menu Control Buttons

There are six menu control buttons.

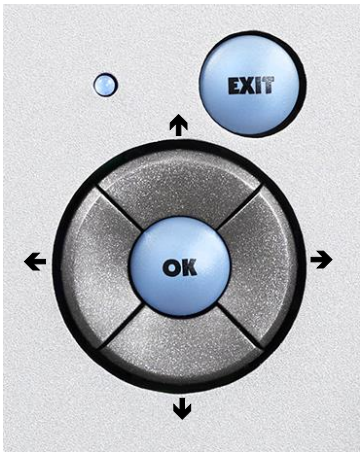


Figure 8: Control menu buttons of the CryptoServer LAN V4

Button	*Function*
EXIT	Quit the currently displayed menu level or menu item
OK	Select the menu level or confirm the menu item
↑	Move up in the menu control
→	Move to the right in the menu control
↓	Move down in the menu control
←	Move to the left in the menu control

Table 5: Control menu buttons and their function

3.3.2 Ports and Operating Elements behind the Front Door

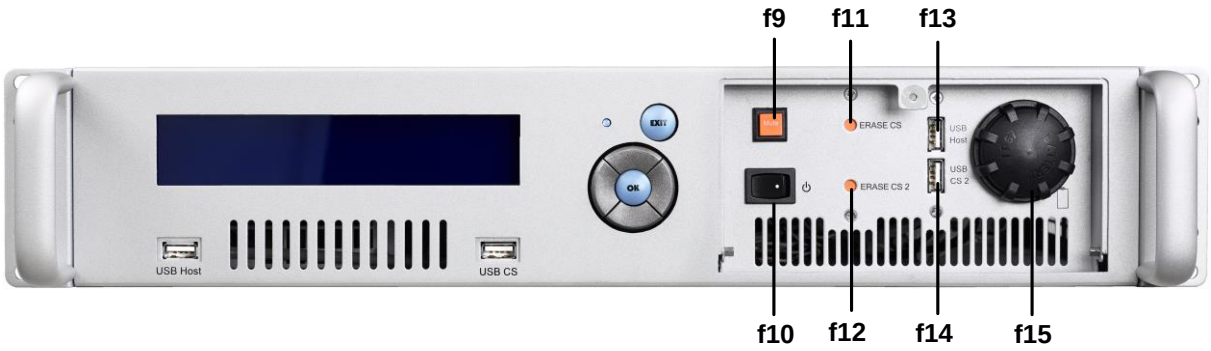


Figure 9: CryptoServer LAN V4 – Ports and operating elements behind the front door

Port/ Op. element	*Description*
f9	Mute key for the signal tone that sounds if a power supply fails or is switched off
f10	On/off switch (Switch for turning on/off the des CryptoServer LAN)
f11	ERASE CS Push-button for performing an *External Erase* on the integrated CryptoServer (CSe-Series or Se-Series Gen2)
f12	ERASE CS 2 (only connected if two CryptoServer are available) Push-button for performing an *External Erase* on a second integrated CryptoServer (CSe-Series or Se-Series Gen2)
f13	USB Host USB 2.0 port of the CryptoServer LAN
f14	USB CS 2 (only connected if two CryptoServer are available) USB 2.0 port of a second integrated CryptoServer used for the administration of this CryptoServer
f15	Battery compartment for the external battery of the CryptoServer LAN

Table 6: Ports and operating elements behind the front door

3.4 Bringing the CryptoServer LAN V4 into Service

To bring the device into service, follow these steps:

1. Put the CryptoServer LAN in a 19" rack.
2. Put it in the place where you want it to stay.

3. Connect the power supply sockets **a3**, **a4** (AC) resp. **d3, d4** (DC) on the rear side of CryptoServer LAN to a power supply using the power supply cables supplied with the device.
4. Connect the **eth0** Ethernet port **a14** (AC)/**d14** (DC) on the rear side of the CryptoServer LAN to your network with a twisted pair cable (RJ45).
5. Switch on the power switches **a5**, **a6** (AC) resp. **d5**, **d6 (DC)** on the rear side of the CryptoServer LAN.
6. Press the on/off switch **f10** on the front panel of the device behind the front door to switch on the CryptoServer LAN.

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

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

Figure 10: Display of CryptoServer LAN V4 – initial view

The values displayed in the figure above for the operating mode (**Mode:**), the temperature in °C (**Temp.:**), the battery state (OK), the transactions number per minute (**Trans./min.:**), the number of currently logged on clients (**Clients:**) and the CryptoServer load for the last 60 seconds (**Load:**) are only example values for a CryptoServer CSe-Series.

The most important thing at this point is that the CryptoServer is running in *Operational Mode* (**Mode: Operational**) after it has been booted and is therefore ready for use.

7. Connect the delivered PIN pad to the computer which you want to use for the remote administration of the CryptoServer LAN/CryptoServer or TimestampServer plug-in card and configure the PIN pad on the computer.
   - On a computer with Windows operating system, install the USB PIN pad driver for Windows. The installation requirements and procedure are provided in chapter "Installing the PIN pad Driver" in the CryptoServer Manual for System Administrators.
   - On a computer with a Linux operating system, define a special udev rule for the usage of the USB PIN pad. For details see chapter "Configuring the PIN Pad" in the CryptoServer Manual for System Administrators. There is no need to install any dedicated PIN pad driver for Linux.

8. Change the password for the users root and cslagent of the CryptoServer LAN as described in chapter "Changing the Password for the Users root and cslagent" of the *CryptoServer LAN Manual for System Administrators*.
9. Configure the IP address for the CryptoServer LAN and for the default gateway.
   - If you want to use static IP addresses, follow the instructions in chapters "Entering the IP Address of the CryptoServer LAN" and "Entering the IP Address of the Default Gateway" of the *CryptoServer LAN Manual for System Administrators*.
   - If you want to use automatic IP configuration via DHCP for the CryptoServer LAN and for the default gateway, follow the instructions in chapter "Setting up DHCP" of the *CryptoServer LAN Manual for System Administrators*.
10. Check the network reachability of CryptoServer LAN as described in chapter "Checking Reachability in Network (ping)" of the *CryptoServer LAN Manual for System Administrators*.
11. If you want to be able to access the CryptoServer LAN remotely, enable the SSH daemon as described in chapter "Activating the SSH Daemon" of the *CryptoServer LAN Manual for System Administrators*.
12. Install the SecurityServer product CD on the computer you want to use for the CryptoServer LAN's remote administration as described in chapter "Installing the CryptoServer Host-Software" in the *CryptoServer Manual for System Administrators*.

4 Maintenance

The maintenance tasks that a customer is permitted to perform on the CryptoServer LAN are to check the power level of the batteries (carrier battery and external battery) and if necessary to change the external battery in the battery compartment, as well as to remove/swap a power supply.

When the external battery reaches a critically low power level (see Chapter 4.1), it must be replaced (see Chapter 4.2).

Apart from this, no maintenance tasks should be carried out on the CryptoServer LAN.

If you should open CryptoServer LAN for any other maintenance work, all liability claims against Utimaco become null and void.

4.1 Checking the Battery Status

The CryptoServer LAN displays LOW when the external battery in the battery compartment or the carrier battery of the CryptoServer CSe/Se-Series Gen2 reaches a critical power level.

To find out which of the batteries of the CryptoServer LAN has reached this critical power level by using the menu control of the CryptoServer LAN, follow these steps:

1. Click OK.
2. Click the ↓ button to select the CryptoServer Administration menu item.
3. Click OK to confirm.
4. Click OK to select the Show CryptoServer Info menu item.
5. Use the ↓ button to go to the Battery State menu item.
6. Click OK to confirm.

In the CryptoServer LAN display, the battery status is shown for example as follows:

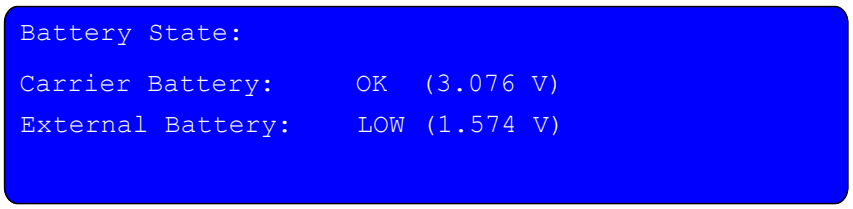


Figure 11: CryptoServer LAN V4 display - Battery state

If the system could not find out the battery status, because the CryptoServer register is currently being accessed by another process, then you should try to find out the battery state again after waiting a few minutes.

In the case of CryptoServer LAN you can change the external battery.
The carrier battery of the CryptoServer must only be replaced by the manufacturer, Utimaco or a certified sales partner.

- If the external battery state displayed is LOW, it means the power level of the CryptoServer external battery has sunk to a critical level. You must now immediately, and whilst the device is in operation, replace the external battery in the battery compartment.
- If the carrier battery state displayed is LOW, it means the power level of the CryptoServer carrier battery has sunk to a critical level. In this case, contact Utimaco or a certified sales partner and have them replace the carrier battery of the CryptoServer.

4.2 Replacing the External Battery

To replace the external battery in the battery compartment of the CryptoServer LAN you will need a new 3.6 V lithium battery which you can purchase from Utimaco.

This battery is not rechargeable.
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.

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

To replace the external battery proceed as follows:

1. Turn the knurled screw counterclockwise to open the front door of the CryptoServer LAN.

Figure 12: Opening the front door of the CryptoServer LAN V4

If you want, you can remove the front door from the bracket.

Figure 13: Removing the front door of the CryptoServer LAN V4

2. Turn the black screw cap of the battery compartment counterclockwise to open it.

Figure 14: Opening the battery compartment of the CryptoServer LAN V4

Figure 15: Removing the screw cap of the battery compartment

3. Take the battery out of the compartment.

Figure 16: Removing the external battery of the CryptoServer LAN V4

4. Make sure the contacts of the new battery and the metal plate inside the black screw cap are clean and grease-free.
5. Now place the new battery in the battery compartment. Make sure that the positive pole of the battery contacts the black screw cap of the battery compartment.

6. Screw on the black screw cap of the battery compartment to close it, by slightly pushing the screw cap with your finger and turning it clockwise with the other hand.

Do not misthread the black screw cap when screwing it on battery compartment.

Figure 17: Screwing on the screw cap of the battery compartment for the external battery

7. Close the front door of the CryptoServer LAN, and lock it by turning the knurled screw clockwise.
8. Check the battery state as described in Chapter 4.1 of this manual.

The battery power level shown in the display of the CryptoServer LAN is not updated very frequently. Therefore, we recommend you to wait for at least three minutes before checking the battery state.

If the state of the external battery is shown as **absence**, check that the new battery has been connected correctly.

4.3 Removing/Swapping a Power Supply Module

You can remove or swap out a power supply module (AC or DC) while the CryptoServer LAN is running normally.

Be sure to wear gloves when removing a power supply module to prevent being burned. The temperature of the failed power supply module might be around 50 ~ 60 °C.

The following example shows step-by-step how to replace the upper AC power supply module as shown in Figure 18. For replacing a DC power supply module follow the same steps for the elements shown in Figure 19.

If a power supply module fails, and needs to be replaced, follow these steps:

1. Switch off the relevant power supply module with the power supply switch a5/d5.
2. Disconnect the power cable from the relevant power supply module (the upper one in our example figures).
3. On a CryptoServer LAN V4 variant c (Figure 2 resp. Figure 6), undo the screw used to attach the guard bracket a17/d15 by using a screwdriver. If you are using a CryptoServer LAN V4 variant b (Figure 1 resp. Figure 5), skip this step.
4. Using a screwdriver, undo the relevant screw a7/d7, which is being used to attach the power supply module on the CryptoServer LAN.

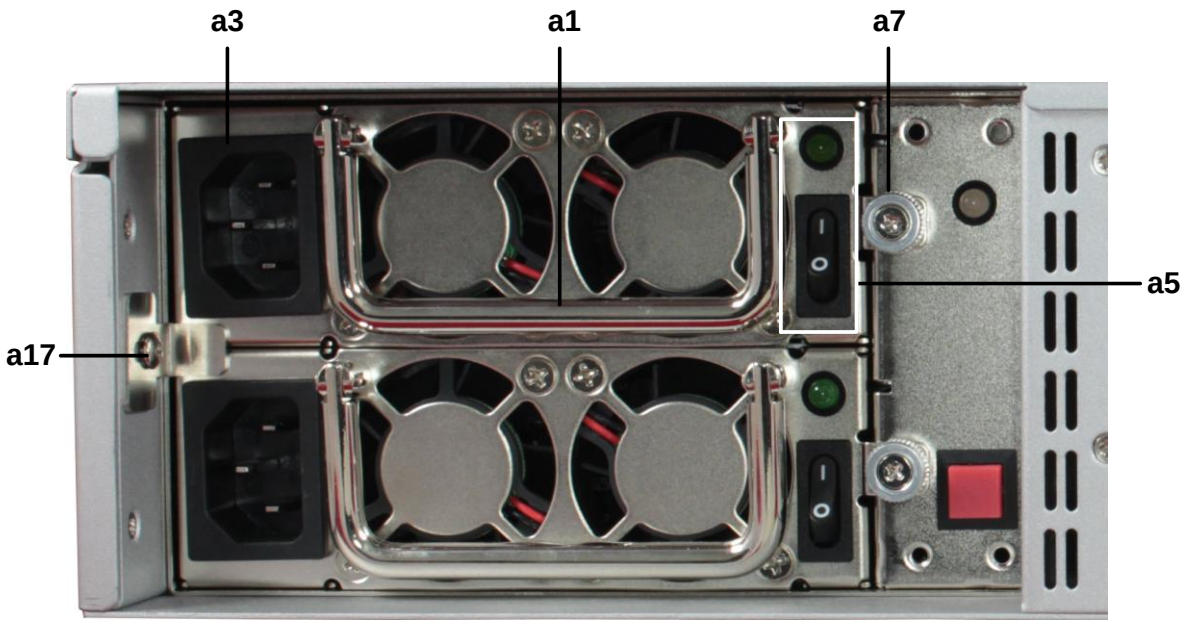


Figure 18: Power supply modules (AC) of the CryptoServer LAN V4

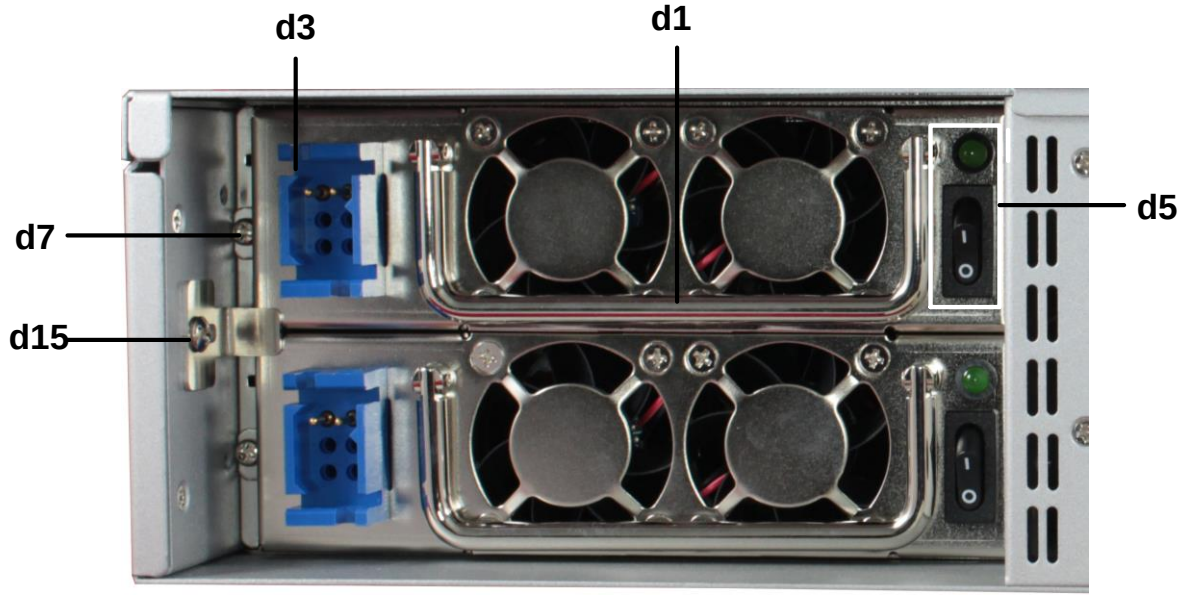


Figure 19: Power supply modules (DC) of the CryptoServer LAN V4

5. Use the handle a1/d1 to carefully pull the power supply module out of the CryptoServer LAN's case.
6. Put the new power supply module in place.

7. Attach the new power supply module to the case with the screw a7/d7 provided for that purpose.
8. On a CryptoServer LAN V4 variant c (Figure 2 resp. Figure 6), attach the guard bracket a17/d15 to the case with the screw to protect both power supply modules against inadvertent displacement during transport/movement. If you are using a CryptoServer LAN V4 variant b (Figure 1 resp. Figure 5), skip this step.
9. Plug the power cable into the new power supply module a3/d3.
10. Switch on the power supply module with the power supply switch a5/d5.

If you have installed the power supply module correctly and provided it with power, the green control light above the power supply switch a5/d5 lights up.

5 Switching off the CryptoServer LAN

You can switch off the CryptoServer LAN by using the menu control.

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

The initial status message in the display panel, as shown for example in Figure 10, 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 the CryptoServer LAN as follows:

1. Click OK.
2. Select the CSLAN Administration menu item.
3. Click OK to confirm the selection.
4. Use the 🡻 button to go to the Shutdown menu item.
5. Click OK to confirm the selection.
6. Respond [ ]Yes to the confirmation prompt Confirm Shutdown by pressing the 🡸 button to insert the asterisk in the brackets select [✱]Yes.
7. 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 CryptoServer LAN completely, switch off the power supply switches a5 and a6 on the rear side of the device.

The CryptoServer LAN should be kept running constantly to prevent the batteries from being used.
If a system is inactive for a long period, the batteries will be used up. After a while this can result in the CryptoServer no longer being supplied with power, and all the data will be deleted. The resulting maintenance tasks are not covered by Utimaco's liability.
On the other hand, a brief interruption to the power supply (if the device is being moved around etc.) does not place a serious demand on the batteries and consequently there is no danger of data and settings etc. being deleted.

6 Disposing of the CryptoServer LAN

In this chapter you can find out what you need to take into account when you want to dispose of your CryptoServer LAN.

Of course, you also have the option of returning the CryptoServer LAN that you no longer require to us, Utimaco, as the manufacturer. In this case, we will take care for disposing of the CryptoServer LAN and the batteries in an environmentally friendly way.

6.1 Deleting All Sensitive Data

You must delete all sensitive data in your CryptoServer LAN before disposing of it.

To delete all sensitive data in your CryptoServer LAN proceed as follows:

1. Turn the knurled screw counterclockwise to open the front door of the CryptoServer LAN.

Figure 20: Opening the front door of the CryptoServer LAN V4

If you want, you can remove the front door from the bracket.

Figure 21: Removing the front door of the CryptoServer LAN V4

2. Push the corresponding ERASE push-button by using an appropriate screwdriver.

   If a CryptoServer plug-in card CSe- or Se-Series has been installed in the CryptoServer LAN, pushing the ERASE push-button is only effective if the CryptoServer LAN has been switched on.

   If pushing the ERASE push-button should be applied to a CryptoServer plug-in card Se-Series Gen2 in the CryptoServer LAN, it is not necessary that the CryptoServer LAN has been switched on.

Figure 22: ERASE pushbutton for performing External Erase on a CryptoServer LAN V4

   - If there is a single CryptoServer plug-in card integrated in the CryptoServer LAN, only the ERASE CS push-button is connected.
   - If there are two CryptoServer plug-in cards integrated in the CryptoServer LAN, you have to know exactly which plug-in card is connected to which ERASE push-button.

   An External Erase has been performed on the CryptoServer, and an Alarm has been triggered.

3. Close the front door of the CryptoServer LAN.
4. Make sure that the CryptoServer is in Maintenance Mode and an alarm has been triggered. You can retrieve the CryptoServer status information by using the CryptoServer LAN menu control buttons:
5. On the front panel of the CryptoServer LAN, press the OK button.
   The ➔ arrow on the far left-hand side of the display shows you which submenu you can select with the OK button.
6. Use the OK button to open the CryptoServer Administration menu item.
7. Use the 🡻 button to select Show CryptoServer Info and press the OK button to open the menu item.
8. Use the 🡻 button to select Get State and press the OK button to open the menu item.

   The following information is shown by way of example on the display of the CryptoServer LAN:

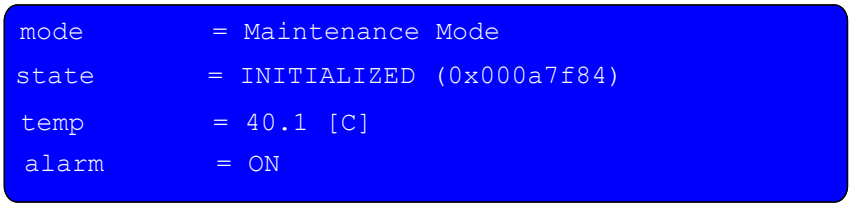


Figure 23: CryptoServer LAN display – status output after deletion of sensitive data

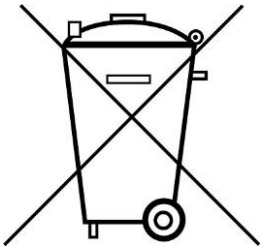
*Regardless of whether you have performed an External Erase (pressing the **ERASE** push-button) or not, the following applies:*
If you remove the CryptoServer PCIe plug-in card from the CryptoServer LAN and remove any battery from this plug-in card, the sensitive data on this plug-in card is deleted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

6.2 Disposing the Batteries

In the CryptoServer LAN you will find three batteries which must be disposed of in an environmentally friendly way.

- The 3.6 V lithium battery made by Saft of type LS 17500
  The battery is located inside the battery compartment. The battery compartment is behind the front door of the CryptoServer LAN.
- The 3 V lithium battery made by FDK of type CR 12600SE-T1
  The battery is located on the CryptoServer plug-in card CSe- or Se-Series Gen2, which is inside the CryptoServer LAN.
- The 3 V lithium coin cell battery for the mainboard of the CryptoServer LAN.
  This battery is located on the mainboard of the CryptoServer LAN.

Remove all batteries from the CryptoServer LAN 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 used batteries in the normal household waste.
Consumers are obliged to bring batteries to a suitable municipal or commercial collection point.
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.

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

7 Technical Data of CryptoServer LAN V4 (AC Power Supply)

Dimensions	Height	88 mm (2 slots (height units))
	Width	446 mm without attachment bracket (19")
	Depth	472 mm excluding handles
Weight	13 kg	
Operating power	100 V ~240 V, 50~60 Hz AC	
Power supply	2 x 320 W	
Power consumption (effective/apparent)	Typically 75 W/85 VA, maximum 90 W/100 VA	
Heat dissipation	307 BTU/h	
Environmental temperature	in operation	CryptoServer Se-Series Gen2: +10 °C to +50 °C CryptoServer CSe-Series: +10 °C to +40 °C
	in storage	-10 °C to +55 °C (+14 °F to +131 °F)
Humidity	10% to 95% relative humidity, non-condensing	
MTBF	90 000 hours at 25 °C/77 °F (in acc. with MIL-HDBK-217)	
RoHS compliance	Yes	
WEEE	National register for waste electric equipment (EAR) DE39805015	
Conformity	EMC emission: CISPR 22 / CISPR 32 Class B, IEC/EN 61000-3-2, IEC/EN 61000-3-3 EMC immunity: EN 300386, EN 55024 / CISPR 24, IEC/EN 61000-6-2 Equipment safety: IEC/EN 60950-1 (CB scheme) FCC 47 CFR Part 15 Class B UL Climatic and mechanical conditions: EN 300 019: Storage class 1.1, Transportation class 2.1 (with temperature range restricted to the storage environmental temperature given above), stationary use in environments that are protected from the weather class 3.1	

8 Technical Data of CryptoServer LAN V4 (DC Power Supply)

Dimensions	Height	88 mm (2 slots (height units))
	Width	446 mm without attachment bracket (19″)
	Depth	472 mm excluding handles
Weight	13 kg	
Operating power	42 V ~ 60 V DC	
Power supply	2 x 350 W	
Power consumption	Typically 80 W, maximum 95 W	
Heat dissipation	324 BTU/h	
Environmental temperature	in operation	CryptoServer Se-Series Gen2: +10 °C to +50 °C CryptoServer CSe-Series: +10 °C to +40 °C
	in storage	-10 °C to +55 °C (+14 °F to +131 °F)
Humidity	10% to 95% relative humidity, non-condensing	
MTBF	90.000 hours at 25 °C/77 °F (in acc. with MIL-HDBK-217)	
RoHS compliance	Yes	
WEEE	National register for waste electric equipment (EAR) DE39805015	
Conformity	EMC emission: CISPR 22 / CISPR 32 Class A EMC immunity: EN 300386, EN 55024 / CISPR 24, IEC/EN 61000-6-2 Equipment safety: IEC/EN 60950-1 (CB scheme) FCC 47 CFR Part 15 Class A UL Climatic and mechanical conditions: EN 300 019: Storage class 1.1, Transportation class 2.1 (with temperature range restricted to the storage environmental temperature given above), stationary use in environments that are protected from the weather class 3.1	

9 Contact Address for Support Queries

Please feel free to contact us if an error occurs while operating the CryptoServer, or if you have any further questions on CryptoServer.

Utimaco IS GmbH

Germanusstr. 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 back to the manufacturer, we request that you first send us an e-mail containing a short description of the problem and the Diagnostic Information as a txt file, to this e-mail address:

rma-cs@utimaco.com

To save the Diagnostic Information in a txt file on your computer please proceed as described in the manual *CryptoServer – Manual for System Administrators.*