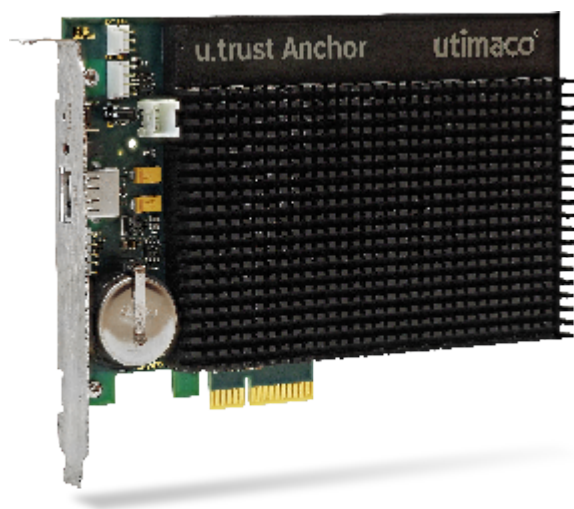


# u.trust Anchor PCIe

## Operating Manual



**utimaco**<sup>®</sup>

## Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet e-mail	<a href="https://support.hsm.utimaco.com/">https://support.hsm.utimaco.com/</a> <a href="mailto:support@utimaco.com">support@utimaco.com</a>
Document Version	1.0.18
Product Version	6.0.0
Date	2024-10-22
Document No.	2020-0042
Status	<b>PUBLISHED</b>

All rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>
---------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
1.1	Downloading the Product Bundle .....	5
1.2	About This Manual.....	5
1.2.1	Target Audience for This Manual.....	5
1.2.2	Document Conventions .....	5
1.2.3	Abbreviations .....	6
1.3	Import and Export Regulations.....	7
1.4	Damage in Transit .....	7
1.5	Deliverables .....	7
1.6	Security Guidelines.....	9
1.6.1	General Advice.....	9
1.6.2	Protected Operational Environment .....	9
<b>2</b>	<b>General Safety Instructions .....</b>	<b>12</b>
2.1	Moving and Storing .....	12
2.2	Battery.....	13
2.3	Safely Transporting the u.trust Anchor .....	13
2.4	Environmental Temperature.....	15
<b>3</b>	<b>u.trust Anchor PCIe Overview .....</b>	<b>16</b>
<b>4</b>	<b>Bringing into Service.....</b>	<b>17</b>
4.1	Prerequisites for Operation .....	17
4.1.1	Software Requirements.....	17
4.1.2	Hardware Requirements.....	17
4.1.3	General and Security Requirements for the Operational Environment .....	18
4.2	Unpacking and Handling.....	18
4.2.1	General Notes.....	20
4.2.2	Checking the Integrity of the Delivery .....	20
4.2.3	Installing the u.trust Anchor PCIe card.....	32
4.3	Installation of the u.trust Anchor Driver Software.....	33
4.3.1	Installation on Linux Operating Systems.....	33
4.3.1.1	Compiling/Installing the Driver.....	33
4.3.1.2	Performing a Functional Test.....	37
4.3.1.3	Updating the Driver on Linux .....	39
4.3.1.4	Uninstalling the Driver .....	39

---

4.3.2	Installation on Windows Operating Systems .....	40
4.3.2.1	Certificate Chain Verification.....	40
4.3.2.2	Installing or Updating the Driver.....	42
4.3.2.3	Performing a Functional Test on Windows.....	45
4.3.2.4	Uninstalling the Driver on Windows.....	47
4.4	Identification and Claiming of u.trust Anchor.....	49
5	<b>Replacing the Battery.....</b>	<b>50</b>
6	<b>Uninstalling the u.trust Anchor PCIe card .....</b>	<b>54</b>
7	<b>Disposing of the u.trust Anchor.....</b>	<b>55</b>
8	<b>Technical Data.....</b>	<b>57</b>
9	<b>Contact Address for Support Queries .....</b>	<b>58</b>
10	<b>References .....</b>	<b>59</b>

# 1 Introduction

Thank you for purchasing our u.trust Anchor. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or comments.

## 1.1 Downloading the Product Bundle

You can download all components that are required to operate the u.trust Anchor device from the Utimaco download portal.

The product bundle is downloadable from the following site:

<https://support.hsm.utimaco.com/support/downloads/>



You have to be registered for this download portal and access to a download area, e.g., „SecurityServer Se Gen2“, must have been granted.

The product bundle includes user documentation, the Global Initial Admin Key, the Utimaco Root Certificate and the administration tools for the device.

## 1.2 About This Manual

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

### 1.2.1 Target Audience for This Manual

This manual is intended for system administrators who bring the u.trust Anchor card into service and administer it.

### 1.2.2 Document Conventions

We use the following document conventions:

<b>Convention</b>	<b>Use</b>	<b>Example</b>
<b>Bold</b>	Items of the Graphical User Interface (GUI), e.g., menu options	Press <b>OK</b>
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

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.



This message marks the result expected after the successful execution of an instruction.

### 1.2.3 Abbreviations

We use the following abbreviations in this manual:

<b>Abbreviation</b>	<b>Meaning</b>
HSM	Hardware Security Module
PKI	Public Key Infrastructure
TSP	Time-Stamp Protocol
TS-SO	Security Officer for the TimestampServer

## 1.3 Import and Export Regulations



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

## 1.4 Damage in Transit

If you discover that the transport boxes are damaged when they arrive, please immediately contact or Utimaco IS GmbH, see [Contact Address for Support Queries](#). Please have the delivery note and the device's serial number ready.

## 1.5 Deliverables

The u.trust Anchor deliverables include:

- One u.trust Anchor PCI Express (PCIe) card

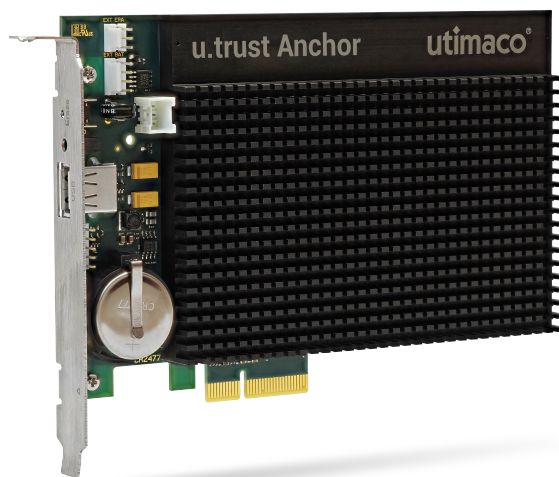


Figure 1 : u.trust Anchor PCIe card

- One u.trust Anchor Operating Manual (this Manual)

You can also use smartcards to administer the u.trust Anchor. These smartcards, as well as the appropriate PIN pad can be purchased from Utimaco IS GmbH.

You cannot use PIN pads and smartcards that were not purchased from Utimaco IS GmbH to administer the u.trust Anchor.



Use only PIN pads and smartcards delivered by Utimaco IS GmbH for the u.trust Anchor administration.

Additional (u.trust Anchor CC/FIPS) deliverables include:

- One PIN pad of type Utimaco cyberJack one (referred to below as PIN pad) to be used for the u.trust Anchor administration. It must be connected to a USB port of the administration computer.



Figure 2 : Utimaco cyberJack one PIN Pad

- One micro USB cable for connecting the PIN pad
- One USB 2.0 extension cable for connecting the PIN pad
- One PIN pad stand
- Ten smartcards for administering the u.trust Anchor



Figure 3 : Smartcard provided by Utimaco

## 1.6 Security Guidelines

### 1.6.1 General Advice

We highly recommend using strong passwords consisting of at least eight random characters, which should include uppercase and lowercase letters, special characters and random numbers.

Keep the passwords secret, do not write them down anywhere and change them regularly.

We highly recommend checking the state of the battery at regular intervals.

### 1.6.2 Protected Operational Environment

Before you start operating the device, ensure that the system environment is highly secure by checking that:

- No secure seal is damaged.
- PIN, PUK (personal unblocking key) or password entry cannot be monitored.
- The device is securely stored and appropriately protected against unauthorized access.
- The PIN pad is securely stored, if purchased.
- The smartcards are securely stored, if purchased.
- Only trustworthy persons have physical-/network access.

- The administration and configuration/setup of the u.trust Anchor shall be exclusively done by verified, trusted, authorized and well-trained persons.
- Only authorized changes to the software and the configuration of device are possible.
- Regular inspections are required to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the u.trust Anchor).
- The u.trust Anchor must be protected against the possibility of attacks that are based on emanations, like electromagnetic emanations or Simple Power Analysis (SPA) or Differential Power Analysis (DPA) attacks.

**Additional measures for operating an u.trust Anchor PCIe card/using an administration computer with the client application:**

**The following information is relevant for operating an u.trust Anchor PCIe card, and for any host PC/server where the u.trust Anchor PCIe card is integrated and where Utimaco host APIs and tools are running:**

- Only trustworthy persons have a physical and network access to the u.trust Anchor and to the administration computer.
  - The administration and configuration/setup of the administration computer shall be exclusively done by verified, trusted, authorized and well-trained persons.
  - The administration computer where the u.trust Anchor PCIe card is installed in shall be placed in a highly secured area that can be only reached by authorized people. Unauthorized persons shall not have any access to the administration computer. It shall be secured by an access control mechanism, for example, password and/or smartcard.
    - The following rules apply for the passwords:
      - The minimum recommended password length is eight characters.
      - The password shall contain uppercase and lowercase letters, at least two special characters and numbers.
      - The password shall be changed periodically, at least every three months.
  - The administration computer shall be checked for malware prior to installing the u.trust Anchor card and the administration tools. Software that is not



trustworthy and not required for the operation and administration of the u.trust Anchor shall be uninstalled.

- An antivirus software with the latest updates installed shall be running on the administration computer.
- We highly recommend using the administration computer exclusively for the operation and administration of the u.trust Anchor. There should be no Internet access and the remote computer administration should be restricted to a minimum.

## 2 General Safety Instructions

---



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

---

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

---



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

---

Do not attempt to repair the u.trust Anchor in any way.

### 2.1 Moving and Storing

When moving and storing the device, follow these instructions:

- The u.trust Anchor should only be moved and stored in its original packaging.
- Although there is no motion detector on the u.trust Anchor card that could initiate the deletion of data, do not subject the device to impacts and vibrations or any other physical events that may damage the packaging.
- You must make sure that the u.trust Anchor is always stored at temperatures between -10 °C and +55 °C (+14 °F and +131 °F).
- If the device is to be stored for a longer time period, please ensure that the battery replacement time is not exceeded. For details, see [Battery](#).
- Keep this manual together with your u.trust Anchor so that it is handy if you need to reinstall the system.

- The PCIe connector is fragile, and can be damaged or even broken during movement and transport by force and acceleration of the computer chassis, where the u.trust Anchor is mounted in.
- There is a point of mechanical stress on the printed circuit board (PCB) near the PCIe bracket, which can be damaged.

For these reasons, careful attention is required during transport, movement and storage of the u.trust Anchor PCIe cards all series. Additionally, see [Safely Transporting the u.trust](#). We strongly recommend removing the u.trust Anchor PCIe card from the computer prior to any planned transport or movement. All cryptographic keys stored on the PCIe card remain securely maintained during the transport or movement since the u.trust Anchor is continuously supplied with power by the carrier battery.

## 2.2 Battery

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



This battery is not rechargeable.

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

## 2.3 Safely Transporting the u.trust Anchor

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

Prerequisites

- Ensure that the requirements in [Moving and Storing](#) are fulfilled.  
Prepare the new location of the u.trust Anchor card according to [General Notes](#).

To ensure the safe transport of the u.trust Anchor PCIe card over long or short distances from the old location to the new location, first check whether an alarm was triggered by recalling information about u.trust Anchor using the `gladm system-info` command:

```
gladm system-info
```

In case of alarm, the output of this command will highlight that an alarm has been triggered followed by a zeroization event. This might be an indicator that the carrier battery has reached the minimum allowed level for assuring the functionality of the u.trust Anchor sensors.

For a particular check of the carrier battery state, the `gladm` command

```
gladm system-metrics
```

can be also used.

This command displays a list of system information. Two extra fields in this list are dedicated to the state of the battery included in this module: the "`csar-main-battery`" and the "`csar-ext-battery`". The external battery is relevant only for the u.trust Anchor LAN. The main battery, however, ensures that the u.trust Anchor sensors and the erase circuit are always able to function correctly when the u.trust Anchor is not installed in a computer. Otherwise, an alarm will be triggered and all secret data on the device will be lost. This can be checked by

```
gladm system-info
```

If the value 1 is assigned to both fields, then continue with step 1 as described step by step below. Otherwise, if the battery value exceeds the limit thresholds, an alarm will be triggered causing the deletion of secrets. If "`csar-main-battery`" is equal to 0, continue with step 1.

1. Replace the carrier battery by a new one (3V, Lithium cell battery, Ø 24.5 mm, L = 7.7 mm, Panasonic CR2477 or equivalent). You find step-by-step instructions on how to do that in Chapter 6, "Replacing the Battery", of this document. This battery ensures the power supply of the u.trust Anchor for at least 6 months.  
If you have replaced the carrier battery, continue with step 4. Otherwise, continue with the next step.
2. Set up the u.trust Anchor following the instructions described in *Setup* in the [u.trust Anchor - Administration Manual](#).
3. Remove the u.trust Anchor PCIe card from the computer. Follow the instructions for removing PCIe cards as specified in the operating manual for your computer as well as the instructions in [Uninstalling the u.trust Anchor PCIe card](#).

4. Put the u.trust Anchor PCIe card into an antistatic wrapping and in the original packaging. If you need an original packaging or/and antistatic wrapping, contact the manufacturer Utimaco IS GmbH.
5. Again, ensure that the requirements in [Moving and Storing](#) are fulfilled.
6. After reaching destination, put the computer, where the u.trust Anchor PCIe card should be mounted in, to the required position, and then mount the u.trust Anchor PCIe card. Follow the instructions for mounting PCIe cards as specified in the operating manual for your computer as well as the instructions in [Installing the u.trust Anchor](#).

## 2.4 Environmental Temperature

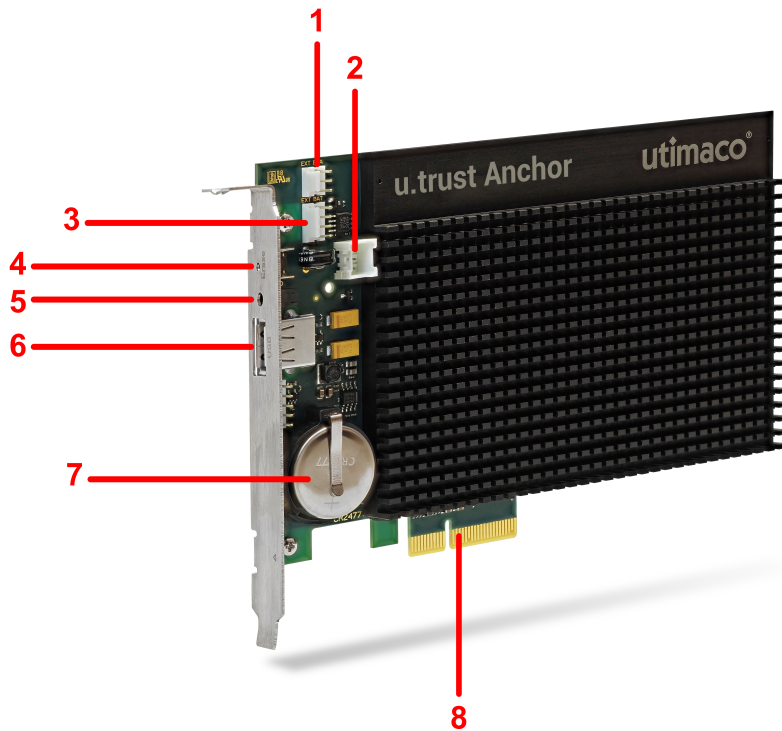
The u.trust Anchor must only be operated and stored in a particular temperature range.

- You must make sure that the u.trust Anchor is always stored at temperatures between -10 °C and +55 °C (+14 °F to +131 °F).



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

### 3 u.trust Anchor PCIe Overview



1. Internal power supply connector
2. Connector for an external battery, e.g., the external battery of u.trust Anchor LAN
3. USB connector (internal) USB connector for additional USB 2.0 connection (not in use)
4. Erase pushbutton
5. LED flash light – indicates the activation of the Erase pushbutton
6. USB port (external): USB 2.0 port for peripheral devices such as a PIN pad (not in use)
7. Battery Supplies power to the sensors and quenching system when the computer is switched off
8. 4 Channel PCIe version 3.x, with a single PCIe bus connector

## 4 Bringing into Service

Before you start up u.trust Anchor, check whether all parts that belong to the delivery, as listed in [Deliverables](#), are present.

### 4.1 Prerequisites for Operation

Before you bring the u.trust Anchor into service, make sure that the prerequisites listed below are fulfilled.

#### 4.1.1 Software Requirements

You need a computer with one of the operating systems listed in the following table. On this computer, the administration software provided by Utimaco shall be installed.

<i><b>Operating System</b></i>	<i><b>CryptoServer</b></i>	<i><b>u.trust Anchor</b></i>
<b>Windows x64</b>		
Windows 10	✓	✓
Windows 11 (Pro)	✓	✓
Windows Server 2016	✓	✓
Windows Server 2019	✓	✓
Windows Server 2022 (Standard)	✓	✓
<b>Linux x64</b>		
Red Hat Enterprise Linux 8	✓	✓
Red Hat Enterprise Linux 9	✓	✓
SUSE Linux Enterprise Server 12	✓	✓
SUSE Linux Enterprise Server 15	✓	✓
Ubuntu 20.04 LTS	✓	✓
Ubuntu 22.04 LTS	✓	✓

Table 2: u.trust Anchor Supported Operating Systems

#### 4.1.2 Hardware Requirements

For using the u.trust Anchor PCIe card, you must mount it into a computer with a free PCIe slot and at least the following system components:

- CPU: Intel x86/x64, AMD x86/x86-64
- Hard disk capacity: at least 120 Mbyte
- RAM: more than 12 Mbyte

The u.trust Anchor is fitted with a system of sensors that can detect whether it is being operated within the permitted temperature range.

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

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

#### **4.1.3 General and Security Requirements for the Operational Environment**

- The u.trust Anchor shall only be installed, operated and stored in environments fulfilling the temperature requirements, see [Environmental Temperature](#).
- Follow the security instructions specified in section [Security Guideline](#).

## **4.2 Unpacking and Handling**

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

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





The u.trust Anchor is packaged in a special anti-static wrapping. Please retain this wrapping in case you need to store or transport the device.

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



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

In particular, you must note the following points.



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

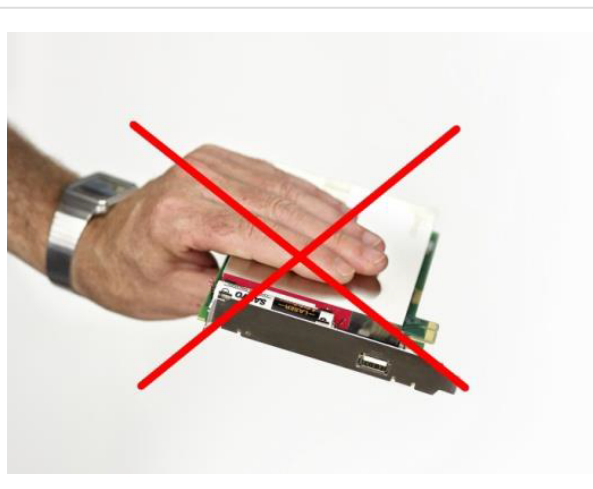
Take care that the circuit board never touches a metallic object (such as a screwdriver or wedding ring).

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



Do not touch any contacts on the card. Handle the u.trust Anchor 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).



### 4.2.1 General Notes

The u.trust Anchor is fitted with a system of sensors that can tell whether it is being operated within a permitted temperature range.



During normal operations, the internal temperature of the u.trust Anchor must not exceed 81 °C (177.8 °F) and fall below -18 °C (-0.4 °F). If it does, the device will automatically trigger the alarm state. Consequently, you must ensure that the u.trust Anchor temperature remains within this range.

To ensure that the internal temperature does not exceed these thresholds, the environmental temperature should not be more than 35 °C (95 °F).

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

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



If you cannot implement this configuration, we strongly recommend you mount a PCIe slot cooling fan directly beside the u.trust Anchor device.

### 4.2.2 Checking the Integrity of the Delivery

Before delivery, the u.trust Anchor PCIe card is packaged in a special antistatic wrapping. Retain this wrapping in case you need to store or transport the device. The u.trust Anchor PCIe card must always be stored in this specific antistatic wrapping to avoid a short circuit on the contact points that supply power.

The antistatic wrapping is put into a special security bag ensuring the tamper-evident transport. This security bag is placed into a covering box the inner side of which is covered with foam material to prevent a physical damage of the PCIe card. The covering box is delivered inside a package.

After receiving the package, you must perform the following steps to ensure that the package has not been opened or exchanged during transport.

❗ If you discover any damages or discrepancies while performing the following steps, immediately contact Utimaco IS GmbH to get information about how to proceed, see [Contact Address for Support Queries](#).

### Checking the Security Bag

The following figure shows the most important security-relevant features of the security bag assuring the secure tamper-evident transport.

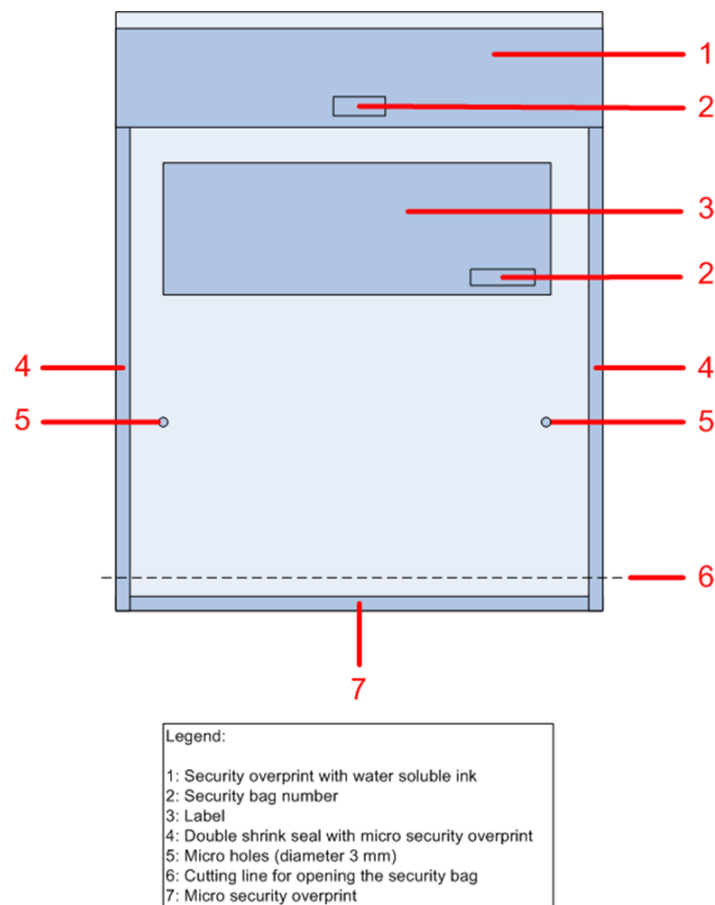


Figure 4 : Schematic view of a security bag



If you discover any damages or discrepancies while performing the following steps, immediately contact Utimaco IS GmbH to get information about how to proceed. The contact data is given in the chapter "Contact Address for Support Queries".

### Check these features before you open the bag:

Check the intactness of the security overprint (item 1) on the upper side of the bag. Make sure it looks as shown in the next exemplary figure.

#### ▪ Intact security overprint

The two blue stripes shall be continuous from the left side to the right side of the bag. In between the blue stripes, there is a transparent field equipped with a heat and cold indicator. Furthermore, a security overprint is printed with black water-soluble ink over the blue stripes and the transparent field. The overprint has a special waved pattern and a variable text sequence. There are two pink vertical stripes, one on the left side of the transparent field and one on the right side of the transparent field. These stripes are indicated by red rectangles in the figure below.



Figure 5 : A sample of an intact security overprint

- The adhesive strip in light yellow or light pink is visible through the transparent field as shown below.



Figure 6 : A detail of a sample of an intact security overprint

- Yellow areas in the transparent field between the blue stripes are okay. For example, yellow spots as indicated by red rectangles as shown below are acceptable. They do not indicate a tamper attempt, especially if they are located in folds. Small folds, as indicated in the example figure by green rectangles, also do not indicate a tamper attempt, but can occur as part of the packaging process.

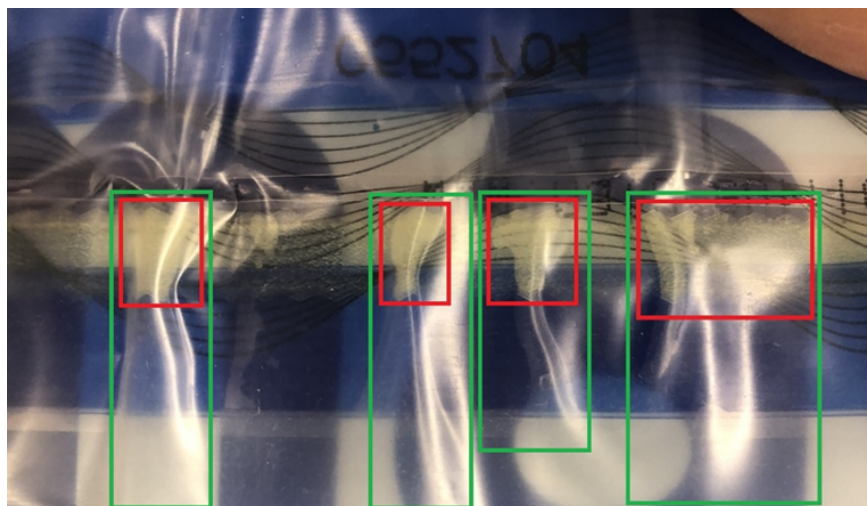


Figure 7 : Example for acceptable yellow spots and folds

- The following list shows some examples for possible damages on the security overprint that immediately indicate a tampered security bag. The items that are described in the text are indicated in the figures by red rectangles. If the security bag enclosing the u.trust Anchor you have received matches even slightly one of the items in the following list, immediately contact Utimaco IS GmbH to get information about how to proceed.

- **Slight red in the transparent field**

Do not open the security bag, if the transparent field between the two blue stripes contains a slightly red area.



Figure 8 : Example for a slight red in the transparent field

- **Pink in the transparent field**

Do not open the security bag, if there are additional pink areas in the transparent field between the two blue stripes. For example, a pink area might be a bar as shown below

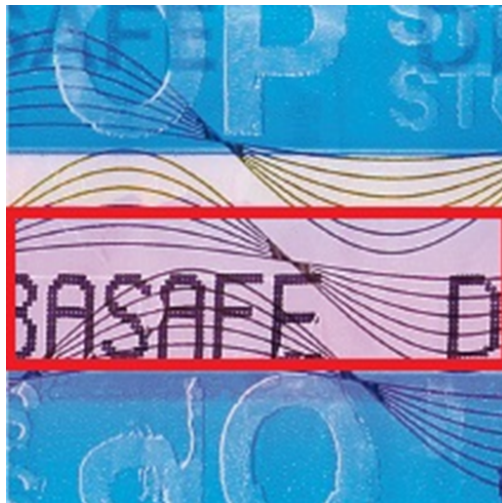


Figure 9 : Example 1 for pink in the transparent field

or tiny spots as shown in the next figure.





Figure 10 : Example 2 for pink in the transparent field

- **Text "STOP" in the blue stripes**

Do not open the security bag, if you see "STOP" written multiple times in white capital letters in one or both blue stripes. The figure shows only parts of this text.



Figure 11 : Example for "STOP" in the blue stripes

- **Damaged black security overprint**

Do not open the security bag, if the black security overprint is damaged. For example, parts of the black security overprint are simply missing



Figure 12 : Example 1 for a damaged black security overprint

or parts of the black security overprint appear blurred or almost transparent as shown below.

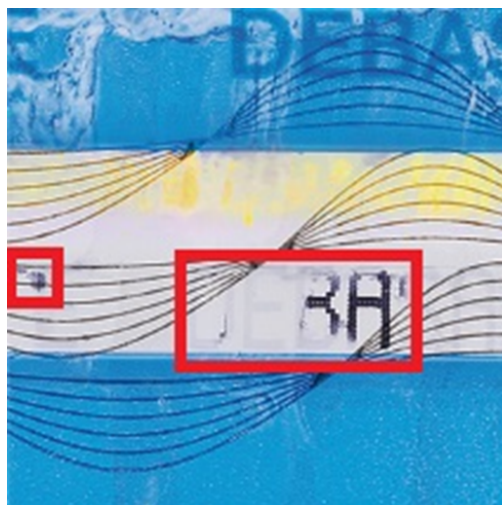


Figure 13 : Example 2 for a damaged black security overprint



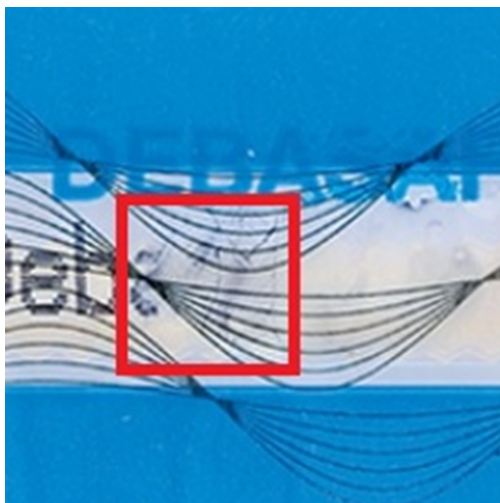


Figure 14 : Example 3 for a damaged black security overprint

- **Damaged blue stripe**

Do not open the security bag, if one or both blue stripes are damaged. For example, the blue color became blurred or appears to be scratched off.

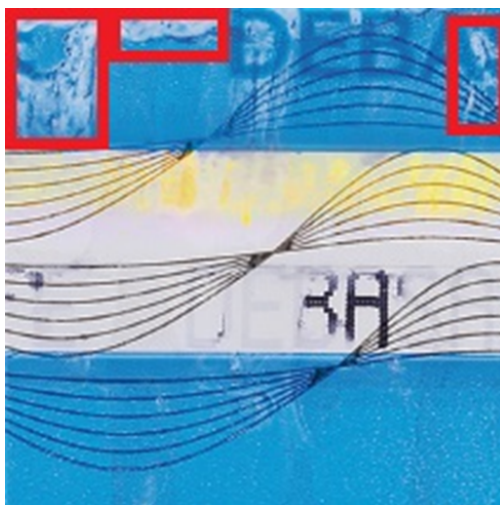
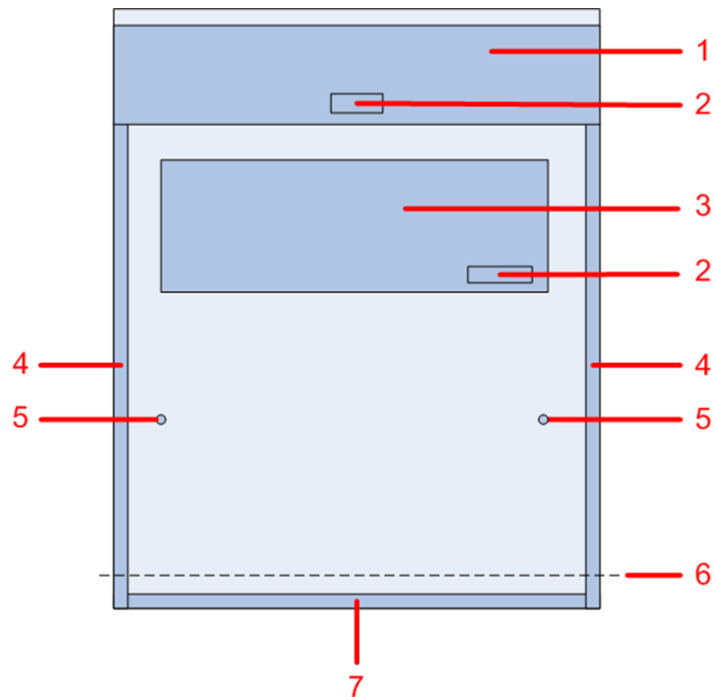


Figure 15 : Example 1 for a damaged blue stripe



Figure 16 : Example 2 for a damaged blue stripe

- Check the availability of the security bag number printed in the middle of the lower blue stripe and in the identification field. This number is shown as item 2.



Legend:	
1:	Security overprint with water soluble ink
2:	Security bag number
3:	Label
4:	Double shrink seal with micro security overprint
5:	Micro holes (diameter 3 mm)
6:	Cutting line for opening the security bag
7:	Micro security overprint

Figure 17 : Schematic view of a security bag

- Make sure that both numbers match the Security bag number specified in the delivery information sheet you have separately received attached to a digitally signed e-mail.
- Check the intactness of the double shrink seal with the micro security overprint (item 4 of the schematic) at both sides of the security bag. The next figure shows a more detailed view of the double shrink seal with the micro security overprint highlighted in a red frame.

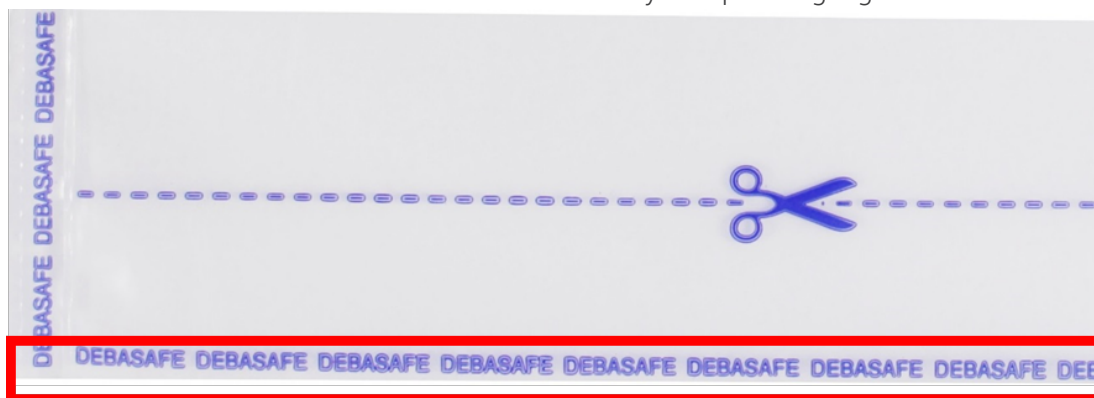


Figure 18 : Micro security overprint



⚠ If the micro security overprint is missing or damaged, do not open the bag. Immediately contact Utimaco IS GmbH to get information about how to proceed.

You can now open the security bag and take the u.trust Anchor PCIe card out of the antistatic wrapping. See also [Unpacking and Handling](#) for further important instructions on unpacking and handling.

### Checking the Device

1. Determine the completeness of the package content as specified in [Deliverables](#).
2. Check that the serial number of the integrated u.trust Anchor card is the same as the one listed in the delivery information sheet. The serial number - CSXXXXXX - is printed on a label on the slot bracket of the PCIe card.
3. Download the product bundle from the Utimaco download portal as described in [Downloading the Product Bundle](#).
4. Calculate the check value. The check value is calculated over the file uTrustAnchor-VX.XX.X.X.zip (hash algorithm SHA-256) and compare it with the check value included in the delivery information sheet.

For example, for calculating the check value (SHA-256) you can use the `sha256sum` Linux command,

```
sha256sum uTrustAnchor-VX.XX.X.X.zip
```

or the `dgst - sha256` OpenSSL command.

```
openssl dgst -sha256 uTrustAnchor-VX.XX.X.X.zip
```

### Checking the smartcards (if purchased)

Check that the serial numbers printed on the delivered smartcards and shown for example in the figure below are the same as included in the delivery information sheet.



Figure 19 : Serial number of the smartcard

### Checking the PIN pad (if purchased)

1. Check that the PIN pad is correctly sealed with two numbered security seals. The security seal numbers must match the ones specified in the delivery information sheet. Make sure that the serial numbers printed on the security seals of the PIN pad and its serial number match the ones specified in the delivery information sheet. All mentioned serial numbers can be found on the bottom of the PIN pad. An example is shown below.



Figure 20 : Serial number and Security seals of the PIN pad

2. Make sure that the connection cables do not show any sign of manipulation and allow connecting the PIN pad to a USB port of the administration computer.



Use only PIN pads delivered by Utimaco.



We recommend not using the PIN pad if any of the conditions above is not fulfilled.



Further steps for HSM identification must be performed. Before these steps can be done, it is for technical reasons required to perform the installation of drivers and tools first, as described in [Bringing into Service](#). Please ensure that afterwards the mandatory next steps of HSM identification are executed. These are described in *Setup the u.trust Anchor - Administration Manual*.

### 4.2.3 Installing the u.trust Anchor PCIe card

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

1. Switch off the computer.
2. Unplug all cables.
3. Open the computer case.
4. Select a free PCIe expansion slot and remove the corresponding slot cover on the rear side of the computer.
5. Insert the u.trust Anchor PCIe card in the computer's PCIe expansion slot. Make sure the card fits securely.
6. Close the computer case.
7. Reconnect the cables.
8. Switch on the computer.

## 4.3 Installation of the u.trust Anchor Driver Software

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

### 4.3.1 Installation on Linux Operating Systems

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

For this reason, the u.trust Anchor driver for Linux is supplied as source code within the product bundle and must be compiled on the target system.

#### 4.3.1.1 Compiling/Installing the Driver

##### Prerequisites

To compile the u.trust Anchor driver on a Linux operating system, the following prerequisites must be available:

- The u.trust Anchor driver package must be available.  
You find the driver package on the product CD in the Software/Linux/Driver directory. The driver supports a maximum of 8 u.trust Anchor PCIe cards. This number can be changed in the source code of the driver.
- Each major Linux distribution has a package for headers, often called `kernel-devel`. Some distributions use other names, for example, `linux-headers-amd64` for a 64-bit Debian. Check the documentation of your distribution. Ensure that this package is installed.
- Ensure that `gcc` is installed.
- Ensure that `make` is installed.
- Root privileges on the computer are required for performing the u.trust Anchor driver installation on a Linux operating system.

##### Check Hardware

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

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

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

## Check OS/Driver

Check if you are running in UEFI or in legacy (BIOS) mode:

```
$ ls /sys/firmware/efi
```

If `/sys/firmware/efi` exists, that means the system uses UEFI.

Check if SecureBoot is enabled:

```
$ mokutil --sb-state
```



If the output shows both UEFI and SecureBoot, the driver will only work if you are running Ubuntu 18 or higher. In all other cases, you will have to disable SecureBoot in your BIOS.

## Build and Install the Driver under Ubuntu/Debian

You find the driver package on the product CD in the `Software/Linux/Driver` directory.

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

```
$ sudo apt install ./cryptoserver-dkms_5.18.0_all.deb
```

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



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

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





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

You find the driver package on the product CD in the Software/Linux/Driver directory.

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

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

For SLES 12, perform the following steps instead:

1. Create a new `temp` directory.

```
mkdir temp
```

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

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

3. Go to this `temp` directory.

```
cd temp
```

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

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

5. Change the value of `allow_unsupported_modules` to `1` in the `/etc/modprobe.d/10-unsupported-modules.conf` file.

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

```
rm -rf temp
```

10. Reboot the computer.

```
reboot
```

On the CentOS/RHEL, the package will only work if you have the `EPEL repository` enabled. A check can be done using `yum repolist`.



The package installation will not automatically sign the module for SecureBoot, so SecureBoot needs to be disabled.

## Configure the Driver

By default, the driver will not enable the cHSM slots, nor the network interface. To do so, set up a `modprobe` configuration file to set `DeviceMask` and `DeviceFlags`, e.g.

```
/etc/modprobe.d/cryptoserver.conf
```

```
options cryptoserver DeviceMask=0xFFFFFFFF DeviceFlags=2
```

Reload the driver to let the changes take effect:

```
$ sudo rmmod cryptoserver
$ sudo modprobe cryptoserver
```



The '\$ sudo rmmod cryptoserver' command may fail if the driver was not loaded.

### Check that the Kernel Module is Working

1. Check for `cryptoserver` in the output of `lsmod`:

```
$ lsmod | grep cryptoserver
```

2. Check that the module did not report any errors:

```
$ dmesg | grep cs
```

3. Check that the device `state` is displayed as `enabled`:

```
$ cat /proc/driver/cryptoserver
```



A reboot is recommended to check, that the driver loads automatically.

#### 4.3.1.2 Performing a Functional Test

To verify that the driver has been installed correctly and that the u.trust Anchor is working properly, follow these steps:

1. Check for `cryptoserver` in the output of the `lsmod`:

```
$ lsmod | grep cryptoserver
Cryptoserver                90112      0
```

2. Check that the module did not report any errors:

```
$ dmesg | grep cs
[ 368.435829] :cs_init_module: cryptoserver driver version 5.20.0
[ 368.435851] :cs_init_module: Major Number: 237
```

```
[ 368.435867] :cs_probe: device found: 168a:c071 168a:0007 model:8 [CSAR-
Series] devfn:0 phys
[ 368.475584] :cs_probe: probe cs2.0 OK
[ 368.475617] :cs_probe: probe cs2.1 OK
[ 368.475642] :cs_probe: probe cs2.2 OK
[ 368.475682] :cs_probe: probe cs2.3 OK
[ 368.475790] :cs_probe: probe cs2.4 OK
[ 368.475840] :cs_probe: probe cs2.5 OK
[ 368.475869] :cs_probe: probe cs2.6 OK
[ 368.475890] :cs_probe: probe cs2.7 OK
[ 368.481040] :cs_probe: probe cs2.8 OK
[ 368.483694] :cs_probe: probe cs2.9 OK
[ 368.483741] :cs_probe: probe cs2.10 OK
[ 368.483777] :cs_probe: probe cs2.11 OK
[ 368.483810] :cs_probe: probe cs2.12 OK
[ 368.483845] :cs_probe: probe cs2.13 OK
[ 368.483875] :cs_probe: probe cs2.14 OK
[ 368.484311] :cs_probe: probe cs2.15 OK
[ 368.484362] :cs_probe: probe cs2.16 OK
[ 368.484405] :cs_probe: probe cs2.17 OK
[ 368.484444] :cs_probe: probe cs2.18 OK
[ 368.484476] :cs_probe: probe cs2.19 OK
[ 368.484746] :cs_probe: probe cs2.20 OK
[ 368.484778] :cs_probe: probe cs2.21 OK
[ 368.484809] :cs_probe: probe cs2.22 OK
[ 368.484843] :cs_probe: probe cs2.23 OK
[ 368.484880] :cs_probe: probe cs2.24 OK
[ 368.484915] :cs_probe: probe cs2.25 OK
[ 368.484973] :cs_probe: probe cs2.26 OK
[ 368.485023] :cs_probe: probe cs2.27 OK
[ 368.485054] :cs_probe: probe cs2.28 OK
[ 368.485095] :cs_probe: probe cs2.29 OK
[ 368.485125] :cs_probe: probe cs2.30 OK
[ 368.485159] :cs_probe: probe cs2.31 OK
[ 368.485184] :cs_init_module: cryptoserver driver was successfully
registered
```

3. . Check that the module status is "ok"

```
cat /proc/driver/cryptoserver
cryptoserver driver version 5.20.0
```

```
card slot          model device  alias      used state    type
-----
```

```

0 0000:02:00.0 8 cs2.0 cs2.0.0 0 enabled physfn (0/28 vf
used)
0 0000:02:00.0 8 cs2.1 cs2.0.1 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.2 cs2.0.2 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.3 cs2.0.3 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.4 cs2.0.4 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.5 cs2.0.5 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.6 cs2.0.6 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.7 cs2.0.7 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.8 cs2.0.8 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.9 cs2.0.9 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.10 cs2.0.10 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.11 cs2.0.11 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.12 cs2.0.12 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.13 cs2.0.13 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.14 cs2.0.14 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.15 cs2.0.15 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.16 cs2.0.16 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.17 cs2.0.17 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.18 cs2.0.18 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.19 cs2.0.19 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.20 cs2.0.20 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.21 cs2.0.21 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.22 cs2.0.22 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.23 cs2.0.23 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.24 cs2.0.24 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.25 cs2.0.25 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.26 cs2.0.26 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.27 cs2.0.27 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.28 cs2.0.28 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.29 cs2.0.29 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.30 cs2.0.30 0 enabled child -> cs2.0
0 0000:02:00.0 8 cs2.31 cs2.0.31 0 enabled child -> cs2.0

```

The `gladm system-get-info` as well as `csadm Getinfo` commands can also be used to perform this check.

### 4.3.1.3 Updating the Driver on Linux

The driver cannot be updated separately, but rather exclusively with a device update.

### 4.3.1.4 Uninstalling the Driver

Depending on the used operating system, you can remove already installed driver packages by running one of the following commands and adjusting the version number as necessary.

```

#centos/rhel
$ sudo yum remove cryptoserver-dkms
# fedora

```

```
$ sudo dnf remove cryptoserver-dkms
# opensuse/sles
$ sudo zypper remove cryptoserver-dkms
# Ubuntu/Debian
$ sudo apt remove cryptoserver-dkms
```

### 4.3.2 Installation on Windows Operating Systems

The u.trust Anchor driver package consists of three files:

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



The files are located in the product bundle in the following directory:

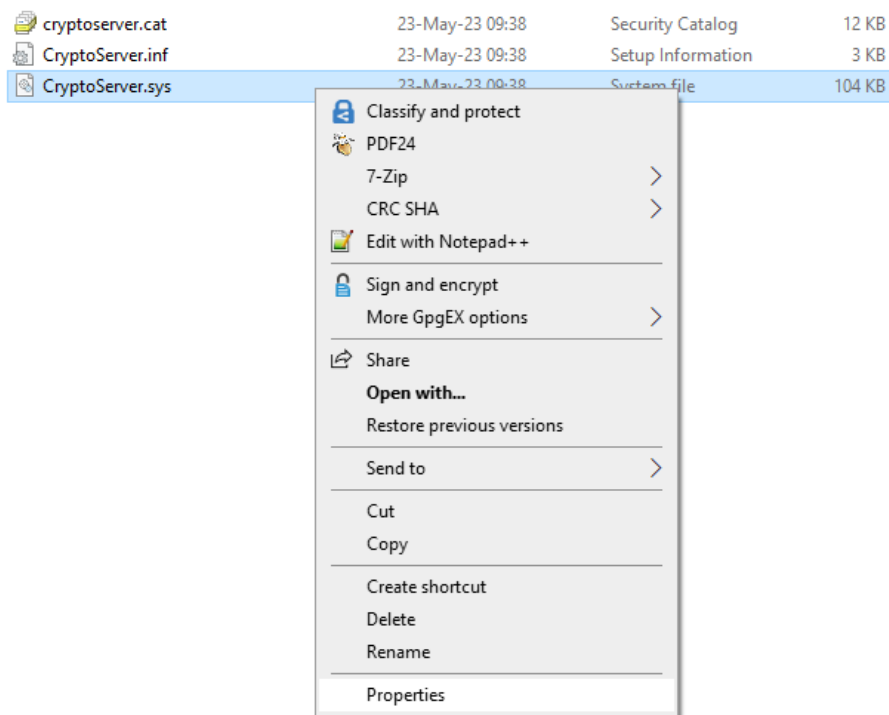
```
Software\Windows\Driver\bin
```

#### 4.3.2.1 Certificate Chain Verification

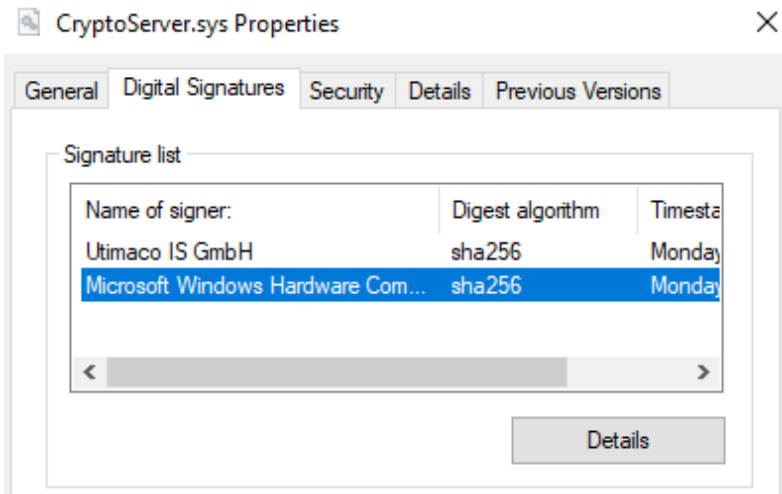
The driver has been signed by Microsoft and the corresponding certificate chain has to be installed.

Verify that the certificate chain has been installed correctly:

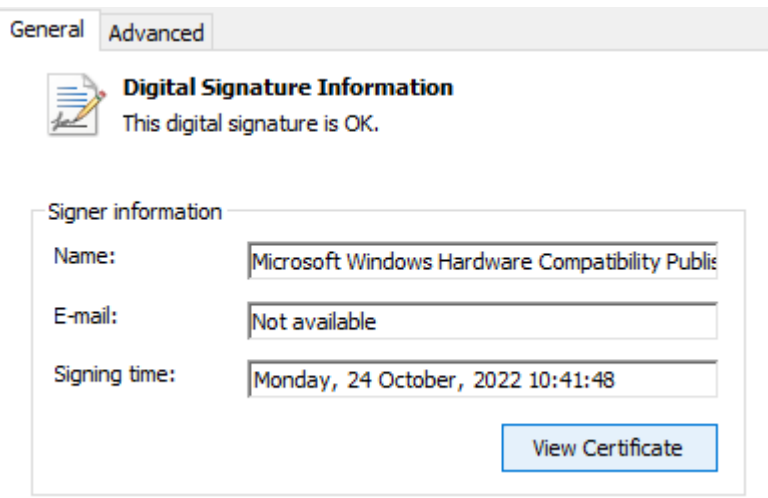
1. Right click the file `CryptoServer.sys` and select **Properties**.



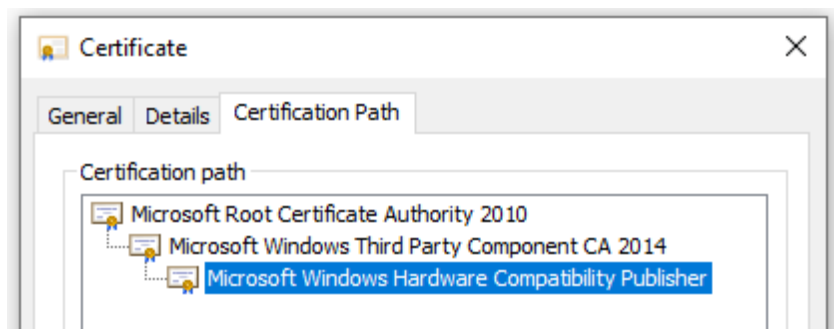
2. Go to **Digital Signature**, select Microsoft's signature from the list and click on **Details**.



3. Click on **View Certificate**.



4. Go to **Certification Path**.



The chain should look like this:

- CN = Microsoft Root Certificate Authority 2010
- CN = Microsoft Windows Third Party Component CA 2014
- CN = Microsoft Windows Hardware Compatibility Publisher

#### 4.3.2.2 Installing or Updating the Driver



Local Administrator rights for the host computer are required to install/update the u.trust Anchor driver.

#### Prerequisites



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

To install/update the u.trust Anchor driver on a computer with a Windows operating system, proceed as follows:

### Procedure

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



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

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

#### Typical

The u.trust Anchor administration tools (gladm, CAT, csadm etc.) and the u.trust Anchor documentations are installed.

#### Custom

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

#### Complete

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

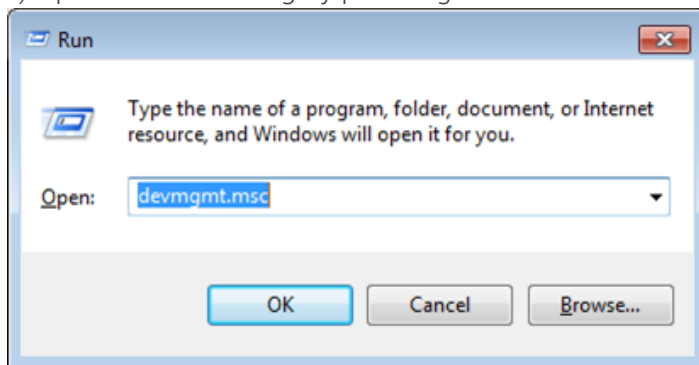
Select **Custom**.

5. The **Select the features to be installed** dialog box opens. By default, **Administration** and **Documentation** are selected.
6. Clear all items that should remain unchanged (not be installed/updated). They are indicated by a red X.

7. Click the small black triangle next to **Drivers > CryptoServer** and select **Will be installed on local hard drive**.
8. Click **Next**.
9. In the **Ready to Install** dialog box, click **Install**.
10. Click **Finish** to complete the software installation.

11. Start the device manager.

a) Open the **Run** dialog by pressing **Windows + R**.



b) Enter `devmgmt.msc` into the text field and click **OK**.

The Windows device manager opens.

**u.trust Anchor** appears under **Cryptographic Devices**.

12. Start the registry editor.

a) Open the **Run** dialog by pressing **Windows + R**.

b) Enter `regedit` into the text field and click **OK**.

c) Verify whether the registry key

**Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CryptoServer\Parameters\DeviceMask** exists and has the following value: `0xFFFFFFFF`

d) If this registry key does not exist, create this registry key: Open

**Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CryptoServer\Parameters** in the registry editor. Click with the right mouse button in the right pane and select **New > DWORD (32-bit) Value**. Enter `DeviceMask`. Press the **Enter** key.

Double-click **DeviceMask**. In the **Value data** field, enter `FFFFFFFF`. Ensure that the **Hexadecimal** option is active. Click **OK**.

e) If the **DeviceMask** registry key has been created in the previous substep, restart the driver via the device manager (In the device manager, click **Cryptographic Devices > u.trust Anchor** with the right mouse button and select **Disable device**. Then select

**Enable device.**) Or, as an alternative, restart the computer, for example, by performing the `shutdown -r -t 0` command in a command line.



The u.trust Anchor driver has been installed/updated.

### 4.3.2.3 Performing a Functional Test on Windows

To check if the driver has been installed correctly and that the u.trust Anchor is functioning as it should, follow these steps:

1. Press **Windows+R** to open **Run** box.
2. Type `cmd` and then click **OK** to open a command line.
  - a. Input the following command sequence to start the gladm administration tool from the product bundle to determine the status of the u.trust Anchor and to check the connection to the u.trust Anchor PCIe card. This assumes that your product bundle drive is the D: drive and that the u.trust Anchor PCIe card is in the first slot.

```
D:
cd Software\Windows\Administration
gladm -d PCI:0 system-get-info
```



`-d` refers to the device specifier/address/name. For details about the `-d` parameter, see *Specifying a Device* in the [u.trust Anchor - Administration Manual](#).



Do not confuse the `-d` parameter for gladm with the `Dev` parameter for csadm. For details about the `Dev` parameter, see *Syntax of csadm* in the [u.trust Anchor - csadm Manual](#).



If the driver has been installed correctly and the u.trust Anchor is functioning as it should, you should see the following information:

- The device system version and build version running on the device
- The software version of the sensory controller
- The hardware revision number
- The UID of the device
- The serial number of the device
- The device type
- Alarms present, if applicable
- Zeroization events, if applicable
- Presence or absence of vendor secret on the device
- Presence or absence of DAK certificate on the device

3. Perform the following command to create a cHSM in cHSM slot 1.

Example:

```
gladm -d PCI:0 chsm-create myADMIN.key 1
```

Do not confuse cHSM slots with PKCS#11 slots and MBK slots.

4. Verify the state of that cHSM.

Example:

```
csadm Dev=PCI:0.1 GetState
```

The `1` in `PCI:0.1` indicates cHSM slot 1.

Example output:

```
mode = Operational Mode
FIPS mode = ON
state = INITIALIZED (0x00100004)
temp = ---
alarm = OFF
bl_ver = 7.00.0.0 (Model: u.trust Anchor cHSM)
```

```
hw_ver = 7.00.0.0
uid = 5f3dd606 b6a28c43 |_= G ,I9 C |
adm1 = a796c345 45224b3b 893895f5 a6ddf906 | EE"K; 8 |
adm2 = 53656375 72697479 53657276 65720000 |SecurityServer |
adm3 = 302e3234 2e310000 00000000 00000000 |0.24.1 |
```

If you cannot communicate with the u.trust Anchor, check that the PCIe card has been mounted correctly and check in the Windows Device Manager to see whether the driver has been installed correctly. After that, repeat the functional test.

If you still cannot communicate with the u.trust Anchor, contact either the reseller who supplied this u.trust Anchor or the Utimaco IS GmbH Customer Service team.

#### 4.3.2.4 Uninstalling the Driver on Windows

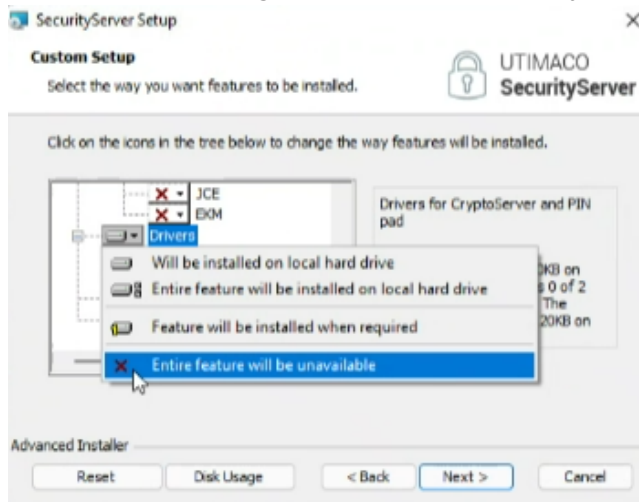


You must uninstall the driver from your computer before you remove the u.trust Anchor. It is not possible to uninstall the driver after you have removed the u.trust Anchor from the computer.

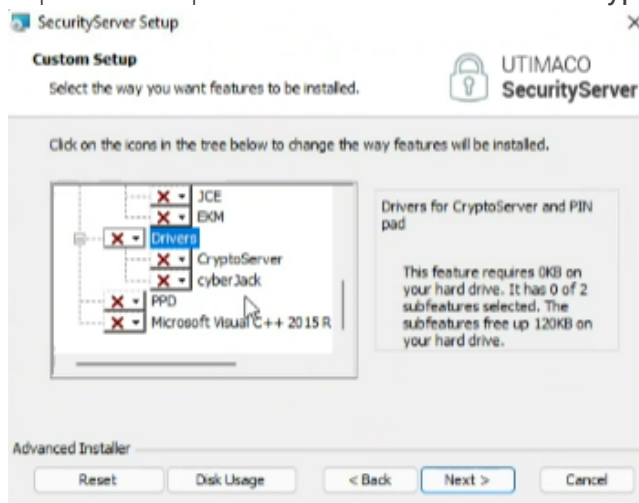
If you want to uninstall the driver, follow the steps below.

1. Click the Windows button in the taskbar.
2. Search for **Apps & features** (**Programs and Features** on older Windows operating systems) in the text field.
3. Search for the **Utimcao SecurityServer** entry.
4. Click the three dots to the right of the **Utimcao SecurityServer** entry.
5. Click **Modify**.
6. Click **Yes**.  
The **SecurityServer Setup Wizard** opens.
7. Click **Next**.
8. Click **Modify**.
9. Scroll down to the **Drivers** entry.

10. Click the black triangle to the left of this entry.



11. Click Entire feature will be unavailable.
12. Repeat the steps 10 and 11 for the Drivers > CryptoServer entry.



13. Click Next.
14. Click Install.
15. Click Finish.



The **u.trust Anchor** driver will now be uninstalled and removed from your computer. After you close the wizard, the device **u.trust Anchor** is also deleted from the **Device Manager** display.

16. Shut down the Windows operating system before removing the u.trust Anchor plug-in card.

## 4.4 Identification and Claiming of u.trust Anchor

Several procedures must be followed to ensure the safety and integrity of the device:

1. **Verifying the Authenticity of the Device**

Note that this step is optional. It is necessary if you want to verify the HSM is genuine and manufactured by Utimaco. This step is expressly recommended from a safety perspective and should be carried out before other certificates are uploaded.

2. **Checking Component Versions**

The device's hardware revision number, software version, and sensory controller version must be verified.

3. **Changing the Authentication Token of the Global Initial Administrator**

The Global Administrator must change the Global Initial Admin Key (GIAK) into an individual Global Admin Authentication Key (GAAK) to change the device state to *INITIALIZED*.

4. **Importing an Initial Operator Secret**

The Global Administrator must create a Wrapping Key, wrap the Operator Secret, and import the wrapped operator secret back to the device.

5. **Importing an Operator Certificate**

As a final step, an Operator Certificate must be imported by the Global Administrator.

All steps are described in detail in the respective sub-chapters of chapter *Setup* in the [u.trust Anchor - Administration Manual](#).

## 5 Replacing the Battery

A battery (carrier battery) ensures the sensor system and the quenching circuit can function even when the u.trust Anchor is switched off.

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

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



This battery is not rechargeable.

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

For this reason, you should check the battery status regularly. For this please use the `gladm` command:

```
gladm system-metrics
```

This command displays a list of system information. Two extra fields in this list are dedicated to the state of the battery included in this module: the "`csar-main-battery`" and the "`csar-ext-battery`". If the corresponding outputs are ok, that means the battery voltage is within acceptable ranges. Otherwise you must replace it as soon as possible. The external battery is only relevant for the u.trust Anchor LAN.



Read the instructions carefully before you change the battery.

1. Before replacing the battery, make sure you have the correct type of battery. We recommend you use only Panasonic CR2477 cell batteries (3V, Lithium, Ø 24.5 mm, L = 7.7 mm) or equivalent.





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

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

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



Clean both battery contacts with alcohol.

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

3. It is recommended to take encrypted snapshots of existing cHSMs by using

```
gladm chsm-snapshot
```

before changing the battery.

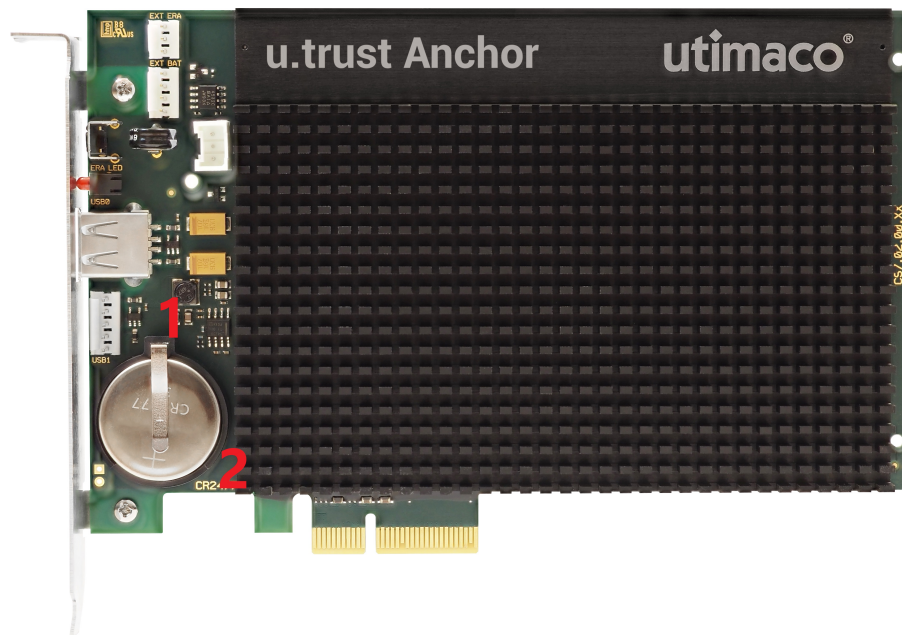
Those can be restored after restarting the device by first loading an operator secret with the `gladm` command

```
gladm key-import-operator-secret
```

and then running the `gladm` command

```
gladm chsm-restore
```

4. Turn off the computer.
5. Remove the u.trust Anchor from the computer.
6. Consider that you have a maximum of 5 minutes for the actual battery replacement in the next two steps. For this period of time, it is guaranteed that a capacitor supplies the PCIe card with electric current and that the data on the PCIe card is not deleted. After a maximum of 30 minutes without a carrier battery, the data on the PCIe card is deleted in any case and the device enters an alarm state.
7. On the reverse of the battery clips you see a hole in the board. Remove the battery (2) from its mounting clips (1).



## 8. Change the battery



Make sure the polarity is correct (see the label on the u.trust Anchor). If the polarity is incorrect, the data on the device will be deleted.





If you remove any power supply (battery and power supply via the PCIe interface) from the PCIe card, the power supply for this PCIe card is guaranteed by means of a capacitor for 5 minutes. Within this time, you have to replace the battery to be on the safe side. If you need more time, you might be too late because an alarm might have been triggered and all sensitive data on the u.trust Anchor is deleted.

If you remove any power supply (battery and power supply via the PCIe interface) from the PCIe card, it is guaranteed that after 30 minutes (at the latest) an alarm is triggered and all sensitive data on the u.trust Anchor is deleted.

9. Reinstall the u.trust Anchor.
10. Make a note of the next battery replacement date.
11. Turn on the computer.
12. Check the status of the u.trust Anchor by using the command `gladm system-info`.
13. Set the time and date of the device using the gladm command

```
gladm system-set-time [-t <val>] [-l <val>] [-u <val>]
```

if required.

14. Restore snapshots like described above if required.



Now, your u.trust Anchor is ready for use again.

## 6 Uninstalling the u.trust Anchor PCIe card



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

1. Switch off the computer, unplug all the cables and open the computer casing.
2. Remove the u.trust Anchor carefully from the PCIe slot. You must never use a tool (for example, screwdriver) to lever the card out of the slot.
3. Close the computer case and reconnect all the cables.
4. Put the u.trust Anchor card into an antistatic wrapping.



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



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

## 7 Disposing of the u.trust Anchor

To dispose of your u.trust Anchor perform the following steps.

1. Perform an External Erase to securely delete all sensitive data from your u.trust Anchor.
  - a. To securely delete all sensitive data from your u.trust Anchor by pushing the Erase-button (2) for at least 10 seconds with an appropriate screwdriver.
  - b. The LED flash light (1) flashes up red to confirm the activation of the Erase-button.

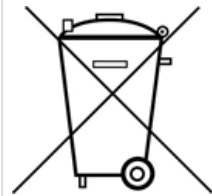


Figure 21 : Slot plate of the u.trust Anchor



You can perform an External Erase even if the u.trust Anchor is not plugged in a computer or if the computer is switched off.

2. Of course, you also have the option of returning the u.trust Anchor that you no longer require to us, Utimaco IS GmbH, as the manufacturer. Below you will find a description of how to dispose of the u.trust Anchor and the battery in an environmentally friendly way. If you want to dispose of the u.trust Anchor yourself, please note that in the u.trust Anchor carrier you will find a battery which must be disposed of in an environmentally friendly way
3. Remove the battery from the u.trust Anchor and note the following general information about rechargeable and non-rechargeable batteries (in accordance with the German Notice Requirement According to §18 BattG (the law concerning batteries)).



You are not permitted to throw away rechargeable or used batteries in the normal household waste. Consumers are obliged to bring batteries to a suitable municipal or commercial collection point. Rechargeable and used batteries can contain harmful materials or heavy metals that can damage the environment and health. Batteries are reused. They contain important raw materials such as iron, zinc, manganese or nickel.

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

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

## 8 Technical Data

<b>Dimensions</b>	PCI Express (PCIe) plug-in card: Length: 167.65 mm ("half" length) Height: 111.15 mm ("full" height)
<b>Weight</b>	420 g
<b>Battery</b>	3V, Lithium cell battery, Ø 24.5 mm, L = 7.7 mm, Panasonic CR2477 or equivalent
<b>Ports</b>	PCIe 3.x x1 USB 2.0 x2
<b>Environmental temperature</b>	Operation: +10 °C to +35 °C (+50 °F to +95 °F) Storage: -10 °C to +55 °C (+14 °F to +131 °F)
<b>Humidity</b>	10 % to 95% relative humidity, non-condensing
<b>MTBF</b>	174.000 hours (as specified in MIL-HDBK-217)
<b>RoHS compliance</b>	Yes
<b>WEEE</b>	National register for waste electric equipment (EAR) DE65203472
<b>Conformity</b>	Interference emission in accordance with EN 55022 Class B Influence of interference in accordance with EN 61000-6-2 (industry) Equipment safety in accordance with IEC 60950-1:2001/EN 60950-1:2001 (CB scheme) FCC 47 CFR Ch. 1 Part 15 Class B

## 9 Contact Address for Support Queries

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH  
Germanusstr. 4  
52080 Aachen  
Germany

### RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

### Other Support Queries

- Mail (preferred contact method)  
[support@utimaco.com](mailto:support@utimaco.com)  
Attach the diagnostic information to your email.
- Web portal  
<https://support.hsm.utimaco.com/support/cases/new/>  
The diagnostic information will be requested in our response if necessary.
- By phone  
AMERICAS +1-844-UTIMACO (+1 844-884-6226)  
EMEA +49 800-627-3081  
APAC +81 800-919-1301  
The diagnostic information will be requested in our response if necessary.



## 10 References

<i><b>Title/Company</b></i>	<i><b>Document No.</b></i>
u.trust Anchor - Administration Manual	2020-0035
u.trust Anchor - csadm Manual	2021-0037