

CryptoServer PCIe

Se-Serie Gen2

Betriebsanleitung

Impressum

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Telefon	AMERICAS: +1-844-UTIMACO (+1 844-884-6226) EMEA: +49 800-627-3081 APAC: +81 800-919-1301
Internet	https://support.hsm.utimaco.com
E-Mail	support@utimaco.com
Dokumentversion	1.2.17
Datum	2024-10-24
Status	Final
Dokument-Nr.	M015-0001-de
Alle Rechte vorbehalten	<p>Kein Teil dieser Dokumentation darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne schriftliche Genehmigung der Utimaco IS GmbH reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.</p> <p>Utimaco IS GmbH behält sich das Recht vor, diese Dokumentation ohne vorherige Ankündigung zu verbessern oder zu verändern. Utimaco IS GmbH übernimmt keine Haftung für Druckfehler und andere Fehlinformationen.</p> <p>Alle Markennamen, Warenzeichen und eingetragenen Warenzeichen sind Eigentum ihrer rechtmäßigen Eigentümer.</p>

Inhaltsverzeichnis

1	Einleitung	5
1.1	Über dieses Handbuch	5
1.1.1	Zielgruppe für dieses Handbuch	5
1.1.2	Inhalt des Handbuchs	5
1.1.3	Typographische Konventionen	6
1.2	Weitere Handbücher	6
1.3	Import- und Exportvorschriften	8
1.4	Transportschäden	8
1.5	Lieferumfang	8
2	Allgemeine Sicherheitshinweise	9
2.1	Transport und Lagerung	9
2.2	Batterie	10
2.3	Den CryptoServer sicher transportieren	10
2.4	Umgebungstemperatur	12
3	Komponenten des CryptoServer Se Gen2 (PCIe)	14
4	Auspacken und Handhabung	15
4.1	Allgemeine Hinweise	16
4.2	Den CryptoServer Se Gen2 einbauen	17
4.3	Den CryptoServer Se Gen2 ausbauen	17
5	Installation der CryptoServer-Treiber-Software	18
5.1	Installation auf Windows-Betriebssystemen	18
5.1.1	Treiber installieren	18
5.1.2	Funktionstest durchführen	21
5.1.3	Treiber deinstallieren	22
5.1.4	Treiber aktualisieren	22
5.2	Installation auf Linux-Betriebssystemen	23
5.2.1	Treiber kompilieren/installieren	23
5.2.2	Funktionstest durchführen	26
5.2.3	Treiber aktualisieren	27
5.2.4	Treiber deinstallieren	28
6	Batterie wechseln	30
7	Entsorgung des CryptoServer Se Gen2	35
8	Technische Daten	36
9	Kontaktadresse für Support-Anfragen	37
	Referenzliste	38

1 Einleitung

Wir danken Ihnen, dass Sie unser Sicherheitssystem CryptoServer der Se-Serie Gen2 (im Folgenden CryptoServer Se Gen2 genannt) erworben haben und hoffen, dass Sie mit unserem Produkt zufrieden sind. Sollten Sie irgendwelche Beanstandungen oder Vorschläge haben, sind wir Ihnen für eine Mitteilung dankbar.

Das Product Bundle kann von der folgenden Website heruntergeladen werden:

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

Für die Nutzung des Downloadportals ist eine Registrierung zwingend erforderlich, zudem muss der Bereich für ein bestimmtes Produkt, z.B. „SecurityServer Se Gen2“, freigeschaltet sein.

1.1 Über dieses Handbuch

Diese Betriebsanleitung enthält alle notwendigen Informationen über die sachgerechte Verwendung der Hardware des CryptoServer Se Gen2 sowie wichtige Sicherheitshinweise, die unbedingt zu befolgen sind, um die Betriebssicherheit des CryptoServer Se Gen2 gewährleisten zu können.

1.1.1 Zielgruppe für dieses Handbuch

Dieses Handbuch richtet sich an die verantwortlichen Systemadministratoren, die einen CryptoServer der Se-Serie Gen2 in Betrieb nehmen und verwalten müssen.

1.1.2 Inhalt des Handbuchs

Kapitel 2 enthält Sicherheitshinweise, die vor dem Auspacken und der Inbetriebnahme des CryptoServer Se Gen2 sorgfältig durchzulesen sind.

Kapitel 3 zeigt die verschiedenen Komponenten des CryptoServer Se Gen2.

Kapitel 4 beinhaltet allgemeine Hinweise zum sicheren Auspacken und Umgang mit dem CryptoServer Se Gen2, sowie beschreibt die allgemeine Vorgehensweise beim Ein- und Ausbauen der CryptoServer Se Gen2 PCIe-Karte.

Kapitel 5 beschreibt, wie der Treiber des CryptoServer Se Gen2 auf dem Host-Rechner unter Windows- und Linux-Betriebssystemen installiert, getestet, aktualisiert und wieder entfernt wird.

Kapitel 6 gibt Anweisungen zum Wechseln der Batterie des CryptoServer Se Gen2.

Kapitel 7 nennt, was zu beachten ist, wenn der CryptoServer Se Gen2 entsorgt werden soll.

Kapitel 8 ist eine Übersicht über die wesentlichen technischen Daten des CryptoServer Se Gen2.

Kapitel 9 enthält die Kontaktdaten des Herstellers, die Sie verwenden können falls Sie Fragen zum CryptoServer Se Gen2 haben oder Probleme während des Betriebs des CryptoServer Se Gen2 auftreten sollten.

1.1.3 Typographische Konventionen

In diesem Handbuch verwenden wir die folgenden Schreibweisen:

Fettschrift	Elemente der grafischen Benutzeroberfläche (GUI), z. B., Menüoptionen
Festbreitenschrift	Dateinamen, Dateispeicherorte, Kommandos, Dateiausgaben, Programmcode-Abschnitte
<i>Kursiv</i>	Referenzen und wichtige Begriffe

Wir haben wichtige Hinweise und Informationen mit Symbolen gekennzeichnet.



Hier finden Sie wichtige Sicherheitshinweise, die Sie befolgen sollten.



Hier finden Sie einen zusätzlichen Hinweis oder eine ergänzende Information.

1.2 Weitere Handbücher

Der CryptoServer wird als PCI-Express (PCIe)-Einsteckkarte in den folgenden Serien zur Verfügung gestellt:

- CryptoServer CSe-Serie
- CryptoServer Se-Serie
- CryptoServer Se-Serie Gen2

Der CryptoServer LAN (Appliance) wird in den folgenden Serien zur Verfügung gestellt:

- CryptoServer LAN CSe-Serie
- CryptoServer LAN Se-Serie
- CryptoServer LAN Se-Serie Gen2

Für die CSe-, Se-Serie und die Se-Serie Gen2 der CryptoServer-PCIe-Karten und des CryptoServer LAN (Appliance) stellen wir auf der Produkt-CD die folgenden Handbücher zur Verfügung:

Quick Start Guides (Kurzanleitungen)

Diese Handbücher finden Sie im Hauptverzeichnis der SecurityServer Produkt-CD. Sie sind nur in englischer Sprache verfügbar, umfassen nicht alle möglichen Einsatzszenarios und sind als Ergänzung zu der Produktdokumentation auf der SecurityServer Produkt-CD gedacht.

- *CryptoServer LAN V5 - Quick Start Guide*
Wenn Sie eine schrittweise Anleitung benötigen, um Ihr CryptoServer LAN in Betrieb zu nehmen, um einen Rechner (Windows) für die Administration des CryptoServer vorzubereiten und um die Administration des CryptoServer mit dem Java-basierten CryptoServer Administration Tool (CAT) zu beginnen, lesen Sie bitte dieses Handbuch.
- *CryptoServer PCIe - Quick Start Guide for Linux*
Wenn Sie eine schrittweise Anleitung benötigen, um Ihre CryptoServer-PCIe-Karte in Betrieb zu nehmen, um den CryptoServer-Treiber auf einem Rechner mit einer minimalen RHEL-Installation zu installieren und um die Administration des CryptoServer mit dem CryptoServer Command-line Administration Tool (csadm) zu beginnen, lesen Sie bitte dieses Handbuch.
- *CryptoServer PCIe - Quick Start Guide for Windows*
Wenn Sie eine schrittweise Anleitung benötigen, um Ihre CryptoServer-PCIe-Karte in Betrieb zu nehmen, um den CryptoServer-Treiber auf einem Windows-Rechner zu installieren und um die Administration des CryptoServer mit dem CryptoServer Command-line Administration Tool (csadm) zu beginnen, lesen Sie bitte dieses Handbuch.

Handbücher für Systemverwalter

Diese Handbücher finden Sie auf der Produkt-CD im folgenden Verzeichnis:

...Documentation\Administration Guides\

- *CryptoServer – Administration Manual*
Wenn Sie eine CryptoServer-PCIe-Karte oder einen CryptoServer LAN mit Hilfe des CryptoServer Administration Tool (CAT) administrieren wollen, lesen Sie bitte dieses Handbuch. Es enthält außerdem eine ausführliche Funktionsbeschreibung des CryptoServer, die für die sach- und produktgerechte Bedienung nötig ist.
- *CryptoServer LAN V5 – Administration Manual*
Wenn Sie einen CryptoServer LAN (Appliance) administrieren wollen, lesen Sie bitte dieses Handbuch. Da im CryptoServer LAN eine CryptoServer-Einsteckkarte eingebaut ist, lesen Sie bitte auch das Handbuch *CryptoServer – Administration Manual*.
- *CryptoServer - Troubleshooting*
Wenn bei der Verwendung einer CryptoServer-PCIe-Karte oder eines CryptoServer LAN (Appliance) Probleme auftreten, lesen Sie bitte dieses Handbuch.
- *CryptoServer - PKCS#11 P11CAT - Manual*
Wenn Sie die PKCS#11 R3-Schnittstelle mit Hilfe des PKCS#11 CryptoServer Administration Tool (P11CAT) administrieren wollen, lesen Sie bitte dieses Handbuch.
- *CryptoServer -csadm Manual*
Wenn Sie eine CryptoServer-PCIe-Karte oder einen CryptoServer LAN mit Hilfe des CryptoServer Command-line Administration Tool (csadm) administrieren wollen, lesen Sie bitte dieses Handbuch (nur in englischer Sprache verfügbar).

Betriebsanleitungen

Diese Handbücher finden Sie auf der Produkt-CD im folgenden Verzeichnis:

...Documentation\Operating Manuals\. Sie enthalten alle nötigen Informationen über die sachgerechte Verwendung der Hardware des CryptoServer LAN (Appliance) bzw. der CryptoServer-PCIe-Karte.

1.3 Import- und Exportvorschriften



Der Export ins und der Einsatz im Ausland von CryptoServer Se Gen2 unterliegt den gesetzlichen Außenhandelsbestimmungen der Bundesrepublik Deutschland und ist genehmigungspflichtig.

Für den Import des CryptoServer Se Gen2 müssen die gesetzlichen Bestimmungen oder anderweitige Vorschriften der jeweiligen Zielländer (Einfuhrgenehmigung) beachtet werden. Bitte wenden Sie sich an Ihre nationale Einfuhrbehörde für genaue Informationen.

1.4 Transportschäden

Mit dem CryptoServer Se Gen2 haben Sie ein Gerät erworben, das vor der Auslieferung sorgfältig getestet und verpackt wurde. Leider können gelegentlich durch den Transport oder unsachgemäße Zwischenlagerung Geräte in beschädigtem Zustand bei Ihnen eintreffen.

Sollte dieser Fall eingetreten sein, setzen Sie sich unverzüglich mit Ihrem Händler oder direkt mit uns (siehe Telefonnummer und E-Mail-Adresse im Kapitel 9) in Verbindung. Bitte halten Sie zu diesem Zweck den der Lieferung beigefügten Lieferschein und die Seriennummer des Gerätes bereit.

1.5 Lieferumfang

Zum Lieferumfang des CryptoServer Se Gen2 gehören:

- ein CryptoServer Se Gen2 (PCI Express)-Einsteckkarte
- eine *CryptoServer PCIe Se-Serie Gen2 Betriebsanleitung* (dieses Handbuch)

Für die Administration des CryptoServer Se Gen2 können optional Smartcards eingesetzt werden. Diese Smartcards, sowie das passende PIN-Pad, können bei der Utimaco IS GmbH erworben werden.

Andere PIN Pads und Smartcards, die nicht von der Utimaco IS GmbH erworben worden sind, können für die Administration des CryptoServer Se Gen2 nicht verwendet werden.

2 Allgemeine Sicherheitshinweise



Bitte befolgen Sie alle am Gerät oder in dieser Anleitung aufgeführten Warnungen, Sicherheitshinweise und Anleitungen, andernfalls kann die Utimaco IS GmbH keinerlei Gewährleistung für entstandene Schäden übernehmen.

Der CryptoServer Se Gen2 ist ein Hardware-Sicherheitsmodul. Er ist mit einer Sensorik ausgerüstet, die bei mechanischen Einwirkungen sowie bei Über- bzw. Unterschreiten der Umgebungstemperatur alle Daten im Gerät löscht.



Lesen Sie vor dem Auspacken und der Inbetriebnahme die folgenden Sicherheitshinweise sorgfältig durch, um die Betriebssicherheit des CryptoServer Se Gen2 zu gewährleisten und ein unbeabsichtigtes Auslösen der Sensorik zu vermeiden. Bewahren Sie diese Anleitung sicher und stets griffbereit auf.

Führen Sie keinerlei Reparaturen am CryptoServer Se Gen2 aus.

2.1 Transport und Lagerung

Beachten Sie beim Transport und Lagerung unbedingt folgende Hinweise:

- Transportieren und lagern Sie den CryptoServer Se Gen2 nur in der Originalverpackung und Antistatikfolie.
- Obwohl es keinen Bewegungssensor auf der CryptoServer-PCIe-Karte gibt, der eine Löschung von Daten anstoßen könnte, vermeiden Sie Stöße und Vibrationen, sowie sonstige mechanische Einwirkungen auf die Verpackung.
- Stellen Sie sicher, dass die Umgebungstemperatur bei Lagerung des CryptoServer Se Gen2 stets innerhalb des Bereichs zwischen -10 °C und +55 °C (+14 °F und +131 °F) liegt.
- Stellen Sie sicher, dass bei einer längeren Lagerung die Batteriewechselzeit nicht überschritten wird. Für Details siehe Kapitel 2.2, "Batterie".
- Verwahren Sie dieses Handbuch zusammen mit dem CryptoServer Se Gen2 auf, so dass dieses bei einem erneuten Einbau zur Verfügung steht.
- Der PCIe-Anschluss ist empfindlich und kann durch Kraft bzw. die Anzugskraft der Halterungen am Rechner, in dem der CryptoServer eingebaut ist, während Transport oder bei Verschiebung bzw. Bewegung beschädigt oder sogar gebrochen werden.
- Auf der Leiterplatte des CryptoServer in der Nähe der PCIe-Halterung befindet sich ein Punkt mechanischer Belastung, der beschädigt werden kann.
- Für die CryptoServer-Leiterplatte ist eine maximale Verbiegung von 2 mm über ihre Oberfläche zulässig.

Aus diesen Gründen ist beim Transport sowie bei der Lagerung der CryptoServer-PCIe-Karten aller Serien besondere Vorsicht erforderlich. Lesen Sie zusätzlich Kapitel 2.3, "Den CryptoServer sicher transportieren". Wir empfehlen, die PCIe-Karte vor einem geplanten Transport oder Bewegung aus dem Rechner auszubauen und sie danach wieder einzubauen. Alle kryptographischen Schlüssel, die auf der PCIe-Karte gespeichert sind, bleiben für die Zeit des Transports sicher, da der CryptoServer weiterhin über die Carrier-Batterie mit Spannung versorgt wird.

2.2 Batterie

Eine 3-V-Lithium-Carrier-Batterie sorgt dafür, dass die Sensorik und die Löschschaltung des CryptoServer Se Gen2 immer funktionsfähig sind, dies bedeutet, auch solange dieser nicht in einem Rechner eingebaut ist oder der Rechner, in dem er sich befindet, ausgeschaltet bleibt. Diese Batterie stellt die Spannungsversorgung der CryptoServer-PCIe-Karte für mindestens 6 Monate sicher und befindet sich bei der Lieferung bereits im Gebrauch.



Diese Batterie ist nicht wiederaufladbar.

Wenn der CryptoServer Se Gen2 nicht in einem eingeschalteten Rechner betrieben wird, sollte die Batterie in regelmäßigen Abständen gewechselt werden. Anderenfalls könnte ein Alarm ausgelöst und alle Daten im Gerät gelöscht werden.

2.3 Den CryptoServer sicher transportieren

Dieses Kapitel beschreibt die Schritte, die durchgeführt werden müssen, um eine CryptoServer-PCIe-Karte aus einem Rechner zu entfernen, sie an einen anderen Ort zu transportieren und dort in einen anderen Rechner einzubauen.

Vorraussetzungen

- Stellen Sie sicher, dass die Anforderungen im Kapitel 2.1, "Transport und Lagerung", erfüllt sind.
- Bereiten Sie den neuen Ort der CryptoServer-PCIe-Karte gemäß Kapitel 4.1, "Allgemeine Hinweise", vor.

Um den sicheren Transport der CryptoServer-PCIe-Karte über lange oder kurze Distanzen vom alten Ort zum neuen Ort zu gewährleisten, gehen Sie folgendermaßen vor:

1. Überprüfen Sie den Status der Carrier-Batterie mit dem Kommando `csadm GetBattState` oder mit dem CryptoServer Administration Tool (CAT).

Beispiel auf einem Windows-Betriebssystem:

```
csadm Dev=PCI:0 GetBattState
```

Beispiel auf einem Linux-Betriebssystem:

```
csadm Dev=/dev/cs2.0 GetBattState
```

Benutzung von CAT:

Klicken Sie auf **Show > Battery State**.

Überprüfen Sie die Ausgabe für die Carrier-Batterie.

Die Carrier-Batterie stellt sicher, dass die Sensoren und der Erase-Schaltkreis des CryptoServers immer betriebsbereit sind, wenn der CryptoServer in keinem Rechner eingebaut ist. Anderenfalls könnte ein Alarm ausgelöst und alle Daten auf dem Gerät gelöscht werden.

Wenn die Spannung der Carrier-Batterie als **ok** angezeigt wird, zum Beispiel,

Carrier Battery: ok (3.068 V),
fahren Sie mit Schritt 3 fort.

Wenn die Spannung der Carrier-Batterie als **low** angezeigt wird, zum Beispiel,

Carrier Battery: low (2.650 V),
fahren Sie mit Schritt 2 fort.

Die externe Batterie ist nur für den CryptoServer LAN relevant.

2. Ersetzen Sie die Carrier-Batterie durch eine neue Batterie (3 V, Lithium, FDK CR 12600 SE-T1 mit Lötflächen, oder gleichartige). In Kapitel 6, "Batterie wechseln"; dieses Dokuments finden Sie eine schrittweise Anleitung hierzu. Beachten Sie, dass diese Batterie die Stromversorgung des CryptoServer Se Gen2 für einen Zeitraum von mindestens 6 Monaten sicherstellt.

Wenn Sie die Carrier-Batterie ersetzt haben, fahren Sie mit Schritt 7 auf Seite 12 fort, Andernfalls fahren Sie mit dem nächsten Schritt fort.

3. Bestimmen Sie als Vorbereitung auf die unten beschriebene Sicherung von Datenbanken den Master-Backup-Key (MBK), der im MBK-Slot 3 benutzt wird. Führen Sie dazu entweder den Befehl `csadm MBKListKeys` gemäß Kapitel "MBKListKeys" in [CSADMIN] durch oder benutzen Sie CAT gemäß Kapitel "Retrieving MBK Information" in [CSMSADM].
4. Notieren Sie sich diesen MBK.



*Dieser MBK wird vom dem Befehl **csadm BackupDatabase** benutzt, um zu erstellende Sicherungsdateien zu schützen.*

*Es ist wichtig, zu notieren, welcher MBK benutzt worden ist, da für eine erfolgreiche Wiederherstellung dieser Sicherungsdatei zu einem späteren Zeitpunkt derselbe MBK im MBK-Slot 3 sein muss. Andernfalls, zum Beispiel nach der Durchführung eines Befehls **csadm MBKImportKey** oder nach einem MBK-Rollover, ist die Sicherungsdatei unzugänglich. Siehe Kapitel "Master Backup Key Rollover" in [CSMSADM] für Details.*

5. Überprüfen Sie, ob alle Shares dieses MBKs als Schlüsseldateien oder auf Smartcards verfügbar sind. Um MBK-Shares auf einer Smartcard zu überprüfen, führen Sie den Befehl `csadm MBKCardInfo` gemäß Kapitel "MBKCardInfo" in [CSADMIN] durch oder benutzen Sie CAT gemäß Kapitel "Retrieving MBK Information" in [CSMSADM].
6. Sichern Sie die folgenden Datenbanken.
 - Benutzerdatenbank (**user.db**)
 - Datenbank der kryptografischen Schlüssel (**CXIKEY.db**)
 - Auditlog-Signaturschlüssel (**auditkey.db**), sofern vorhanden

Um dies umzusetzen können Sie entweder den Befehl `csadm BackupDatabase` gemäß Kapitel "BackupDatabase" in [CSADMIN] durchführen oder CAT gemäß Kapitel "Backing up Databases" in [CSMSADM] benutzen,

Beispiel:

```
csadm LogonSign=ADMIN,:cs2:cjo:USB0 BackupDatabase=CXKEY.db BackupDatabase=user.db
BackupDatabase=auditkey.db
```

7. Bauen Sie die CryptoServer-PCIe-Karte aus dem Rechner aus. Befolgen Sie beim Ausbau unbedingt die im Betriebshandbuch Ihres Rechners angegebenen Anweisungen zum Ausbau von PCIe-Karten sowie die Anweisungen im Kapitel 4.3, "Den CryptoServer Se Gen2 ausbauen", dieses Dokuments.
8. Legen Sie die CryptoServer-PCIe-Karte in Antistatikfolie und in die Originalverpackung. Sollten Sie über keine Originalverpackung und Antistatikfolie verfügen, wenden Sie sich an den Hersteller Utimaco IS GmbH.
9. Noch einmal: Stellen Sie sicher, dass die Anforderungen im Kapitel 2.1, "Transport und Lagerung", erfüllt sind.
10. Am Zielort stellen Sie den Rechner, in dem die CryptoServer-PCIe-Karte eingebaut werden soll, an seine vorgesehene Position und bauen Sie anschließend die CryptoServer-PCIe-Karte ein. Befolgen Sie hierbei die im Betriebshandbuch des Rechners angegebenen Anweisungen zum Einbau von PCIe-Karten sowie die Anweisungen im Kapitel 4.2, "Den CryptoServer Se Gen2 einbauen", dieses Dokuments.

2.4 Umgebungstemperatur

Der CryptoServer Se Gen2 darf nur in einem begrenzten Temperaturbereich betrieben und gelagert werden.

- Stellen Sie sicher, dass die Umgebungstemperatur bei Lagerung des CryptoServer Se Gen2 stets zwischen -10 °C und +55 °C (+14 °F bis +131 °F) liegt.
- Stellen Sie sicher, dass die Umgebungstemperatur für den Betrieb des CryptoServer Gen2 PCIe stets zwischen +10 °C und +45 °C (+50 °F bis +113 °F) liegt.



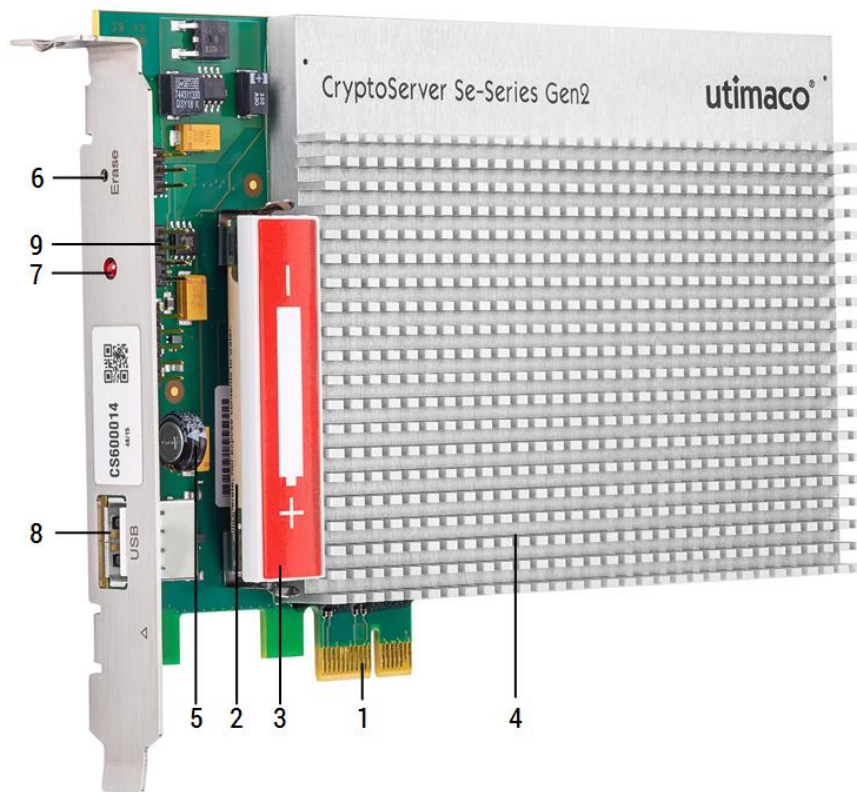
Der Betrieb außerhalb der erlaubten Umgebungstemperatur kann dazu führen, dass alle Daten im Gerät gelöscht werden.

Aus Sicherheitsgründen implementiert die CryptoServer Se Gen2-PCIe-Karte einen Mechanismus, der aktiv das Gerät davor schützt, unter Extremtemperaturen betrieben zu werden. Zu diesem Zweck implementiert die CryptoServer Se Gen2-PCIe-Karte einen Temperatursensor, der in der CryptoServer Se Gen2-PCIe-Karte angebracht ist und der permanent die Temperatur überwacht, um eine unmittelbare Aktion für den Fall anzustoßen, dass der erlaubte Bereich verlassen wird. Für den erlaubten Temperaturbereich des Temperatursensors, siehe das Kapitel „Temperature Monitoring in [CSMSADM]“. Dieses Kapitel beschreibt im Detail, bei welchen Temperaturen der CryptoServer Se Gen2 heruntergefahren wird oder sogar ein Alarm ausgelöst wird und alle sensitiven Daten gelöscht werden. Es besteht also das Risiko, dass der CryptoServer Se Gen2 heruntergefahren wird und alle sensitiven Daten gelöscht werden, weil eine zu niedrige oder zu hohe Umgebungstemperatur mittelbar die Innentemperatur aus dem erlaubten Bereich

bringt..

3 Komponenten des CryptoServer Se Gen2 (PCIe)

Der CryptoServer Se Gen2 besteht aus den folgenden Komponenten:



- 1 PCI Express Bus (PCIe x1) der PCIe-Einsteckkarte
- 2 Batterie:
Zur Spannungsversorgung der Sensorik und Löschschaltung bei ausgeschaltetem Rechner
- 3 Batterieschutzdeckel
- 4 Gekapselte Recheneinheit:
Der mechanische Schutz verhindert die Manipulation und das Auslesen der kryptographischen Daten
- 5 Kondensator:
Übernimmt die Spannungsversorgung während eines Batteriewechsels für ca. fünf Minuten
- 6 Erase-Taster
Taster zum Durchführen eines External-Erase
- 7 LED-Leuchte
Indikator (leuchtet rot auf) für das Aktivieren des Erase-Tasters
- 8 USB-Schnittstelle (extern):
USB 2.0-Anschluss für Peripheriegeräte wie z.B. PIN-Pad
- 9 USB-Schnittstelle (intern):
Steckerleiste für zusätzlichen USB 2.0-Anschluß

4 Auspacken und Handhabung

Ab Werk sind bereits mehrere kryptographische Schlüssel im CryptoServer Se Gen2 gespeichert, ohne die das Gerät nicht betrieben werden kann. Gehen Sie daher beim Auspacken und später beim Ein- und Ausbau vorsichtig mit dem Gerät um.

Der CryptoServer Se Gen2 ist außerdem ab Werk mit einer Batterie bestückt, die bei der Auslieferung bereits in Betrieb ist, d.h. einzelne Kontaktpunkte und Bauteile stehen dauerhaft unter Spannung.



Der CryptoServer Se Gen2 ist in einer speziellen Antistatikfolie verpackt. Bewahren Sie diese Antistatikfolie für eine spätere Lagerung oder Transport auf.

Die Lagerung des CryptoServer Se Gen2 darf nur in dieser Antistatikfolie erfolgen, da viele andere Antistatikfolien leitfähiger sind und es daher zu einem Kurzschluss der spannungsführenden Kontaktpunkte und Bauteile kommen kann.



Beachten Sie beim Ein- und Ausbau die gängigen Vorschriften für das Arbeiten an elektrischen Geräten sowie alle elektrostatischen Schutzmaßnahmen. Beachten Sie insbesondere die folgenden Hinweise.



Legen Sie die Trägerplatine niemals mit der Unterseite auf eine leitende Oberfläche (z. B. den Metalldeckel eines Computers), dies kann einen Kurzschluss verursachen.

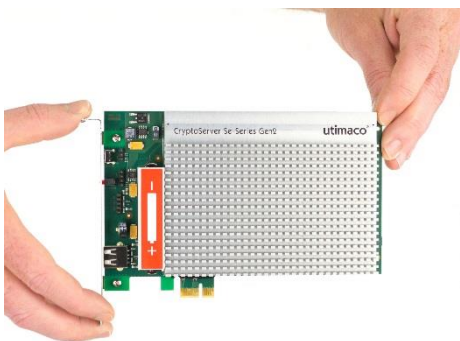
Achten Sie darauf, dass sie die Platine nicht mit einem metallischen Gegenstand (z. B. Schraubenzieher, Ehering) berühren.

Berühren Sie niemals die Kontakte auf der Rückseite der Trägerplatine.



Fassen Sie den CryptoServer Se Gen2 nur an dem Befestigungsblech und an den Kanten der Trägerplatine an (siehe linke Abbildung unten).

Üben Sie keinerlei Druck auf die gekapselte Einheit aus, und berühren Sie niemals die Kontakte auf der Rückseite der Trägerplatine (siehe rechte Abbildung unten).



Richtig



Falsch

4.1 Allgemeine Hinweise

Der CryptoServer Se Gen2 ist mit einer Sensorik ausgerüstet, die feststellt, ob er innerhalb einer zulässigen Temperaturspanne betrieben wird.



Die interne Temperatur des CryptoServer Se Gen2 darf während des Betriebs 62 °C nicht überschreiten, da sich das Gerät sonst abschaltet. Dies erfordert eine ausreichende Kühlung des CryptoServer Se Gen2.

Damit diese interne Temperatur nicht überschritten wird, sollte die Umgebungstemperatur nicht mehr als 45 °C (113 °F) betragen.

Beachten Sie daher unbedingt folgende Einbauhinweise:

- Wählen Sie einen ausreichend kühlen und gut belüfteten Aufstellungsort für den Rechner, in dem Sie den CryptoServer Se Gen2 betreiben möchten.
- Vermeiden Sie Wärmequellen wie Heizung oder direkte Sonneneinstrahlung.
- Achten Sie darauf, dass sich der Steckplatz des CryptoServer Se Gen2 im gekühlten Luftstrom des Rechners befindet.
- Positionieren Sie den CryptoServer Se Gen2 nur unterhalb von anderen stark Wärme abstrahlenden Einsteckkarten.
- Halten Sie jeweils einen Steckplatz frei zu anderen stark Wärme abstrahlenden Einsteckkarten, sowie zu weiteren CryptoServer Se Gen2.



Können diese Einbauhinweise nicht umgesetzt werden, wird dringend der Einsatz eines PCIe-Slot-Lüfters empfohlen, der direkt neben dem CryptoServer Se Gen2 montiert werden sollte.

4.2 Den CryptoServer Se Gen2 einbauen

Befolgen Sie beim Einbau unbedingt die im Betriebshandbuch Ihres Rechners angegebenen Anweisungen zum Einbau von PCIe-Einsteckkarten. Die folgenden Schritte beschreiben lediglich die allgemeine Vorgehensweise:

1. Schalten Sie den Rechner aus.
2. Entfernen Sie alle Kabel.
3. Öffnen Sie das Rechnergehäuse.
4. Wählen Sie einen freien PCIe-Steckplatz und entfernen Sie das zugehörige Slot-Blech an der Rückseite des Rechners.
5. Stecken Sie die CryptoServer Se Gen2-Einsteckkarte in den PCIe-Steckplatz des Rechners. Achten Sie darauf, dass die Karte richtig einrastet.
6. Verschließen Sie das Rechnergehäuse, schließen Sie alle Kabel wieder an und schalten Sie den Rechner ein.

4.3 Den CryptoServer Se Gen2 ausbauen

Ein Ausbau des CryptoServer Se Gen2 wird bei einem Batteriewechsel oder bei einem eventuellen Transport bzw. Lagerung notwendig.



Befolgen Sie beim Ausbau unbedingt die im Betriebshandbuch Ihres Rechners angegebenen Anweisungen zum Ausbau von PCIe-Einsteckkarten.

1. Schalten Sie den Rechner aus.
2. Entfernen Sie alle Kabel.
3. Öffnen Sie das Rechnergehäuse.
4. Entnehmen Sie den CryptoServer Se Gen2 vorsichtig aus dem PCIe-Steckplatz. Hebeln Sie die Karte auf keinen Fall mit einem Gegenstand (z. B. Schraubendreher) aus dem Steckplatz heraus.
5. Verschließen Sie das Rechnergehäuse.
6. Schließen Sie alle Kabel wieder an.



Beachten Sie, dass die Kühlkörper nach dem Ausschalten des Rechners über einen gewissen Zeitraum noch sehr heiß sein können. Lassen Sie die Kühlkörper zunächst abkühlen, bevor Sie den CryptoServer Se Gen2 ausbauen.

5 Installation der CryptoServer-Treiber-Software

Die aktuelle Liste der unterstützten Betriebssysteme entnehmen Sie bitte dem Dokument CS_PD_SecurityServer_SupportedPlatforms.pdf, das Sie auf der Produkt-CD im Verzeichnis ...\\Documentation\\Product Details finden.

Im Folgenden wird beschrieben, wie der Treiber des CryptoServer Se Gen2 auf dem Host-Rechner unter den verschiedenen Betriebssystemen installiert, getestet, aktualisiert und wieder entfernt wird.

5.1 Installation auf Windows-Betriebssystemen

Für die Installation bzw. die Aktualisierung des CryptoServer-Treibers benötigen Sie folgende Dateien:

- CryptoServer.sys (Treiberprogramm)
- CryptoServer.inf (Installationsskript)
- cryptoserver.cat (Katalogdatei)



*Sie finden diese Dateien auf der Produkt CD im folgenden Verzeichnis:
...\\Software\\Windows\\Driver\\bin.*

5.1.1 Treiber installieren auf Windows



Sie müssen über lokale Administratorrechte auf dem Host-Rechner verfügen, auf dem der Treiber für den CryptoServer Se Gen2 installiert werden soll.



Der Treiber unterstützt maximal 32 CryptoServer-PCIe-Karten.

Voraussetzungen

Um die GUI-Tools zu benutzen, muss Ihre Java-Installation unbegrenzte Crypto unterstützen. Wenn Ihr System keine JRE hat, laden Sie eine von <http://openjdk.java.net/Next> herunter, und installieren Sie die entsprechenden Dateien der Java-Sicherheitsrichtlinie, zum Beispiel

UnlimitedJCEPolicyJDK11.zip von der Website openjdk.java.net. Dekomprimieren Sie sie, und kopieren Sie die Dateien *.jar in Ihr Verzeichnis /lib/security.

Vorgehensweise

Um den CryptoServer-Treiber auf Ihrem Rechner mit einem Windows-Betriebssystem zu installieren, führen Sie die folgenden Schritte durch:

1. Klicken Sie im obersten Verzeichnis des Produkt-Bundles auf die Datei **SecurityServer-<version number>.msi**.



*Gegebenenfalls werden Sie aufgefordert, die Microsoft-Laufzeitumgebung (VCRedist) zu installieren. Klicken Sie auf **OK**, um den entsprechenden Dialog zu bestätigen.*

2. Klicken Sie im Installationsprogramm auf **Next**.
3. Klicken Sie im Dialog **Select Installation Folder** auf die Schaltfläche **Browse...**, um ein anderes Verzeichnis für die Installation der Software zu verwenden, oder bestätigen Sie das Standardinstallationsverzeichnis.

4. Klicken Sie auf **Next**.

Der Dialog **Choose Setup Type** wird geöffnet.

Typical

Die CryptoServer-Administrations-Tools (CAT, csadm etc.) und die CryptoServer-Dokumentation werden installiert.

Custom

Dieser Installationstyp lässt Sie die zu installierenden Leistungsmerkmale auswählen.


Complete

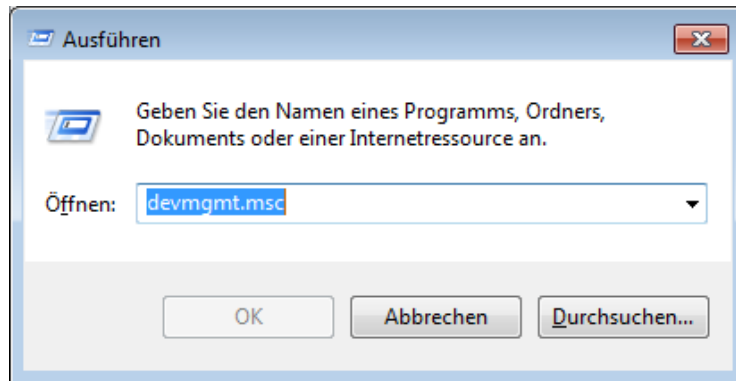
Dies entspricht der Auswahl aller Leistungsmerkmale einer **Custom**-Installation ohne **PCIe driver** und **PIN Pad driver**.

Wählen Sie **Custom** aus.

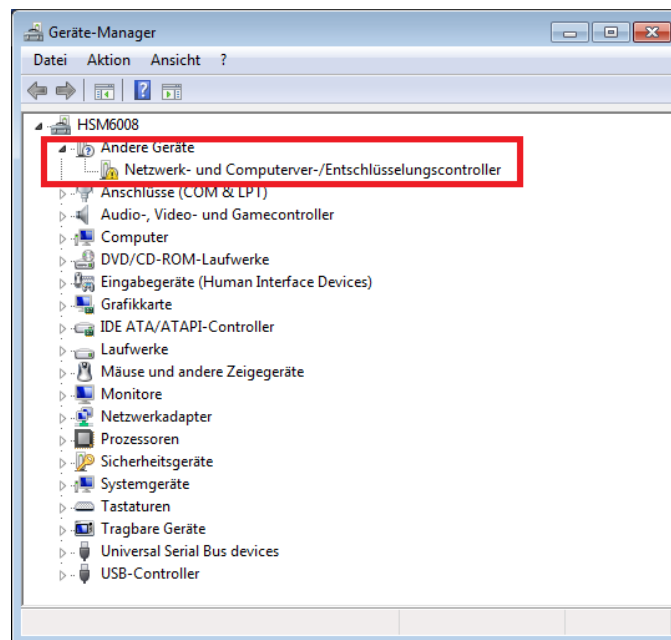
5. Der Dialog **Select the features to be installed** wird geöffnet. Standardmäßig sind **Administration** und **Documentation** ausgewählt.
6. Deselektieren Sie alle Leistungsmerkmale, die unverändert bleiben sollen (nicht installiert/aktualisiert werden sollen). Sie sind durch ein rotes X gekennzeichnet.
7. Klicken Sie auf das kleine schwarze Dreieck neben **Drivers > CryptoServer**, und selektieren Sie **Will be installed on local hard drive**.
8. Klicken Sie auf **Next**.
9. Klicken Sie im Dialog **Ready to Install** auf **Install**.
10. Klicken Sie auf **Finish**, um die Software-Installation abzuschließen.

11. Starten Sie den Windows-Geräte-Manager.

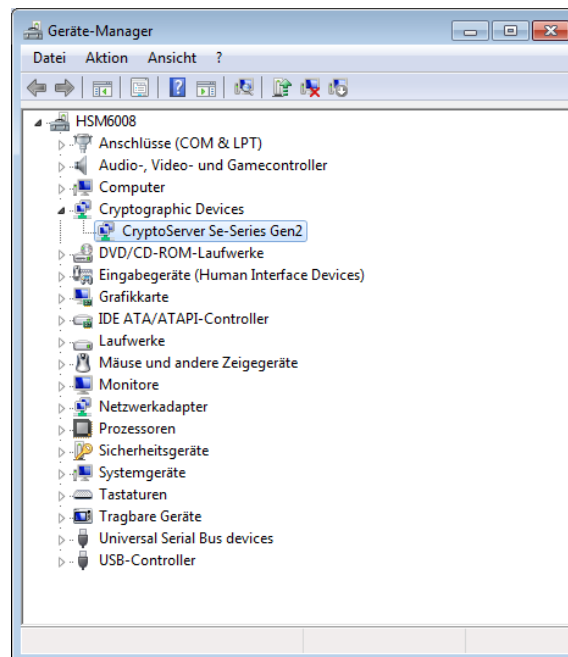
- a) Öffnen Sie den Dialog **Ausführen** durch Drücken und gedrückt halten der Windows-Taste  und gleichzeitiges Drücken der R-Taste.



- b) Geben Sie in das Textfeld `devmgmt.msc` ein und drücken Sie die ENTER-Taste. Der Windows-Geräte-Manager öffnet sich.



12. Der CryptoServer Se Gen2 wird jetzt im Windows-Geräte-Manager als Gerät **CryptoServer Se-Series Gen2** unter **Cryptographic Devices** angezeigt.



5.1.2 Funktionstest durchführen

Prüfen Sie die korrekte Installation des Treibers und die Funktionsfähigkeit des CryptoServer Se Gen2 und gehen Sie dabei wie folgt vor:

1. Wählen Sie über das Windows **Start**-Menü die Option **Run**
2. Geben Sie in dem sich öffnenden Fenster den Namen `cmd` ein.
3. Starten Sie das Kommandozeilenfenster mit **OK**.
4. Geben Sie folgende Befehlssequenz ein, um das Administrationsprogramm `csadm` von der Produkt-CD zu starten und hiermit den Status des CryptoServer Se Gen2 zu ermitteln. Es wird hierbei angenommen, dass das CD/DVD-Laufwerk den Laufwerksnamen `D` trägt und es sich um eine CryptoServer-PCIe-Karte im ersten Slot handelt.

```
D:
cd Software\Windows\Administration
set CRYPTOSERVER=PCI:0
csadm GetState
```

Bei erfolgreich installiertem Treiber und funktionsfähigem CryptoServer Se Gen2 erscheint folgende Ausgabe:

```
mode    = Operational Mode
state   = INITIALIZED (0x00100004)
temp    = 36.1 [C]
alarm   = OFF
bl_ver  = 5.00.5.5      (Model: Se-Series Gen2)
```

```
uid      = 6e000018 850bbe01          |      =*
adm1     = 53653530 20202020 43533434 34383739 | Se1500   CS6000024
adm2     = 53656375 72697479 53657276 65720000 | SecurityServer
adm3     = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

Sollte eine Kommunikation mit dem CryptoServer Se Gen2 nicht zustande kommen, prüfen Sie, ob die PCIe-Einsteckkarte korrekt eingebaut wurde und ob der Treiber im Windows Geräte-Manager korrekt installiert wurde. Danach wiederholen Sie den Funktionstest.

Sollte weiterhin keine Kommunikation mit dem CryptoServer Se Gen2 zustande kommen, wenden Sie sich bitte an den Händler, von dem Sie den CryptoServer Se Gen2 erworben haben, oder an den Kundendienst der Utimaco IS GmbH.

Wenn Sie mehrere CryptoServer-PCIe-Karten benutzen oder die Karte in einem anderen Slot ist, ersetzen Sie für jede weitere Karte in der obigen Befehlssequenz PCI:0 durch PCI:1 or PCI:2 etc. und führen Sie diese Befehlssequenz erneut aus.

5.1.3 Treiber deinstallieren



Deinstallieren Sie zuerst den Treiber von Ihrem Computer, bevor Sie den CryptoServer Se Gen2 aus dem Rechner ausbauen.

Eine Deinstallation des Treibers ist nach der Entnahme des CryptoServer Se Gen2 aus dem Rechner nicht mehr möglich.

Wenn Sie den Se Treiber deinstallieren wollen, gehen Sie wie folgt vor.

1. Öffnen Sie den Geräte-Manager über das Windows-**Start**-Menü > **Systemsteuerung** > **System** > **Geräte-Manager**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät **CryptoServer Se Gen2-Series** und wählen Sie die Option **Deinstallieren** aus.
3. Wählen Sie im nachfolgenden Fenster die Option, dass die Treibersoftware von Ihrem Rechner gelöscht werden soll und bestätigen Sie mit **OK**. Der Treiber des CryptoServer Se Gen2 wird nun deinstalliert und von Ihrem Rechner entfernt.

Nach Beenden des Assistenten wird auch das Gerät **CryptoServer Se Gen2-Series** aus der Anzeige im Geräte-Manager entfernt.

4. Fahren Sie das Windows-Betriebssystem herunter, bevor Sie die CryptoServer Se Gen2-Einsteckkarte entfernen.

5.1.4 Treiber aktualisieren

Wenn Sie den Treiber zu einem späteren Zeitpunkt aktualisieren wollen:

1. Öffnen Sie den Geräte-Manager über das Windows-**Start**-Menü > **Systemsteuerung** > **System** > **Geräte-Manager**.

2. Klicken Sie mit der rechten Maustaste auf das Gerät **CryptoServer Se Gen2-Serie** und wählen Sie die Kontextmenüoption **Treibersoftware aktualisieren...** aus.
3. Wählen Sie die Option **Auf dem Computer nach Treibersoftware suchen.** aus.
4. Klicken Sie auf **Durchsuchen.**

Die weiteren Schritte zur Auswahl und Installation des neuen Treibers entsprechen dem Ablauf wie bei der erstmaligen Installation des Treibers beschrieben in Kapitel 5.1.

5.2 Installation auf Linux-Betriebssystemen

Aufgrund der Architektur des Linux-Kernels ist es leider nicht möglich, einen installationsfertigen Treiber zu erstellen.

Der CryptoServer-Treiber für Linux wird deshalb im Quellcode ausgeliefert und muss auf dem Zielsystem kompiliert werden.

5.2.1 Treiber auf Linux installieren

5.2.1.1 Voraussetzungen

Für die Kompilierung des CryptoServer-Treibers müssen die folgenden Voraussetzungen erfüllt sein:

- Der Quellcode des CryptoServer-Treibers muss vorhanden sein.
Sie finden den Quellcode des Treibers auf der Produkt-CD im Verzeichnis **Software/Linux/Driver**.
Der Treiber unterstützt maximal 8 CryptoServer-PCIe-Karten. Diese Anzahl kann im Quellcode des Treibers geändert werden.
- Jede größere Linux-Distribution hat ein Package für Headers, das oft "kernel-devel" genannt wird. Manche Distributionen benutzen andere Namen, zum Beispiel "linux-headers-amd64" für ein 64-bit-Debian. Schlagen Sie dazu in der Dokumentation Ihrer Distribution nach. Stellen Sie sicher, dass dieses Package installiert ist.
- Stellen Sie sicher, dass gcc installiert ist.
- Stellen Sie sicher, dass make installiert ist.
- Um die Kompilierung/Installation des CryptoServer-Treibers auf einem Linux-Betriebssystem durchführen zu können, müssen Sie über root-Rechte verfügen.

5.2.1.2 Hardware überprüfen

Vor dem Start der Treiberinstallation muss die Hardware überprüft werden.

Überprüfen Sie, ob die Karte auf Ihrem Rechner detektiert wird, indem Sie den Befehl `lspci -d '*:c071'` ausführen und dann nach **168a:c071** suchen.

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

5.2.1.3 Betriebssystem/Treiber überprüfen

Überprüfen Sie, ob UEFI oder der Legacy-(BIOS)-Modus benutzt wird:

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

Wenn `/sys/firmware/efi` existiert, bedeutet dies, dass das System UEFI benutzt.

Überprüfen Sie, ob SecureBoot aktiviert ist:

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



Wenn die Ausgabe sowohl UEFI als auch SecureBoot zeigt, funktioniert der Treiber nur, wenn er auf Ubuntu 18 oder höher läuft. In allen anderen Fällen muss SecureBoot im BIOS deaktiviert werden.

5.2.1.4 Treiber auf Ubuntu/Debian bauen und installieren

Sie finden die Quellcodedateien des Treibers im Verzeichnis `Software/Linux/Driver` im Produkt-Bundle.

1. Führen Sie den folgenden Befehl – gegebenenfalls unter Anpassung der Versionsnummer – aus, um das Kernel-Modul zu bauen und zu installieren. Das Modul wird bei Kernel-Aktualisierungen (mittels DKMS) erneut gebaut:

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

2. Nach einem Neustart werden Sie im MOK-Utility sein. Wählen Sie **enroll key** aus, und geben Sie das vorher gewählte Passwort erneut ein.



In diesem Fall ist ein Neustart empfehlenswert, um sicherzustellen, dass der Treiber automatisch lädt.

5.2.1.5 Treiber auf CentOS/Fedora/openSUSE/SLES/RHEL bauen und installieren



Für SLES 12 nicht die folgenden Schritte sondern die weiter unten beschriebenen Schritte durchführen.

Sie finden die Quellcodedateien des Treibers im Verzeichnis `Software/Linux/Driver` im Produkt-Bundle.

Führen Sie die folgenden Befehle – gegebenenfalls unter Anpassung der Versionsnummer – aus, um das Kernel-Modul zu bauen und zu installieren. Das Modul wird bei Kernel-Aktualisierungen (mittels DKMS) erneut gebaut:

```
# 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
```

Führen Sie für SLES 12 stattdessen die folgenden Schritte durch:

1. Create a new temp directory.

```
mkdir temp
```

2. Verschieben Sie die Datei `cryptoserver-dkms-5.19.0-Linux.rpm` – gegebenenfalls unter Anpassung der Versionsnummer - in dieses Verzeichnis `temp`.

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

3. Gehen Sie in dieses Verzeichnis `temp`.

```
cd temp
```

4. Führen Sie – gegebenenfalls unter Anpassung der Versionsnummer – die folgenden Befehle durch.

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

5. Ändern Sie den Wert von `allow_unsupported_modules` auf 1 in der Datei `/etc/modprobe.d/10-unsupported-modules.conf`.
6. Erstellen Sie die Datei `/etc/modules-load.d/cryptoserver.conf` mit der Zeile `cryptoserver` als Inhalt.
7. Erstellen Sie die Datei `/etc/modprobe.d/70-cryptoserver.conf` mit der Zeile `options cryptoserver DeviceMask=0xFFFFFFFF` als Inhalt.
8. Gehen Sie in das Verzeichnis, in dem Sie oben das Verzeichnis `temp` erstellt haben.
9. Löschen Sie das oben erstellte Verzeichnis `temp`. Löschen Sie nicht das Verzeichnis `/tmp`.

```
rm -rf temp
```

10. Starten Sie den Rechner neu.

```
reboot
```

Auf CentOS/RHEL wird das Paket nur funktionieren, wenn das EPEL-Repository aktiviert worden ist. Eine Überprüfung kann mittels `yum repolist` erfolgen.



Die Paket-Installation wird nicht automatisch das Modul für SecureBoot signieren, also muss SecureBoot deaktiviert sein.

5.2.1.6 Treiber konfigurieren

Standardmäßig aktiviert der Treiber weder cHSM-Slots, noch die Netzwerkschnittstelle. Um das zu tun, erstellen Sie eine Konfigurationsdatei `modprobe`, um `DeviceMask` und `DeviceFlags` zu setzen, zum Beispiel `/etc/modprobe.d/cryptoserver.conf`.

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

Laden Sie den Treiber erneut, damit die Änderungen wirksam werden:

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

Die Ausführung des Befehls '`$ sudo rmmod cryptoserver`' kann scheitern, wenn der Treiber nicht geladen wurde.

5.2.2 Funktionstest durchführen

Um die korrekte Installation des Treibers und die Funktionsfähigkeit des CryptoServer Se Gen2 zu überprüfen, gehen Sie wie folgt vor:

1. Kopieren Sie das CryptoServer Administration Tool `csadm` von der Produkt-CD auf Ihre lokale Festplatte.

Beispiel :

```
cp <Pfad zur Produkt-CD>/Software/Linux/Administration/csadm .
```

2. Machen Sie die Datei `csadm` ausführbar.

```
chmod u+x csadm
```

3. Überprüfen Sie die Verbindung zum CryptoServer.

```
csadm Dev=/dev/cs2.0 GetState
```

Die 0 in `cs2.0` zeigt an, dass Sie versuchen, sich mit einer CryptoServer-PCIe-Karte im ersten gefundenen PCIe-Slot zu verbinden.

Bei erfolgreich installiertem Treiber und funktionsfähigem CryptoServer Se Gen2 erscheint eine Ausgabe, die dem folgenden Beispiel ähnelt:

```
mode    = Operational Mode
state   = INITIALIZED (0x0100004)
temp    = 36.1 [C]
alarm   = OFF
bl_ver  = 5.00.0.5      (Model: Se-Series Gen2)
```

```
uid      = 6e000018 850bbe01          |   =*
adm1     = 53653530 20202020 43533434 34383739 | Se1500   CS600024
adm2     = 53656375 72697479 53657276 65720000 | SecurityServer
adm3     = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

Stellen Sie sicher, dass die folgenden Zeilen gezeigt werden.

```
mode     = Operational Mode
alarm    = OFF
```

Sie zeigen an, dass der CryptoServer im Operational Mode ist und dass kein Alarm anliegt.

4. Wenn es Probleme gibt, eine Ausgabe ähnlich der obigen zu erzeugen, führen Sie die folgenden Unterschritte durch.

- a) Überprüfen Sie, ob das Kernel-Modul läuft.

```
lsmod | grep cryptoserver
```

Beispielausgabe:

```
Cryptoserver 90112 0
```

- b) Überprüfen Sie, ob der Geräteknoten erstellt worden ist.

```
ls /dev/cs2.0
```

Beispielausgabe:

```
crw-rw-rw- 1 root root 240, 0 Dez 19 16:17 /dev/cs2.0
```

- c) Überprüfen Sie auf Fehlermeldungen.

```
dmesg | grep :cs
```

- d) Sollte eine Kommunikation mit dem CryptoServer Se Gen2 nicht zustande kommen, prüfen Sie, ob die PCIe-Karte korrekt eingebaut und der Treiber korrekt installiert wurde. Danach wiederholen Sie den Funktionstest.

Sollte weiterhin keine Kommunikation mit dem CryptoServer Se Gen2 zustande kommen, wenden Sie sich an den Händler, von dem Sie den CryptoServer Se Gen2 erworben haben, oder an den Kundendienst der Utimaco IS GmbH. Details dazu finden Sie im Kapitel 9, "Kontaktadresse für Support-Anfragen".

- e) Wenn Sie mehrere CryptoServer-PCIe-Karten benutzen oder die Karte im zweiten, dritten etc. gefundenen PCIe-Slot ist, ersetzen Sie für jede weitere Karte in dem obigen Befehl `/dev/cs2.0` durch `/dev/cs2.1` oder `/dev/cs2.2` etc. und führen Sie diesen Befehl erneut aus.

5.2.3 Treiber aktualisieren

5.2.3.1 Treiber einer SecurityServer-Freigabe < 4.30 aktualisieren

Wenn Sie den Treiber aktualisieren wollen, gehen Sie wie folgt vor:

1. Entladen Sie das Kernel-Modul.

```
modprobe -r cs2
```

2. Bestimmen Sie Ihre Kernel-Version.

```
uname -r
```

3. Löschen Sie das Kernel-Modul `cs2.ko`.

```
rm /lib/modules/<Kernel-Version>/extra/cs2.ko
```

4. Löschen Sie die Geräte-Datei cs2a.

```
rm /dev/cs2a
```

5. Löschen Sie die udev-Regel, die automatisch den Geräteknoten erstellt. Dieser Befehl kann fehlschlagen, wenn Sie die udev-Regel nicht installiert haben.

```
rm /lib/udev/rules.d/10-cryptoserver.rules
```

6. Führen Sie die folgenden Unterschritte in Abhängigkeit von Ihrer Linux-Distribution durch.
SLES

Löschen Sie die Zeile cs2 in der Datei /etc/modules.

RHEL

Löschen Sie die Zeile modprobe cs2 in der Datei /etc/rc.modules.

7. Starten Sie den Rechner neu.
8. Führen Sie die Schritte im Kapitel 5.2.1, "Treiber auf Linux installieren", durch.
9. Führen Sie die Schritte im Kapitel 5.2.2, "Funktionstest durchführen", durch.

5.2.3.2 Treiber einer SecurityServer-Freigabe 4.30 aktualisieren

Um den CryptoServer-Treiber einer Freigabe 4.30 zu aktualisieren, führen Sie die folgenden Schritte durch.

1. Nur für SLES: Löschen Sie die Zeile cryptoserver in der Datei /etc/modules.
2. Nur für RHEL: Löschen Sie die Zeile modprobe cryptoserver in der Datei /etc/rc.modules.
3. Führen Sie die Schritte im Kapitel 5.2.1, "Treiber auf Linux installieren", durch.
4. Führen Sie die Schritte im Kapitel 5.2.2, "Funktionstest durchführen", durch.

5.2.3.3 Treiber einer SecurityServer-Freigabe ≥ 4.31 aktualisieren

Um den CryptoServer-Treiber einer SecurityServer-Freigabe ≥ 4.31 zu aktualisieren, führen Sie die Schritte im Kapitel 5.2.1, "Treiber auf Linux installieren", und im Kapitel 5.2.2, "Funktionstest durchführen", durch.

5.2.4 Treiber deinstallieren

Wenn Sie den Treiber entfernen wollen, führen Sie folgende Befehle als root-/Super-Benutzer aus:

1. Entladen Sie das Kernel Modul.

```
modprobe -r cryptoserver
```

2. Bestimmen Sie Ihre Kernel-Version.

```
uname -r
```

3. Löschen Sie das Kernel-Modul `cryptoserver.ko`.

```
rm /lib/modules/<Kernel-Version>/extra/cryptoserver.ko
```

4. Deaktivieren Sie das automatische Laden des Kernel-Moduls. Führen Sie dazu für Linux-Distributionen, die systemd benutzen (RHEL 8 und höher und SLES 12 und höher), den folgenden Befehl durch.

```
rm /etc/modules-load.d/cryptoserver.conf
```

Für andere Linux-Distributionen schlagen Sie in der jeweiligen Dokumentation nach.

5. Wenn es keine anderen externen Kernel-Module gibt, können Sie den Wert der Variablen `allow_unsupported_modules` in der Datei `/etc/modprobe.d/10-unsupported-modules.conf` auf den Wert 0 ändern.
6. Fahren Sie den Rechner herunter, bevor Sie die CryptoServer Se Gen2-PCIe-Karte entfernen.

6 Batterie wechseln

Eine Batterie (*Carrier Battery*) sorgt dafür, dass die Löschschaltung und die Sensorik immer funktionsfähig sind, auch wenn der CryptoServer Se Gen2 ausgeschaltet ist.

Wird der CryptoServer Se Gen2 in einem Rechner betrieben, erfolgt seine Stromversorgung über die PCIe-Schnittstelle. In diesem Fall wird die Batterie nicht beansprucht, eine bereits teilweise entladene Batterie wird hierdurch aber nicht wieder aufgeladen.

Wird der CryptoServer Se Gen2 nicht über die PCIe-Schnittstelle mit Strom versorgt, z. B. bei Lagerung oder ausgeschaltetem Rechner, übernimmt die *Carrier Battery* diese Aufgabe. Diese Batterie stellt die Stromversorgung des CryptoServer Se Gen2 für einen Zeitraum von mindestens 6 Monaten sicher.



Diese Batterie ist nicht wiederaufladbar.

Die Batterie muss abhängig von der Betriebszeit des CryptoServer Se Gen2, in bestimmten Abständen ausgetauscht werden. Wird die Batterie nicht rechtzeitig ausgetauscht, wird ein Alarm im CryptoServer ausgelöst und die Daten im CryptoServer Se Gen2 werden gelöscht.

Der Zustand der Batterie sollte daher regelmäßig überprüft werden. Führen Sie hierzu das Kommando `GetBattState` des Administrationsprogramms `csadm` aus.

```
csadm Dev=PCI:0 GetBattState
```

Ausgabe-Beispiel:

Carrier Battery: low (2.540 V)

External Battery: absence

Wenn für die Carrier-Batterie der Status **LOW** ausgegeben wird, müssen Sie diese so bald wie möglich wechseln. Die externe Batterie ist nur für den CryptoServer LAN relevant.



Lesen Sie vor dem Wechsel der Batterie die Beschreibung der folgenden Arbeitsschritte sorgfältig durch.

1. Stellen Sie sicher, dass Sie vor dem Wechsel der Batterie die entsprechende Ersatzbatterie zur Hand haben. Wir empfehlen, nur die FDK CR 12600 SE-T1 mit Lötflähen oder gleichartige zu verwenden.



Bei der Verwendung falscher Batterien besteht Explosionsgefahr. Für Schäden, die durch den Einsatz von Batterien entstehen, die nicht von der Utimaco IS GmbH empfohlen worden sind, wird keine Gewährleistung übernommen.

Achten Sie bitte auf eine fach- und umweltgerechte Entsorgung Ihrer Altbatterien.

2. Stellen Sie sicher, dass die Batteriekontakte sauber und fettfrei sind.



*Reinigen Sie die Kontakte und die Lötflächen der Batterie mit Alkohol.
Vermeiden Sie im Folgenden, die Kontakte mit den Fingern zu berühren.*

3. Bestimmen Sie als Vorbereitung auf die unten beschriebene Sicherung von Datenbanken den Master-Backup-Key (MBK), der im MBK-Slot 3 benutzt wird. Führen Sie dazu entweder den Befehl `csadm MBKListKeys` gemäß Kapitel "MBKListKeys" in [CSADMIN] durch oder benutzen Sie CAT gemäß Kapitel "Retrieving MBK Information" in [CSMSADM].
4. Notieren Sie sich diesen MBK.



*Dieser MBK wird vom dem Befehl `csadm BackupDatabase` benutzt, um zu erstellende Sicherungsdateien zu schützen.
Es ist wichtig, zu notieren, welcher MBK benutzt worden ist, da für eine erfolgreiche Wiederherstellung dieser Sicherungsdatei zu einem späteren Zeitpunkt derselbe MBK im MBK-Slot 3 sein muss. Andernfalls, zum Beispiel nach der Durchführung eines Befehls `csadm MBKImportKey` oder nach einem MBK-Rollover, ist die Sicherungsdatei unzugänglich.
Siehe Kapitel "Master Backup Key Rollover" in [CSMSADM] für Details.*

5. Überprüfen Sie, ob alle Shares dieses MBKs als Schlüsseldateien oder auf Smartcards verfügbar sind. Um MBK-Shares auf einer Smartcard zu überprüfen, führen Sie den Befehl `csadm MBKCardInfo` gemäß Kapitel "MBKCardInfo" in [CSADMIN] durch oder benutzen Sie CAT gemäß Kapitel "Retrieving MBK Information" in [CSMSADM],

6. Sichern Sie die folgenden Datenbanken.

Benutzerdatenbank (`user.db`)

Datenbank der kryptografischen Schlüssel (`CXIKEY.db`)

HSM-Authentisierungsschlüssel (`authkey.db`), sofern vorhanden

Auditlog-Signaturschlüssel (`auditkey.db`), sofern vorhanden

Um dies umzusetzen können Sie entweder den Befehl `csadm BackupDatabase` gemäß Kapitel "BackupDatabase" in [CSADMIN] durchführen oder CAT gemäß Kapitel "Backing up Databases" in [CSMSADM] benutzen,

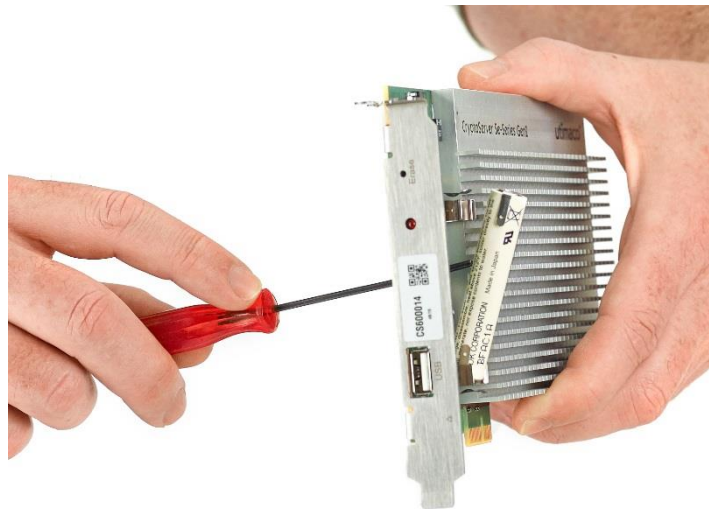
Beispiel:

```
csadm LogonSign=ADMIN,:cs2:cjo:USB0 BackupDatabase=CXIKEY.db BackupDatabase=user.db  
BackupDatabase=authkey.db BackupDatabase=auditkey.db
```

7. Schalten Sie den Rechner aus.
8. Bauen Sie den CryptoServer Se Gen2 aus dem Rechner aus.
9. Beachten Sie, dass Sie maximal 5 Minuten für den eigentlichen Batteriewechsel in den nächsten beiden Schritten zur Verfügung haben. Ein Kondensator stellt für diesen Zeitraum

sicher, dass die PCIe-Karte mit Strom versorgt ist und die Daten auf der Karte nicht gelöscht werden. Nach maximal 30 Minuten ohne Batterie werden die Daten auf der PCIe-Karte in jedem Fall gelöscht.

10. Auf der Rückseite der Batterieklemmen befindet sich ein Loch in der Platine. Stecken Sie einen dünnen Stift (oder Schraubendreher) durch das Loch, um so die Batterie aus den Klammern zu entfernen (siehe die Abbildung unten).

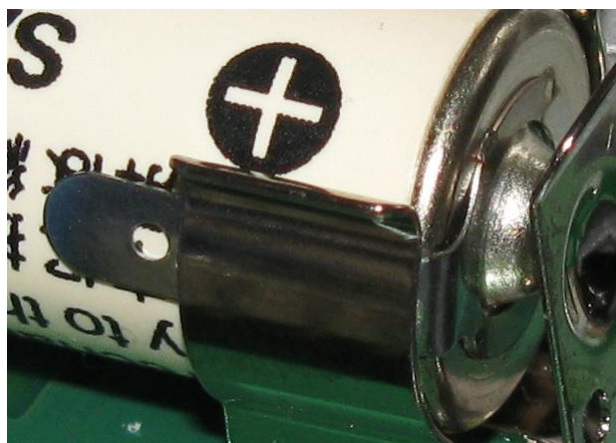


11. Wechseln Sie die Batterie aus.



Achten Sie dabei auf die richtige Polarität (siehe Aufkleber auf dem CryptoServer Se Gen2). Bei falscher Polung werden die Daten im Gerät gelöscht.

Wenn Sie die Batterie zum Wechseln entfernen, achten Sie besonders auf die Polarität und vergleichen Sie die Einlagerichtung mit der Richtung auf dem Aufkleber auf der Batterieabdeckung. Nachdem sie die Austauschbatterie eingelegt haben, stellen Sie sicher, dass Sie die Abdeckung mit der korrekten Ausrichtung des Polaritätsaufkleber wieder aufsetzen. Achten Sie bitte unbedingt darauf, dass die Lötflansen, die an der Batterie angebracht sind, Kontakt zu den Seitenhalterungen für die Batterie haben (siehe die Abbildung unten).



Für den Wechsel der Batterie stehen Ihnen maximal 5 Minuten zur Verfügung. Während dieser Zeit übernimmt ein Kondensator die Stromversorgung des CryptoServer Se Gen2. Wenn Sie innerhalb von maximal 30 Minuten nicht die neue Batterie eingesetzt haben, wird ein Alarm ausgelöst und alle sensitiven Daten im CryptoServer Se Gen2 werden gelöscht.

12. Bauen Sie den CryptoServer Se Gen2 wieder ein.
13. Notieren Sie sich das Datum für den nächsten Batteriewechsel.
14. Schalten Sie den Rechner wieder ein.
15. Überprüfen Sie den Status des CryptoServer Se Gen2. Sie können hierfür das CryptoServer-Administrationstool Ihrer Wahl verwenden – csadm oder CAT.

Beispiel mit dem csadm-Kommando **GetState**:

```
csadm PCI:0 GetState
```

Sollten Sie länger als fünf Minuten für den Batteriewechsel gebraucht haben, zeigt die Ausgabe des **GetState**-Kommandos an,

dass ein Alarm ausgelöst wurde

```
alarm = ON
```

sowie den Grund für den Alarm:

```
sens    = 02bf
- Alarm has occurred
- Power failed
```

Dies bedeutet, dass die Sensorik längere Zeit ohne Stromversorgung geblieben ist.

GetState Ausgabe-Beispiel:

```
mode    = Maintenance Mode
state   = INITIALIZED (0x020aff84)
temp    = 36.1 [C]
alarm   = ON
sens    = 02ff
```

- Alarm has occurred
- Power failed

```
bl_ver  = 5.00.0.5      (Model: Se-Series Gen2)
uid     = 6e000018 850bbe01 |   =*
adm1    = 53653530 20202020 43533434 34383739 | Se1500  CS600024
adm2    = 53656375 72697479 53657276 65720000 | SecurityServer
adm3    = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

16. Setzen Sie den Alarm zurück. Sie können hierfür das CryptoServer-Administrationstool Ihrer Wahl verwenden – csadm oder CAT.

Beispiel mit dem csadm-Kommando **ResetAlarm**:

```
csadm Dev=PCI:0 LogonSign=ADMIN,;cs2:cjo:USB0 ResetAlarm
```

17. Stellen Sie die Uhrzeit und das Datum des CryptoServer Se Gen2 ein. Sie können hierfür das CryptoServer-Administrationstool Ihrer Wahl verwenden – csadm oder CAT.

Beispiel mit dem csadm-Kommando **SetTime**:

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

Ihr CryptoServer Se Gen2 ist nun wieder einsatzbereit.

7 Entsorgung des CryptoServer Se Gen2

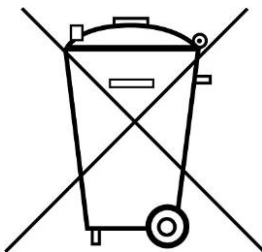
Führen Sie die folgenden Schritte durch, um einen CryptoServer Se Gen2 zu entsorgen.

1. Führen Sie ein External Erase durch, um alle sensiblen Daten im CryptoServer sicher zu löschen. Details dazu entnehmen Sie dem Handbuch CryptoServer – Administration Manual.

Sie haben selbstverständlich die Möglichkeit, den nicht mehr benötigten CryptoServer Se Gen2 an uns, den Hersteller Utimaco IS GmbH, zurückzusenden. In diesem Fall kümmern wir uns um die umweltgerechte Entsorgung des CryptoServer Se Gen2 und der Batterie.

Wenn Sie den CryptoServer Se Gen2 selber entsorgen wollen, beachten Sie, dass auf dem Carrier des CryptoServer Se Gen2 sich eine Batterie befindet, die umweltgerecht entsorgt werden muss.

2. Entnehmen Sie die Batterie des CryptoServer Se Gen2 und beachten Sie die folgenden allgemeinen Hinweise für Akkus und Batterien (Hinweispflicht gem. §18 BattG):



Akkus und Altbatterien dürfen nicht in den Hausmüll.

Verbraucher sind verpflichtet, Batterien zu einer geeigneten Sammelstelle bei Handel oder Kommune zu bringen.

Akkus und Altbatterien enthalten möglicherweise Schadstoffe oder Schwermetalle, die Umwelt und Gesundheit schaden können.

Batterien werden wieder verwendet, sie enthalten wichtige Rohstoffe wie Eisen, Zink, Mangan oder Nickel.

Unabhängig davon, ob Sie eine External Erase durchgeführt haben oder nicht, gilt Folgendes: Wenn Sie die CryptoServer-PCIe-Einsteckkarte aus dem Rechner entfernen und jegliche Batterie aus dieser Einsteckkarte entfernen, werden die sensiblen Daten auf dieser Einsteckkarte in jedem Fall nach 30 Minuten automatisch gelöscht.

Sie können die Batterie des CryptoServer Se Gen2 entweder bei einer geeigneten Sammelstelle bei Handel oder Kommune abgeben, oder an uns, den Hersteller Utimaco IS GmbH, zurücksenden.

8 Technische Daten

Abmessungen	PCI Express (PCIe)-Einsteckkarte: Länge: 167,65 mm („halbe“ Länge) Höhe: 111,15 mm („volle“ Höhe)
Gewicht	400 g
Batterie	3 V, Lithium, Ø 12 mm, L = 600 mm, FDK CR 12600 SE-T1 mit Lötflähen, oder gleichartige
Schnittstellen	PCIe x1 2 USB 2.0
Umgebungstemperatur	Betrieb: +10 °C bis +45 °C (+50 °F to +113 °F) Lagerung: -10 °C bis +55 °C (+14 °F to +131 °F)
Luftfeuchtigkeit	10 % bis 95 % relative Luftfeuchtigkeit, nicht kondensierend
MTBF	360.000 Stunden (nach MIL-HDBK-217)
RoHS Konformität	Ja
WEEE	Elektro-Altgeräte-Register DE65203472
Konformität	Störaussendung nach EN 55022 Klasse B Störbeeinflussung nach EN 61000-6-2 (Industriebereich) Gerätesicherheit nach EN/IEC 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 FCC 47 CFR Ch. 1 Part 15 Class B

9 Kontaktadresse für Support-Anfragen

Wenn während des Betriebs des CryptoServer LAN ein Fehler auftritt, lesen Sie [CSTrSh], um ihn zu beheben.

Wenn der Fehler danach immer noch vorliegt, bereiten Sie Diagnoseinformationen in einer .txt-Datei auf Ihrem Rechner wie in [CSTrSh] beschrieben vor.

Wenn Sie weitergehende Fragen zu dem CryptoServer LAN haben, setzen Sie sich bitte mit uns in Verbindung.

Sie erreichen uns von Montag bis Freitag von 09.00 Uhr bis 17.00 Uhr außer an deutschen Feiertagen und Brauchtumstagen.

Utimaco IS GmbH

Germanusstr. 4

52080 Aachen

Germany

■ RMA-Anforderung (Return Merchandise Authorization)

Wenn Sie einen CryptoServer an Utimaco IS GmbH zurücksenden möchten, d. h. Sie öffnen einen neuen RMA-Fall, wird gefordert, dass Sie die folgende Webadresse verwenden. RMA-Fälle können nicht per E-Mail oder Telefon geöffnet werden.

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

■ Für andere Support-Anfragen verwenden Sie die folgenden Kontaktdaten:

Per E-Mail (bevorzugte Kontaktmöglichkeit)

support@utimaco.com

Hängen Sie die Diagnoseinformationen an Ihre E-Mail.

Per Webportal

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

Die Diagnoseinformationen werden gegebenenfalls in unserer Antwort angefordert werden.

Per Telefon

☐ AMERICAS: +1-844-UTIMACO (+1 844-884-6226)

☐ EMEA: +49 800-627-3081

☐ APAC: +81 800-919-1301

Die Diagnoseinformationen werden gegebenenfalls in unserer Antwort angefordert werden.

Referenzliste

<i>Reference</i>	<i>Title/Company</i>	<i>Document No.</i>
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH.	2009-0003
[CSMSADM]	CryptoServer – Administration Manual/Utimaco IS GmbH.	M010-0001-en
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH.	M011-0008-en