

CryptoServer

CAT Manual

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	https://support.hsm.utimaco.com/ support@utimaco.com
Document Version	1.1.15
Product Version	6.0.0
Date	2024-10-23
Document No.	2021-0055
Status	PUBLISHED

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

1	Introduction	6
2	Installation	7
3	Overview of the Graphical User Interface	9
4	Setting Up the CryptoServer	12
4.1	Setting up a New Device.....	12
4.2	Switching between Devices.....	14
4.3	Setting up Microsoft CryptoAPI and Cryptography API: Next Generation (CNG).....	14
4.4	Setting up a PIN Pad	14
4.5	Setting up JCE.....	16
4.5.1	Setting up a User for JCE	16
4.5.2	Modifying the Device Address and User Name in the File CryptoServer.cfg	17
4.6	Setting up CXI.....	20
4.7	Setting up Extensible Key Management (EKM)	21
4.7.1	Setting up an EKM User.....	22
4.7.2	Modifying the Device Address in the File cssqlekm.cfg	23
4.7.3	Creating a Credential on the SQL Server	26
5	Administering the CryptoServer with CAT	27
5.1	Basic Administration	27
5.1.1	Logging in a User.....	27
5.1.2	Setting the Time	28
5.1.3	Changing the User Authentication Key of ADMIN.....	30
5.1.4	Changing the PIN for Smartcards.....	32
5.2	Managing Users.....	32
5.2.1	User Profiles	32
5.2.2	Creating a User	34
5.2.3	Adding PKCS#11 Security Officers with RSA Signature Authentication with a Smartcard .	38
5.2.4	Deleting a User	41
5.2.5	Creating a User Data Backup.....	41
5.2.6	Restoring User Data	43
5.2.7	Changing a User Authentication Token	47
5.2.8	Changing Another User's Authentication Token	48
5.3	Managing Smartcards and Keys.....	49
5.3.1	Generating a User Authentication Key with Backup Shares on Smartcards.....	49

5.3.2	Restoring a User Authentication Key from a Backup on Smartcards	50
5.3.3	Copying User Authentication Key Backup Shares from One Smartcard to Another Smartcard.....	52
5.3.4	Generating a User Authentication Key on a Smartcard without any Backup.....	53
5.3.5	Changing the PIN for User Authentication Keys on a Smartcard	55
5.3.6	Showing the Contents of a Smartcard.....	56
5.3.7	Generating a User Authentication Key as a Keyfile	57
5.3.8	Changing the Password for a Keyfile.....	58
5.3.9	Copying a Keyfile to a Smartcard (Backup)	59
5.4	Managing Databases	60
5.4.1	Backing up Databases	60
5.4.2	Restoring Databases	62
5.4.3	Cloning Databases.....	64
5.5	Managing Logs	67
5.5.1	Viewing the Boot Log.....	67
5.5.2	Deleting Displayed Log Entries	68
5.5.3	Saving Displayed Log Entries	68
5.5.4	Retrieving and Saving the Audit Log	69
5.5.5	Configuring the Audit Log Files	70
5.5.6	Deleting an Audit Log	73
5.6	Managing Master Backup Keys	74
5.6.1	Generating an MBK.....	75
5.6.2	Importing an MBK.....	79
5.6.3	Creating an MBK Backup.....	82
5.6.4	Changing the PIN for MBK Key Shares on Smartcards.....	85
5.6.5	Retrieving MBK Information	86
6	Monitoring the CryptoServer	87
6.1	Viewing the Status of the CryptoServer.....	87
6.2	Viewing the Battery State of the CryptoServer	91
6.3	Viewing Driver Information.....	91
6.4	Listing the Firmware.....	92
6.5	Listing All Files	95
7	Maintaining the CryptoServer	96
7.1	Installing/Updating the Firmware.....	96

7.2	Resetting an Alarm	98
7.3	Clearing the CryptoServer.....	98
7.3.1	Performing a Clear.....	100
7.3.2	Performing a Clear to Factory Settings	101
7.3.3	Performing an External Erase.....	102
7.4	Setting up the CryptoServer after a Clear/Clear to Factory Settings.....	102
7.5	Preparing Diagnostic Information	103
8	Contact Address for Support Queries	105
9	References	106

1 Introduction

Thank you for purchasing our CryptoServer security system. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any questions or comments.

This document provides information about the *CryptoServer Administration Tool (CAT)*. It is a Java application used to administer CryptoServer PCIe cards as well as CryptoServer LANs. CAT handles all typical administration tasks involved in bringing the CryptoServer into operation, monitoring its status and managing the users, firmware and keys.

The CAT also has a range of other useful functions that can be implemented for keyfiles and smartcards without involving the CryptoServer.

All operating systems that are currently supported for the CAT host computer are listed in the document [CS_PD_SecurityServer_SupportedPlatforms.pdf](#) provided on the SecurityServer/CryptoServer SDK product CD in the directory `...\Documentation\Product Details`.

The CAT runs in the Java runtime environments (JRE) 11 and 14/15.

2 Installation

This section describes how to install CAT using the `cat.jar` file contained in the product bundle. However, on Windows, CAT is usually installed along with the other CryptoServer host software when the CryptoServer is set up by using the `SecurityServer-<version number>.msi` (for CryptoServer 4.40.0 and later) or `CryptoServerSetup-<version number>.exe` (for CryptoServer versions earlier than 4.40.0) files, see *Installing the Host Software and CryptoServer Simulator* in the [CryptoServer - Administration Manual \(p. 106\)](#). For the Windows 64-bit operating system, `SecurityServer-<version number>.msi` can also be used to perform an installation without user interaction for specified components, see *Installing the Host Software and CryptoServer Simulator Without User Interaction* in the [CryptoServer - Administration Manual \(p. 106\)](#).

Prerequisites

- The CAT can be installed on Linux and Windows 64-bit systems. You will find the list of all currently supported operating systems in the document `CS_PD_SecurityServer_Supported_Platforms.pdf` in the SecurityServer product bundle in the directory `...\Documentation\Product Details`.
- On a 64-bit computer, only a 64-bit Java SE Runtime Environment is supported by the CryptoServer.
- If you use a 64-bit computer, perform the following command in a command-line to verify whether a 64-bit version of the Java SE Runtime environment has been installed on your computer:

```
java -d64 -version
```

Output example:

```
java version "1.7.0_51"
```

```
Java(TM) SE Runtime Environment (build 1.7.0_51-b13)
```

```
Java HotSpot(TM) 64-Bit Server VM (build 24.51-b03, mixed mode)
```

- To be able to use the CAT, install first the appropriate Sun Java Runtime Environment for the Java version available on your computer. Perform the following command in a command-line to retrieve the installed Java version:

```
java -version
```

Use the package manager for your Unix/Linux system to install the Oracle Java Runtime Environment.

Procedure

On an administration computer running a Windows operating system, CAT is installed by default during the installation of the CryptoServer software provided in the SecurityServer bundle.

The following steps describe how to install CAT on a Windows host computer without using the CryptoServer installer file, `SecurityServer-<version number>.msi` or `CryptoServerSetup-<version>.exe`, provided on the SecurityServer bundle.

You will find the CAT installation file for Windows, `cat.jar`, on the SecurityServer bundle here:

- For Windows 64-bit operating systems
`Software\Windows\Administration\`
- For Linux 64-bit operating systems
`Software/Linux/Administration/`

1. Copy the `cat.jar` file into the following directory.

On Windows: `cp <path to the Product CD>/Software/Linux/Administration/cat.jar ~/`

On Linux: Copy the `<path to the Product CD>\Software\Windows\Administration\cat.jar` file into the target directory.

2. Start CAT with the following command:

On Windows, for example: `C:\Program Files\Utimaco\SecurityServer\Administration\cat.jar`

On Linux: `java -jar ~/cat.jar`



CAT has been installed successfully.



CAT starts by default automatically once the CryptoServer host software has been installed correctly.

3 Overview of the Graphical User Interface

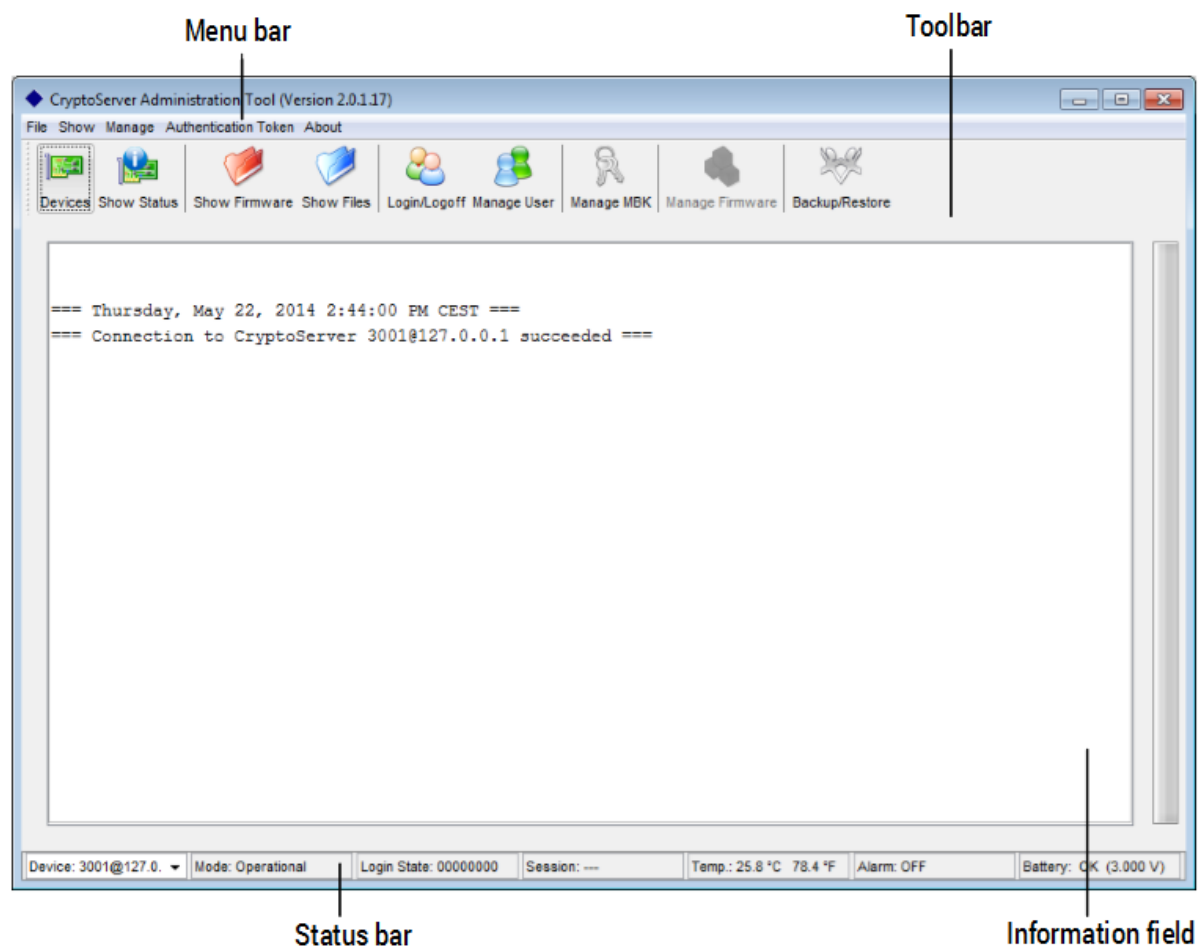


Figure 1 : CAT Main Window

The CAT main window is the main operating control of CAT. It contains the following elements:

- **Menu bar**

The menu bar is located directly under the title bar in the upper border of the CAT main window. It provides access all functions for CryptoServer administration.

- **Toolbar**

The toolbar is located under the menu bar. It provides quick access to the most often used administration functions of CAT, like setting up a new device, getting the current CryptoServer status, user management, logging on/logging off from CryptoServer, the management of Master Backup Keys and firmware.

- **Information field**

The information field comprises the middle area of the CAT main window under the toolbar. Here various status and firmware information is shown which can be retrieved by clicking the **Show** menu, as well as by clicking the **Show Status**, **Show Files** and **Show Firmware** buttons in the toolbar.

- **Status bar**

The status bar is located on the bottom border of the CAT main window. Here the device to be administered can be selected by using the combo box **Device** at the lower left window border.

Furthermore, the most important status information about the administered CryptoServer is shown:

- **Mode**

Operating Mode of the CryptoServer. If the CryptoServer is running correctly and is ready for use, *Operational* is displayed.

- **Login State**

Current authentication status. If the default administrator, ADMIN with authentication status 22000000, is logged into the CryptoServer, this authentication status is displayed here. If another administrator with authentication status 20000000 has logged on at the same time, the total authentication status 42000000 is displayed here.

- **Session**

Current remaining time until the existing Secure Messaging session is terminated. A Secure Messaging connection to the CryptoServer is established every time an administrator logs in to the CryptoServer. This connection is set to a maximum duration of 14 minutes and 59 seconds. The remaining length of time for the Secure Messaging connection is displayed here. The duration of the Secure Messaging connection resets to 14 minutes and 59 seconds every time an administrator sends a command to the CryptoServer, or when another administrator logs in to the CryptoServer. No matter how many administrators log in simultaneously to the CryptoServer, only one Secure Messaging connection is ever set up to the CryptoServer. As a consequence, when a Logoff All is performed, all administrators who are currently logged on are logged off simultaneously. This is because the Secure Messaging connection, which is being used by these multiple administrators, is terminated.

- **Temp**

Current temperature of the CryptoServer in °C and in °F

- **Alarm**

Alarm state. This shows whether an alarm is present. *OFF* indicates no alarm has been triggered, *ON* indicates an alarm has occurred.

- **Battery**

Status of the CryptoServer Carrier Battery. The status and the power of the carrier battery (in V) are displayed here. The status can be either *OK* or *LOW*. If *LOW* is displayed, this means the carrier battery is in a critical state. If the CryptoServer is running on a computer, it is supplied with power via the PCI or PCIe interface. If the CryptoServer is running as a standalone device, it is powered by the carrier battery. If the status drops to *LOW* it may happen that the supply of power can no longer be guaranteed. This may trigger an alarm, which then deletes all data from the CryptoServer.

4 Setting Up the CryptoServer

4.1 Setting up a New Device

Using CAT you can administer several CryptoServers simultaneously which you have set up previously in CAT.

Procedure

1. Start CAT.



When first installing the CryptoServer provided on the SecurityServer product CD, CAT starts automatically and the dialog box **CryptoServer Devices** opens. In this case, proceed with step 3.



If CAT starts with the `invalid auth. key` error message, either delete the `CS_AUTH_KEYS` environment variable or update it by performing the `csadm GetHSMAuthKey` command, see `GetHSMAuthKey` in the [CryptoServer – csadm Manual \(p. 106\)](#) for details.

2. Click **Devices** in the toolbar.
→ The dialog box **CryptoServer Devices** opens.
3. Enter the address of the device you want to use in the New Device text box.
Possible address entries:

Device address	Description
<code>/dev/cs2.n</code> where $n = \{0, 1, 2, \dots, 7\}$	Local CryptoServer No. $n+1$ on a UNIX system. The maximum number of eight CryptoServer PCIe cards can be changed in the source of the Linux driver.
<code>PCI:n</code> where $n = \{0, 1, 2, \dots, 31\}$	Local CryptoServer No. $n+1$ on a Windows system

<i>Device address</i>	<i>Description</i>
TCP:288@194.168.4.107	IP address and port number of a CryptoServer LAN In csadm commands, always use IP addresses without leading zeros although they are shown on the CryptoServer LAN display, e.g., 194.168.004.107.
TCP:194.168.4.107	IP address of a CryptoServer LAN (default: port=288) In csadm commands, always use IP addresses without leading zeros although they are shown on the CryptoServer LAN display, e.g., 194.168.004.107.
194.168.4.107	IP address of a CryptoServer LAN (default: protocol=TCP, port=288) In csadm commands, always use IP addresses without leading zeros although they are shown on the CryptoServer LAN display, e.g., 194.168.004.107.
TCP:288@cslan01	Host name and port number of a CryptoServer LAN (using DNS request to resolve host name)
TCP:cslan01	Host name of a CryptoServer LAN (using DNS request to resolve host name, default: port=288)
cslan01	Host name of a CryptoServer LAN (using DNS request to resolve host name, default: protocol=TCP, port=288)
TCP:3001@127.0.0.1 or TCP:3001@localhost	Local CryptoServer Simulator for Windows/Linux (SDK)
3001@127.0.0.1 or 3001@localhost	Local CryptoServer Simulator for Windows/Linux (SDK) with the default protocol TCP

Table 1: Device Addresses



If a CryptoServer LAN is used, the CryptoServer LAN's IP address and the IP address of the default gateway have to be configured first with the menu control options on the front panel of the CryptoServer LAN. For step-by-step instructions, see the [CryptoServer LAN - Quick Start Guide \(p. 106\)](#) or the [CryptoServer LAN V5 – Administration Manual \(p. 106\)](#). From CSLANOS version 4.2.0 and later the Internet Protocols IPv4 and IPv6 are supported. In CAT, always use IP addresses without leading zeros although they are shown in the display on the front panel of the CryptoServer LAN, e.g., 194.168.004.107.

4. Click **Add to List** to confirm the entry.
5. Click **Test** to check whether a connection to the device can be established.
 - If the connection has been created successfully, a message appears both in a separate window and in the CAT main window.

6. Click **OK**.
 - The **CryptoServer Devices** dialog box.



The new CryptoServer Device has been set up successfully and the information field of the CAT main window confirms the connection, additionally displaying information about the date and time of the connection.

4.2 Switching between Devices

In the left part of the status bar in CAT's main window, you see which devices have been set up. Here you can select which devices you want to administer with the CAT.

4.3 Setting up Microsoft CryptoAPI and Cryptography API: Next Generation (CNG)

The CSP/CNG cryptographic interface is accessed via the CXI firmware module and cannot be configured by using CAT.



You must generate and import an MBK into the CryptoServer before you can use Microsoft CSP/CNG.

For a detailed functional description and instructions about how to configure the CryptoServer CSP/CNG Provider, see [CryptoServer - CryptoServer CSP and CNG Key Storage Provider \(p. 106\)](#). The document is provided on the SecurityServer/CryptoServer SDK product CD in the directory `\Documentation\Administration Guides`.

4.4 Setting up a PIN Pad

Prerequisites

- The device address of the CryptoServer is set up in CAT (see [Setting up a New Device \(p. 12\)](#)).
- The supplied PIN pad is connected to the host computer.

- For Windows: The PIN pad driver is installed, see *Installing the PIN Pad Driver* in the [CryptoServer - Administration Manual \(p. 106\)](#).
- For Linux: The udev rule is defined, see *Installing the PIN Pad Driver* in the [CryptoServer - Administration Manual \(p. 106\)](#).

Procedure

1. Start CAT.
2. Click the **File** menu and select Settings.
→ The **Settings** dialog box opens.
3. Select the **Autodetection** option in the **Type** box.
→ The PIN pad is automatically recognized by the CryptoServer.
In case the PIN pad could not be recognized automatically by the CryptoServer, select the option corresponding to the name of your PIN pad: **REINER SCT cyberJack** or **Utimaco cyberJack One**.
 - a. Select the port the PIN pad is connected to under **Port**. By default, **USB port** is selected.
If you want to use a PIN pad that is connect to another computer in the network, select the **PPD** (PIN pad daemon) option and enter a port number and an IP address. For details, see *Syntax for Authenticating a Command of a CryptoServer Tool/API* in the [CryptoServer – Administration Manual \(p. 106\)](#). The instructions for csadm commands in *Using a Local PIN Pad for a Remote CryptoServer* in the same manual can be used like the actions applied in an analog way to actions in CAT. The **PPD** option is available in the SecurityServer 4.30/CryptoServer SDK 4.30 and later.
4. Click **OK** to confirm your selection.
5. Click the **Timeout** tab.
6. Set the **Connection Timeout** between the CAT and the CryptoServer in milliseconds. The default setting is 5000 milliseconds. This default setting means that the CAT attempts to set up a connection to the CryptoServer for 5 seconds. If this does not succeed, the attempt is interrupted due to a timeout.
7. Click **OK**.



The selected settings are saved and the PIN pad has been set up successfully.



When using the PIN pad at a later date for an authentication, make sure that the PIN pad is connected to the correct port, see *Authentication Mechanisms* in the [CryptoServer - Administration Manual \(p. 106\)](#) or [Logging in a User \(p. 27\)](#).

4.5 Setting up JCE

This chapter describes how to configure the Java Cryptography Extension (JCE) to work with the CAT.

4.5.1 Setting up a User for JCE

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 20000000,
see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
5. Click **Manage User** in the toolbar.
→ The User Management dialog box opens.
6. Click **Add User...**
→ The **Add User** dialog box opens.
7. In the **Name of New User** field, enter the name Cryptographic User.



Do not use the characters `<, >, :, ", !, ?, *, /, \, |` in user names.

8. In the **User Profile** drop-down combo box, select **Cryptographic User**.
9. In the **Authentication Mechanism** group, select the authentication mechanism that should be used to authenticate the user.
10. Optionally enter attributes in the **Custom String** field of the **Attributes** group. If you do not set an attribute, the cryptographic user will not be able to access any cryptographic key on the CryptoServer.

Each cryptographic key on the CryptoServer is assigned to a specific key group called `CXI_GROUP`, and can only be accessed by users who are members of the same `CXI_GROUP`. The `CXI_GROUP` membership has to be set on user creation as an attribute in the **Custom String** field in the format `CXI_GROUP=<Name of the group>`. If the cryptographic user should be granted access to keys in multiple key groups, set `CXI_GROUP=*`.



Do not use the characters `<`, `>`, `:`, `"`, `!`, `?`, `*`, `/`, `\`, `|` in the name of the CXI key group.

11. Click **OK** to confirm your selection.
12. Depending on which authentication mechanism you selected, follow the instructions in the CAT or on the PIN pad.



The JCE user has been created successfully.



The authentication status 00000002 for the user Cryptographic User has already been defined when the CXI interface was programmed and cannot be changed retrospectively at a later date.

4.5.2 Modifying the Device Address and User Name in the File CryptoServer.cfg

The `CryptoServer.cfg` file must be modified and provided to use JCE. The file can be found in the default directory `C:\Program Files\Utimaco\SecurityServer\Software\JCE\`.

The file must be modified for the used CryptoServer hardware (CryptoServer PCIe card or CryptoServer LAN). From CSLAN version 4.2.0 onwards, the Internet Protocols IPv4 and IPv6 are supported. If you want to use the CryptoServer Simulator, enter `3001@127.0.0.1` as the device.

A **DefaultUser** with the name `JCE` has already been created in this configuration file. This name has to be modified as well.

Procedure

1. Open the `CryptoServer.cfg` file with an appropriate text editing program. After installation, the `CryptoServer.cfg` file looks like this:

```
Configuration File for JCE CryptoServer Provider

#LogFile = C:/<user directory>/CryptoServerJCE.log#LogLevel = 2
#LogSize = 10000

# exemplary device specifier
#Device = 192.168.4.183 Device = PCI:0
#Device = 3001@127.0.0.1
#Device = /dev/cs2

# exemplary cluster configuration:
#Device = PCI:0 \
# 192.168.4.183 \
# 192.168.4.185 \
# 192.168.4.186

ConnectionTimeout = 3000
Timeout = 30000
EndSessionOnShutdown = 1
KeepSessionAlive = 0
DefaultUser = JCE
#KeyGroup = MyGroup
#KeySpecifier = 42

#StoreKeysExternal = false
#KeyStorePath = C:/<user directory>/JCE.sdb
```

All lines starting with a number sign (#) are comments, i. e., these lines do not apply. In the example above several devices have been set up (`Device =`) but only the line without a number sign at the beginning of the line (`Device = PCI:0`) applies after the installation. All device entries you are not currently using must have the # in front.



The `ConnectionTimeout` parameter specifies the maximum time in milliseconds to wait before the connection establishment is aborted if the device is not responding.

In practice, the timeout can reach approximately $2 \cdot n \cdot T$.

Legend:

- n: Number of HSMS specified by the `Device` parameter
- T: The timeout value specified by the `ConnectionTimeout` parameter

The `Timeout` parameter specifies the maximum time in milliseconds to wait for the answer from CryptoServer after sending a command.

In practice, the timeout can reach approximately $2 \cdot n \cdot T$.

Legend:

- n: Number of HSMS specified by the `Device` parameter
- T: The timeout value specified by the `Timeout` parameter

2. Modify it to suit your situation.

Examples:

- If you are using a CryptoServer PCIe card in a Windows computer and the card is located in the second slot, change `PCI:0` to `PCI:1`.
- If you are using a CryptoServer PCIe card in a Linux computer and the card is located in the first slot, remove the number sign in front of the `#Device = /dev/cs2` entry, and change this entry to `/dev/cs2.0`. If the card is in the second slot, change it to `/dev/cs2.1`.
- If you are using a CryptoServer LAN, remove the number sign in front of the `#Device = 192.168.4.183` entry, and enter the IP address of your CryptoServer LAN.
- If you want to use the CryptoServer Simulator, enter `3001@127.0.0.1`.

3. Modify the name of the **DefaultUser** from `JCE` to `Cryptographic User` that has been created according to [Setting up a User for JCE \(p. 16\)](#).



You do not have to assign a password to the **DefaultUser**.

4. Save your changes and close the `CryptoServer.cfg` file.



The `CryptoServer.cfg` file has been modified.

4.6 Setting up CXI

You can administer all cryptographic interfaces via the CXI interface, which was specially developed by Utimaco IS GmbH. You can control all other cryptographic interfaces and their functions on the CryptoServer via the CXI interface. In this respect, the CXI interface plays a more prominent role than the other cryptographic interfaces.

Prerequisites

- The Master Backup Key (MBK) is loaded into the CryptoServer.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with at least authentication status 20000000, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
5. Click **Manage User** on the toolbar.
→ The **User Management** dialog box opens.
6. Click **Add User**.
→ The **Add User** dialog box opens.
7. In the **Name of New User** field, enter a unique name for the CXI user, e.g. `CXIuser`.



Do not use the characters `<, >, :, ", !, ?, *, /, \, |` in user names.

8. Select the predefined **Cryptographic User** profile under **User Profile**.

9. Under **Authentication Mechanism**, select the required authentication mechanism you require. If a password is used (HMAC), a password must be assigned.
10. Optionally enter attributes in the **Custom String** text box of the **Attributes** group. If you do not set an attribute, the cryptographic user will not be able to access any cryptographic key on the CryptoServer.

Each cryptographic key on the CryptoServer is assigned to a specific key group called `CXI_GROUP`, and can only be accessed by users who are members of the same `CXI_GROUP`. The `CXI_GROUP` membership has to be set on user creation as an attribute in the **Custom String** text box in the format `CXI_GROUP=<Name of the group>`. If the cryptographic user should be granted access to keys in multiple key groups, set `CXI_GROUP=*`.



Do not use the characters `<`, `>`, `:`, `"`, `!`, `?`, `*`, `/`, `\`, `|` in the name of the CXI key group.

11. Click **OK** to confirm your selection.



The CXI user has been set up successfully.



The authentication status 00000002 for the user Cryptographic User was defined when the CXI interface was programmed and cannot be changed retrospectively.

4.7 Setting up Extensible Key Management (EKM)

The CryptoServer supports Extensible Key Management (EKM) for the following versions of SQL Server:

- Microsoft SQL Server, SP1, on a Windows Server 2008
- Microsoft SQL Server 2008 R2 on a Windows Server 2008 R2

On the CryptoServer, EKM functions are provided by the CXI firmware module.



The Master Backup Key (MBK) must be loaded into the CryptoServer before EKM can be used.

4.7.1 Setting up an EKM User

A Cryptographic User has been created in this firmware module. This Cryptographic User is also the EKM user. You must set up the Cryptographic User on the CryptoServer before you can use EKM. The CAT provides the appropriate authorization profile for the Cryptographic User.

Procedure

1. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
2. Log in to the CryptoServer with an authentication status of at least 20000000,
see [Logging in a User \(p. 27\)](#).
3. Click **Close**.
4. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.
5. In the **User Management** dialog box, click the **Add User** button.
→ The **Add User** dialog box opens.
6. In the **Name of New User** field, enter a unique name for the Cryptographic User. In our example, this is S ven .



Do not use the characters `<, >, :, ", !, ?, *, /, \, |` in user names.

7. Select the predefined **Cryptographic User** profile in the **User Profile** group.
8. In the **Authentication Mechanism** group, select **Password (HMAC)**.
9. Optionally enter attributes on the **Custom String** text box of the **Attributes** group. If you do not want EKM to have the ability to process clients, do not enter anything.
Each cryptographic key on the CryptoServer is assigned to a specific key group called

`CXI_GROUP`, and may only be accessed by users who are members of the same `CXI_GROUP`. Therefore, the `CXI_GROUP` membership has to be set on user creation as an attribute in the **Custom String** text box.

If you want EKM to have the ability to process clients, you must set the following in the Attributes group: `CXI_GROUP=<Name of the group>`. We use `SvenGroup` for our example: `CXI_GROUP=SvenGroup`. If the cryptographic user should be granted access to keys in multiple key groups, set `CXI_GROUP=*` as the user attribute.



Do not use the characters `<`, `>`, `:`, `"`, `!`, `?`, `*`, `/`, `\`, `|` in the name of the group (`CXI_GROUP=`).

10. Click **OK**.
→ The **Set Password of new User** dialog box opens.
11. Enter a unique password for the Cryptographic User.
12. Confirm the password.
13. Click **OK**.



The EKM user has been created successfully.

4.7.2 Modifying the Device Address in the File `cssqlekm.cfg`

The `cssqlekm.cfg` configuration file must be modified and provided to use EKM. The file can be found on your SQL in the default directory `C:\ProgramData\Utimaco\EKM`.

The file must be modified for the used CryptoServer hardware (CryptoServer PCIe card or CryptoServer LAN). As of CSLAN version 4.2.0, the Internet Protocols IPv4 and IPv6 are supported. If the CryptoServer Simulator should be used, enter `3001@127.0.0.1` as the device specifier.

Procedure

1. Use an appropriate text editor to open the configuration file `cssqlekm.cfg`. The `cssqlekm.cfg` configuration file looks like this on your SQL Server:

```
# This is a sample configuration file

# path to logfile
LogFile = C:/ProgramData/Utimaco/EKM/cssqlekm.log

# loglevel
LogLevel = 3

# maximum logsize in bytes
LogSize = 1000000

# path to the EKM Keystore
KeyStore = C:/ProgramData/Utimaco/EKM/cssqlekm.sdb

# local CryptoServer device
Device = PCI:0

# remote CryptoServer
#Device = 192.168.1.2

# cluster of Cryptoserver
#Device = PCI:0 192.168.4.183
# 192.168.4.184
# 192.168.4.185
# 192.168.4.186
# 192.168.4.187

# timeout on connection attempt
ConnectionTimeout = 5000

# command timeout
Timeout = 60000
```

All lines starting with a number sign (#) are comments, i. e., these lines do not apply. In the example above several devices have been set up (Device =) but only the line without a number sign at the beginning of the line (Device = PCI:0) applies after the installation.

2. Adjust the following part of the configuration file according to your situation. All device entries you are not currently using must have the # in front.

```
# local CryptoServer device
Device = PCI:0

# remote CryptoServer
#Device = 192.168.1.2
```


Examples:

- If you are using a CryptoServer PCIe card in a Windows computer and the card is located in the second slot, change `PCI:0` to `PCI:1`.
 - If you are using a CryptoServer PCIe card in a Linux computer and the card is located in the first slot, remove the number sign in front of the `#Device = /dev/cs2` entry, and change this entry to `/dev/cs2.0`. If the card is in the second slot, change it to `/dev/cs2.1`.
 - If you are using a CryptoServer LAN, remove the number sign in front of the `#Device = 192.168.4.183` entry, and enter the IP address of your CryptoServer LAN.
 - If you want to use the CryptoServer Simulator, enter `3001@127.0.0.1`.
3. If you use a cluster of CryptoServers and an MSSQL Error 33027 "Cannot load library 'C:\...\Lib\cssqlekm.dll'" is shown when you access the EKM provider, make sure that there are no backslashes after the IP addresses.

Example: Replace

```
# cluster of Cryptoserver
#Device = PCI:0 192.168.4.183 \
# 192.168.4.184 \
# 192.168.4.185 \
# 192.168.4.186 \
# 192.168.4.187
```

by the following:

```
# cluster of Cryptoserver
Device = PCI:0 192.168.4.183
      192.168.4.184
      192.168.4.185
      192.168.4.186
      192.168.4.187
```

4. Save your changes and close the `cssqlekm.cfg` file.



The `cssqlekm.cfg` file has been modified.

4.7.3 Creating a Credential on the SQL Server

To enable the SQL database to work with the CryptoServer, a credential must be created on the SQL Server. To do so, you can for example use the Microsoft SQL Server Management Studio. An SQL Statement must have the following appearance:

```
CREATE CREDENTIAL <credential-name> WITH  
IDENTITY='<CryptoServer=User>@<CXI_GROUP>',
```

```
SECRET='<CryptoServer=User-Password>',
```

```
FOR CRYPTOGRAPHIC PROVIDER utimaco
```

This is the SQL Statement that you need to adjust. The user name and the password of the user Cryptographic User on the CryptoServer need to be entered.

The value of the Attribute that was entered when setting up a user Cryptographic User must match the value entered in the Credential (Identity). Consequently, in our example, the modified SQL Statement would look like this:

```
CREATE CREDENTIAL SvenCred WITH IDENTITY='Sven@SvenGroup',
```

```
SECRET='password',
```

```
FOR CRYPTOGRAPHIC PROVIDER utimaco
```

5 Administering the CryptoServer with CAT

5.1 Basic Administration

This chapter describes the administrative tasks performed on a CryptoServer.

5.1.1 Logging in a User

Specific security-relevant actions can only be performed by users who are logged on to the CryptoServer respectively users who have authenticated themselves successfully against the CryptoServer.

Logging in a User

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
 - The **Login/Logoff User** dialog box opens. It contains a list of all users created on the device and the default user ADMIN.
3. Select the user you require (e.g. ADMIN) and click **Login**.
 - The dialog box **Choose User Token** for Login opens.
4. Select the appropriate authentication mechanism.
 - a. **Smartcard Token**
 - i. If the user is using RSA or ECDSA signature authentication with a smartcard or RSA smartcard authentication, click **Smartcard Token**.
 - ii. Click **OK** in the **Choose User Token for Login** dialog box.
 - iii. Follow the instructions on the PIN pad.

User with RSA/ECDSA signature authentication

The PIN pad can be connected to a USB port of the computer where CAT is running.

User with RSA smartcard authentication

The PIN pad has to be connected directly to the USB port of the CryptoServer PCIe card. It is not sufficient to connect the PIN pad to a port of the computer CAT is running on.

If the user is used on a CryptoServer LAN, the PIN pad may also be connected to a port on the front panel that is directly connected to the CryptoServer

PCIe card. Depending on the CryptoServer LAN version, this is a USB port labeled **CS USB**, **USB CS**, **USB CS2** or **HSM**.

If you use the CryptoServer Simulator, the smartcard must be inserted in any case into a PIN pad that is connected to the computer where CAT is running (USB port), see *Authentication Mechanisms* in the [CryptoServer - Administration Manual](#) (p. 106).

b. **Keyfile Token**

- i. If the user is using an RSA or ECDSA user authentication key stored in a keyfile, click **Keyfile Token**.
 - ii. Click the search button (...) next to the **Key Path** text box. The **Set Name and Path for User Keyfile Token** dialog box opens.
 - iii. Select the keyfile you require, e.g., `ADMIN.key`.
 - iv. Click **Open**.
 - v. In case the keyfile is protected with a password, enter the password in the **Password** text box.
5. Click **OK** in the **Choose User Token for Login** dialog box.
→ The **Choose User Token for Login** dialog box closes.



A green check mark appears on the left hand side of the user item. The user has successfully been logged in.

5.1.2 Setting the Time

The real time clock (RTC) of the CryptoServer shows the date and time with millisecond precision. This precise time information is required for the logfile because every entry is stored here along with the exact time at which it was made. This time information can also be used for applications, such as the timestamp service.



The time of the CryptoServer can be set up by one or more (n-person rule) authenticated users with min. permission 2 (i.e., authentication status 02000000) in the user group 6 or by the default user ADMIN.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. On the **Manage** menu, click **Date/Time**.
→ The CryptoServer Date/Time dialog box opens.

The actual time of the CryptoServer PCIe card has no time zone but it is defined/regarded as a time in the GMT (UTC) time zone. This time is converted into the time zone of the administration computer and is shown in the **CryptoServer time / Local Time** field. The time of the administration computer is shown in the **Apply host time / Local Time** field. The administration computer is the computer CAT is running on.



If a CryptoServer CP5 LAN is used and the time of the CryptoServer CP5 LAN host should be returned, perform the `csadm CSLGetTime` command instead, see *CSLGetTime* in the [CryptoServer – csadm Manual \(p. 106\)](#). If the time of the CryptoServer CP5 LAN host should be set, perform the `csadm CSLSetTime` command.

Two options are available to set up the date and time of the CryptoServer.

- **Apply host time**
Select this option to transfer the date and time from the administration computer and use it for the CryptoServer. The time zone is automatically converted into the GMT (UTC) time zone of the CryptoServer.
- **Apply time manually**
Select this option to set the date and the time of the CryptoServer manually. Use

the predefined date and time format. The time zone is automatically converted into the GMT (UTC) time zone of the CryptoServer.

6. Click **Apply**.
→ The settings are saved.
7. Click **OK**.
The **CryptoServer Date/Time** dialog box closes.



The time of the CryptoServer has been set successfully.



If you only want to view the time on the CryptoServer, and not to set it, you do not need to be logged in to the CryptoServer.



The time of the CryptoServer must be reset after every alarm triggered by a power failure or if the battery level falls too low.

5.1.3 Changing the User Authentication Key of ADMIN

The default administrator ADMIN has a user authentication key stored on a smartcard or as a keyfile, which is known to the manufacturer Utimaco IS GmbH, see *Default Administrator Key* in the [CryptoServer - Administration Manual \(p. 106\)](#). For this reason, it is imperative this user authentication key is changed. The new user authentication key can be generated as a keyfile or on a smartcard. The following example shows how to generate the key on a smartcard.

First, generate a new user authentication key and then assign this key to the default administrator ADMIN. To do so at least three smartcards are needed.

1. Start CAT.

2. In the **Authentication Token** menu, click **Smartcard**.
→ The **Smartcard Token Management** dialog box opens. The **Generate with Backup** tab is shown by default.
3. The default administrator ADMIN is obliged to use the RSA signature method and therefore the **RSA** option must be selected.
4. In the **Key-Info** text box, enter a key name.
5. Select the key length in the **RSA Key Length (bits)** box.



For security reasons, we recommend you not change the default value 2048 for the RSA Key Length (bits).

6. In the **Number of Backups** box, specify how many backups are to be generated from this key. For one backup you require two backup smartcards.
7. Click **Generate**.
8. Follow the instructions on the PIN pad. A confirmation window opens confirming the successful generation of the new authentication token.
9. Click **Close**.
10. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.
11. Select the ADMIN user.
12. Click the **Change Token/Password** button.
→ The **Choose User Token for Login** dialog box opens.
13. Use the current user authentication key to log in to the CryptoServer as the default administrator ADMIN and click **OK**.
→ A confirmation window opens confirming the successful authentication of the ADMIN user.
14. Click **OK**.
→ The dialog box **Choose new User Token** opens.
15. Select **Smartcard Token**.
16. Click **OK**.

17. Insert the smartcard with the new user authentication key into the PIN pad.

18. Press the **OK** key on the PIN pad.



The user authentication key for the default administrator ADMIN has been successfully changed and the system confirms this in a separate window.

5.1.4 Changing the PIN for Smartcards

If a smartcard has been purchased from Utimaco for administering the CryptoServer, we recommend that the predefined default PIN for these cards are changed.

The following PINs on the smartcards can be changed:

- The smartcard PIN for the user authentication key, see [2021-0055 Changing the PIN for the MBK Smartcards \(p. 55\)](#).
- The smartcard PIN for the MBK, see [Changing the PIN for MBK Key Shares on Smartcards \(p. 85\)](#).

5.2 Managing Users

This chapter describes processes for user management.



To create one or more new user, at least permission 2 in the user group 7 (min. required authentication status 20000000) is required.

5.2.1 User Profiles

User profiles with predefined roles have been set up in the CAT for the convenient creation of new users. These user profiles have been assigned the appropriate permissions in their individual user groups, according to their roles. The choice of authentication mechanism is possible only on user creation and cannot be modified at a later point of time. Later on, only

the user's authentication token (password or keyfile) can be changed, which has been created according to the selected authentication mechanism.

<i>User profile</i>	<i>Permission</i>	<i>Default authentication mechanism</i>	<i>Description</i>
ADMIN Manager one-person rule	22000000	Smartcard (RSA Signature) Can only be changed on user creation	Corresponds to the default administrator ADMIN who is granted permission 2 in the user groups 6 (System Administration) and 7 (User Management), and can therefore authenticate all CryptoServer user and system management commands on its own.
ADMIN Manager two-person rule	11000000	Smartcard (RSA Signature) Can only be changed on user creation	Embodies the two-person rule. It is granted permission 1 (limited) in the user groups 6 (System Administration) and 7 (User Management) and requires a second person to authenticate user and system management commands to the CryptoServer.
User Management one-person rule	20000000	Smartcard (RSA Signature) Can only be changed on user creation	Granted permission 2 in user group 7 (User Management) and can authenticate all user management commands to the CryptoServer on its own.
User Management two-person rule	10000000	Smartcard (RSA Signature) Can only be changed on user creation	Embodies the two-person rule. It is granted permission 1 in user group 7 (User Management) and requires a second person to authenticate commands to the CryptoServer.
System Manager one-person rule	02000000	Smartcard (RSA Signature) Can only be changed on user creation	Granted permission 2 in user group 6 (System Administration) and can authenticate all system management commands to the CryptoServer on its own.
System Manager two-person rule	01000000	Smartcard (RSA Signature) Can only be changed on user creation	Embodies the two-person rule. It is granted permission 1 in user group 6 (System Administration) and requires a second person to authenticate system management commands to the CryptoServer.
NTP Manager one-person rule	00200000	Smartcard (RSA Signature) Can only be changed on user creation	Granted permission 2 in user group 5 (NTP Administration) and can authenticate all NTP administration commands to the CryptoServer on its own.

User profile	Permission	Default authentication mechanism	Description
NTP Manager two-person rule	00100000	Smartcard (RSA Signature) Can only be changed on user creation	Embodies the two-person rule. It is granted permission 1 in user group 5 (NTP Administration) and requires a second person to authenticate NTP administration commands to the CryptoServer.
Cryptographic User	00000002	Smartcard (RSA Signature) Can only be changed on user creation	Granted permission 2 in user group 0 and can authenticate all key management commands to the CryptoServer and use cryptographic keys on its own. Use this profile to administer the following cryptographic interfaces: CXI, JCE, CSP/CNG, OpenSSL and EKM.
Customized User	To be defined individually	Password (HMAC) Can only be changed on user creation	This is a user for customer-specific applications, e.g., PKCS#11.

Table 2: User profiles available in CAT

5.2.2 Creating a User

Prerequisites

- Creating a new user must be authenticated by a user manager with at least authentication status 20000000 or the default administrator ADMIN.
- If the user manager uses RSA or ECDSA signature authentication with a smartcard or RSA smartcard authentication, the PIN pad must be connected and the appropriate smartcard and smartcard holder must be available. A smartcard holder is a person knowing the PIN for accessing the smartcard. See *Authentication Mechanisms* in the [CryptoServer - Administration Manual \(p. 106\)](#) or [Logging in a User \(p. 27\)](#) to determine the port the PIN pad has to be connected to.
- If the new user shall use RSA or ECDSA signature authentication with a smartcard or RSA smartcard authentication, a PIN pad must be connected to the host computer where CAT is installed to make the new user's private authentication key available, see [Setting up a PIN Pad \(p. 14\)](#).

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer as a user manager with at least authentication status 20000000 or as the default administrator ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.
6. Click **Add User**.
→ The **Add User** dialog box opens.
7. Enter a unique name for the new user in the **Name of New User** text box.



Do not use the characters `<, >, :, ", !, ?, *, /, \, |` in user names.

When creating a PKCS#11 Security Officer (SO), the name of a Security Officer must be `SO_XXXX` with `XXXX` being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from `SO_0000` to `SO_9999`.

When creating a PKCS#11 User, the name of the User must be `USR_XXXX` with `XXXX` being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from `USR_0000` to `USR_9999`.

When creating a PKCS#11 key manager, it is advisable but not mandatory to use `KM_XXXX` as the name of the key manager with `XXXX` being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from `KM_0000` to `KM_9999`.

For more information, see *PKCS#11 Users* in the [CryptoServer - Administration Manual \(p. 106\)](#).

8. Click **ADMIN Manager one-person rule**.
9. Select the required role-based User Profile. All available user profiles are listed and explained in [User Profiles \(p. 32\)](#). To create the PKCS#11 User, select the **Cryptographic User** profile. To create a user with specific permissions that do not match the permissions

of any predefined user profile, e.g., PKCS#11 Security Officer (SO) or PKCS#11 Key Manager, select the **Customized User** profile.

10. Specify the authentication mechanism for the new user under **Authentication Mechanism**, see *Authentication Mechanisms* in the [CryptoServer - Administration Manual](#) (p. 106). For a PKCS#11 Security Officer or the PKCS#11 User, only HMAC password authentication is supported. For more information, see *PKCS#11 Users* in the [CryptoServer - Administration Manual](#) (p. 106).

Authentication mechanism	Authentication mechanism naming in the user management	Authentication mechanism naming in the "Add User" dialog
HMAC password authentication	HMAC Password	Password (HMAC)
RSA signature authentication with a keyfile	RSA Sign	Smartcard (RSA Signature)
RSA signature authentication with a smartcard		Keyfile (RSA Signature)
ECDSA signature authentication with a keyfile	ECDSA Sign	Smartcard (ECDSA Signature)
ECDSA signature authentication with a smartcard		Keyfile (ECDSA Signature)
RSA smartcard authentication	RSA Smartcard	Smartcard (PIN Pad at CryptoServer)

Table 3: Naming of authentication mechanisms in CAT

11. If the **Customized User** profile is selected, define the user permissions in the different user groups under **Group/Role and Permission Level**, see [User Profiles](#) (p. 32). For a PKCS#11 Security Officer, select **2** in the **Group 2** text box. For a PKCS#11 Key Manager, select **2** in the **Group 1** text box. For more information, see *PKCS#11 Users* in the [CryptoServer - Administration Manual](#) (p. 106).
12. If you are creating a **Cryptographic User** or a **Customized User**, enter an **Attribute** for the user. Each cryptographic key on the CryptoServer is assigned to a specific key group called `CXI_GROUP`, and may only be accessed by users who are members of the same `CXI_GROUP`. Therefore, the `CXI_GROUP` membership has to be set on user creation as an **Attribute** in the format `CXI_GROUP=<Name of the group>`. If the cryptographic user should be granted access to keys in multiple key groups, set `CXI_GROUP=*` as the user attribute. For PKCS#11 User (Key Manager) or Security Officer the correct format

for the attribute is `CXI_GROUP=<slot number>`, for example for PKCS#11 slot 1
`CXI_GROUP=SLOT_0001`.



Do not use the characters `<`, `>`, `:`, `"`, `!`, `?`, `*`, `/`, `\`, `|` in the name of the CXI key group.

If no attribute is set, the cryptographic user/key manager will not be able to access any cryptographic key on the CryptoServer,

13. Click **OK**.

- a. If the **Password (HMAC)** is the selected authentication mechanism, the **Set Password of new User** dialog box opens.
 - i. Enter a unique, secure password in the **Password** text box.
 - ii. Confirm your password entry in the **Confirm Password** text box.
 - iii. Click **OK**.
→ The dialog box **Add User** closes.
- b. If the **Smartcard (RSA Signature)**, **Smartcard (ECDSA Signature)** or **Smartcard (PIN Pad on CryptoServer)** authentication mechanism is selected, the **Choose User Token to Add a New User** dialog box opens with the preselected option **Smartcard Token**.
 - i. Click **OK** and follow the instructions on the display of the PIN pad.
 - ii. Insert the smartcard the key is stored on, and press **OK** on the PIN pad.
→ The dialog box **Add User** closes.
- c. If the **Keyfile (RSA Signature)** or **Keyfile (ECDSA Signature)** authentication mechanism is selected, the **Choose User Token to Add a New User** dialog box opens with the preselected option **Keyfile Token**.
 - i. Click **OK**.
 - ii. Click the search button (...) next to the **Key Path** field.
 - iii. Select the keyfile path.
 - iv. Click **Open**.
 - v. Click **OK** in the **Choose User Token to Add a New User** dialog box.
→ The dialog box **Add User** closes automatically.



The new user was created successfully and appears in the list of users in the **User Management** dialog box.

5.2.3 Adding PKCS#11 Security Officers with RSA Signature Authentication with a Smartcard

The process for creating a new user, see [Creating a User \(p. 34\)](#), includes the following specifications for PKCS#11 Security Officers:

- The name of a Security Officer must be `SO_xxxx` with `xxxx` being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from `SO_0000` to `SO_9999`.
- The Security Officer must have at least permission 00000200.
- The Security Officer must be assigned to the appropriate key group/PKCS#11 slot. The slot specifier may range from `SLOT_0000` to `SLOT_9999`.
- Only HMAC password authentication is supported.

However, if there is the need to enforce having two users with RSA signature authentication with a smartcard to perform actions as a Security Officer, this section describes how to create the needed users.

Needed Users

- A Security Officer named `SO_0000` (0000 for PKCS#11 slot 0) with permission 00000000 and HMAC password authentication. The purpose of this user is to provide a user with the needed name `SO_0000` and the HMAC password authentication enforced by PKCS#11. The permission must be 00000000 so that this user cannot perform any action at all and other users providing the needed permissions and the desired RSA signature authentications with a smartcard are needed.
- A Security Officer named, for example, `SOSC1_0000` with permission 00000100 and RSA signature authentication with a smartcard. This user provides the desired RSA signature authentication with a smartcard and the first half of the needed permission.

- A Security Officer named, for example, `SOSC2_0000` with permission 00000100 and RSA signature authentication with a smartcard. This user provides the desired RSA signature authentication with a smartcard and the second half of the needed permission.

When all three users are logged in, the summarized permission of the three users is $00000000 + 00000100 + 00000100 = 00000200$.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer as a user manager with at least authentication status 20000000 or as the default administrator ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box.
5. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.
6. Click **Add User**.
→ The **Add User** dialog box opens.
7. Enter `SO_0000` in the **Name of New User** text box.
8. Click **ADMIN Manager one-person rule**.
9. Select the **Customized User** profile.
10. Specify the key group/PKCS#11 slot specifier under **Attribute > Custom String**.
Example for PKCS#11 slot 0: `CXI_GROUP=SLOT_0000`
11. Click **OK**.
→ The **Set Password of new User** dialog box opens.
12. Enter a unique, secure password in the **Password** text box.
13. Confirm your password entry in the **Confirm Password** text box.
14. Close the **Set Password of new User** dialog box by clicking **OK**.
→ The dialog box **Add User** closes automatically. The new user is created and appears in the list of users in the **User Management** dialog box.

15. Click **Add User**.
→ The **Add User** dialog box opens.
16. Enter a unique name for the new user, for example, `SOSC1_0000`, in the **Name of New User** text box.
17. Click **ADMIN Manager one-person rule**.
18. Select the **Customized User** profile.
19. Click **Smartcard (RSA Signature)** under **Authentication Mechanism**.
20. Select **1** in the **Group 2** text box under **Group/Role and Permission Level**.
21. Specify the key group/PKCS#11 slot specifier under **Attribute > Custom String**.
Example for PKCS#11 slot 0: `CXI_GROUP=SLOT_0000`.
22. Click **OK**.
→ The **Choose User Token to Add a New User** dialog box opens with the preselected option **Smartcard Token**.
 - a. Click **OK** and follow the instructions on the display of the PIN pad.
23. Insert the smartcard the key is stored on and press **OK** on the PIN pad.
→ The dialog box **Add User** closes automatically. The new user is created and appears in the list of users in the **User Management** dialog box.
24. Repeat the user creation process and replace the name of the user to be created, `SOSC1_0000` by, for example, `SOSC2_0000`.
25. Click **Close**.
26. Log in the three new users, see [Logging in a User \(p. 27\)](#).



Three users are now logged in with a minimum permission of 00000200 and the desired actions as a Security Officer can be performed.



As an alternative, the steps in *Adding PKCS#11 Security Officers with RSA Signature Authentication with a Smartcard* in the [CryptoServer – csadm Manual \(p. 106\)](#) can be performed.

5.2.4 Deleting a User



To guarantee that the CryptoServer can be administered even after deleting the default user ADMIN, an internal check of the permissions of the remaining users is performed every time a user should be deleted. The default user ADMIN or any other CryptoServer user will only be deleted if the sum of the permissions of the remaining users, using a signature-based authentication mechanism, is at least 2 in the user group 7 and at least 1 in the user group 6. Otherwise, the deletion of the user will fail by returning the appropriate error message

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 20000000 or as the default user ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click the **Manage User** button in the toolbar.
→ The **User Management** dialog box opens.
6. Select the user to be deleted from the user list.
7. Click **Delete User...**.
→ A separate window asks for confirmation for the deletion.
8. Confirm the deletion with **Yes**.



The selected user has been deleted successfully.

5.2.5 Creating a User Data Backup

Prerequisites

- The Master Backup Key (MBK) is imported into the CryptoServer, see [Importing an MBK \(p. 79\)](#). If the MBK in MBK slot 3 is the autogenerated MBK named **AUTO-GEN**, no user data can be backed up.
- As of SecurityServer 6.0.0, a new user backup structure/format has been introduced.
 - For creating and restoring backups, it is recommended to use a SecurityServer/ CAT version that matches the firmware version.
 - Backups with the format earlier than 6.0.0 are still possible to be restored, except in FIPS mode because FIPS does not allow the old format.
 - Restoring a backup with the new format into firmware version < 6.0.0 is not possible. This procedure would cause an `Illegal length of command block` error (B0830008). Generally, restoring backups of a newer firmware version into older firmware is not supported.
 - As of version 6.0.0, customers must perform a user backup (no database backup) to back up users, because backing up the user database (`user.db`) is not supported anymore.



As of u.trust Anchor FIPS 140-3 6.0.0, a new firmware and a new user data backup format are applied. As a consequence, if you have backed up user data using an u.trust Anchor < 6.0.0 (i.e. using the old firmware with the old user data backup format), this data backup cannot be restored in one step by u.trust Anchor FIPS 140-3 >= 6.0.0.

Instead, proceed as follows:

- a. Restore the user data backup using u.trust Anchor non-FIPS >= 6.0.0.
- b. Create a new user data backup using u.trust Anchor non-FIPS >= 6.0.0 (i.e. using the new firmware with the new user data backup format).
- c. Restore the new user data backup using u.trust Anchor FIPS 140-3 >= 6.0.0 (i.e. using the new firmware with the new user data backup format).



If the CryptoServer version is < V4.30, the user ADMIN is not included in the backed up file.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 20000000,
see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.
6. Click **Backup Users...**
→ The **Set Name and Path for User Backup File** dialog box opens.
7. In the **File name** text box assign a unique name for the backup file.
8. Click **Save**.



The user backup file is stored by default in the `C:\Program Files\Utimaco\SecurityServer\Administration` directory. The type of the created backup file is by default `UserBackup (*.ubu)`.

5.2.6 Restoring User Data

Prerequisites

- The MBK that has been used to create the user data backup now must have been imported into the CryptoServer.
- As of SecurityServer 6.0.0, a new user backup structure/format has been introduced.
 - For creating and restoring backups, it is recommended to use a SecurityServer/CAT version that matches the firmware version.
 - Backups with the format earlier than 6.0.0 are still possible to be restored, except in FIPS mode because FIPS does not allow the old format.
 - Restoring a backup with the new format into firmware version < 6.0.0 is not possible. This procedure would cause an `Illegal length of command block` error.

ror (B0830008). Generally, restoring backups of a newer firmware version into older firmware is not supported.

- As of version 6.0.0, customers must perform a user backup (no database backup) to back up users, because backing up the user database (`user.db`) is not supported anymore.



As of u.trust Anchor FIPS 140-3 6.0.0, a new firmware and a new user data backup format are applied. As a consequence, if you have backed up user data using an u.trust Anchor < 6.0.0 (i.e. using the old firmware with the old user data backup format), this data backup cannot be restored in one step by u.trust Anchor FIPS 140-3 >= 6.0.0.

Instead, proceed as follows:

- Restore the user data backup using u.trust Anchor non-FIPS >= 6.0.0.
- Create a new user data backup using u.trust Anchor non-FIPS >= 6.0.0 (i.e. using the new firmware with the new user data backup format).
- Restore the new user data backup using u.trust Anchor FIPS 140-3 >= 6.0.0 (i.e. using the new firmware with the new user data backup format).

If users cannot be restored, for example because they use a HASH that is no longer supported for HMAC authentication, they will be skipped during the restore. Administrators get an output, how many users have been restored and listing those who could not be restored.

For example, skipping/not restoring invalid users prevents users who can no longer log in from ending up in the database.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 20000000 or as the default user ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click **Manage User** in the toolbar.
→ The **User Management** dialog box opens.

6. Click **Restore Users...**
→ The **Restore Behavior** dialog box opens.
7. Select one of the offered options.
 - **Replace user.db with backup** (default)

Scenario	Action	Audit Log Entry	Output
User in the backup file does not exist yet in the <code>user.db</code> database.	User is added.	Restore User	User <user name> added to user.db
User in the backup file already exists in the <code>user.db</code> database.	User is overwritten.	Delete User and Restore User	User <user name> replaced in user.db
A single user manager is logged in and this user manager is included in the backup file or several user managers are logged in and at least one of these user managers is included in the backup file.	<code>error number != 0</code> and The restore operation is aborted and not a single user account is restored.	None	RestoreUser in 'replace' mode is not supported when logged-in user manager(s) shall be restored.
User exists in the <code>user.db</code> database but not in the backup file.	User is deleted. If this user is a single logged-in user manager, deleting this user manager is the last operation of the procedure, because deleting this user manager terminates the Secure Messaging session.	Delete User	User <user name> removed from HSM

- **Add users from backup and overwrite existing users**

Scenario	Action	Audit Log Entry	Output
User in the backup file does not exist yet in the <code>user.db</code> database.	User is added.	Restore User	User <username> added to user.db
User in the backup file already exists with in the <code>user.db</code> database and user is not logged in.	User is overwritten.	Delete User and Restore User	User <user name> replaced in user.db

Scenario	Action	Audit Log Entry	Output
User in the backup file already exists with in the <code>user.db</code> database and user is logged in.	None	None	User <user name> not replaced in <code>user.db</code> because the user is currently logged in
User exists in the <code>user.db</code> database but not in the backup file.	None	None	None



However, this applies only to the logged-in user of the current session to perform the CAT action. If a user is logged in by using another tool, for example, via P11CAT, this user is overwritten.

- Add users from backup

Scenario	Action	Audit Log Entry	Output
User in the backup file does not exist yet in the <code>user.db</code> database.	User is added	Restore User	User <username> added to <code>user.db</code>
User in the backup file already exists with in the <code>user.db</code> database.	None	None	User <username> not added to <code>user.db</code> because the account already exists
User exists in the <code>user.db</code> database but not in the backup file.	None	None	None

The audit log entries `Delete User` and `Restore User` mentioned above are actually as follows:

FC:0x083 SFC:0x05 Delete User '<user name>' [error code]

and

FC:0x083 SFC:0x0D Restore User '<user name>' (<Optional user name>, <authentication mechanism ID> <user's permission>) [error code]

See `OS_AUDIT_CLASS_USER` in the [CryptoServer - Administration Manual \(p. 106\)](#) for details.

8. Click **Backup File**.

→ The **Open User Backup File** dialog box opens.

9. Select the appropriate user backup file (*.ubu).
10. Click **Open**.
11. Click **OK**.



The user was restored successfully. A confirmation note in the information field of the CAT main window is displayed.

5.2.7 Changing a User Authentication Token

A user can change their password or user authentication key.

The authentication mechanism cannot be changed. Once it has been decided that a particular user shall log in using an HMAC password that cannot be changed retrospectively. Only the password itself can be changed or swapped.

1. Open CAT.
2. Click **Manage User**.
 - The **User Management** dialog box opens.
3. Select your user name in the list of users.
4. Click the **Change Token/Password** button.
 - The **User Password of <user name>** dialog box opens.
5. Enter your current password in the **Password** text box.
6. Click **OK**.
 - The **User Password of <user name>** dialog box closes and the **Change User Password** dialog box opens.
7. Enter here in the **Confirm Old Password** text box your old password.
8. Enter here in the **New Password** text box your new password.
9. Repeat your new password entry in the **Confirm New Password** text box.
10. Confirm the entry by clicking **OK**.
 - The **Change User Password** dialog box closes. In a separate window, you now see that you have successfully changed your password.

11. Click **OK** to close this window.
12. Click **Close**.
 - The **User Management** dialog box closes.



The authentication token has been changed successfully.

5.2.8 Changing Another User's Authentication Token

As an administrator, e.g., the default administrator ADMIN, you can change the password of another user. To do so, proceed as follows:

1. Open CAT.
2. Log in as an administrator (see [Logging in a User \(p. 27\)](#)).
3. Click **Manage User**.
 - The **User Management** dialog box opens.
4. Select the other user's name in the list of users.
5. Click the **Change Token/Password** button.
 - The **Change User Password** dialog box opens.
6. Enter here in the **New Password** text box the new password for the other user.
7. Repeat your new password entry in the **Confirm New Password** text box.
8. Confirm the entry by clicking **OK**.
 - The **Change User Password** dialog box closes. In a separate window, you now see that you have successfully changed your password.
9. Click **OK** to close this window.
10. Click **Close**.
 - The **User Management** dialog box closes.



The authentication token has been changed successfully.

5.3 Managing Smartcards and Keys

CAT provides a wide range of key and smartcard management functions.

5.3.1 Generating a User Authentication Key with Backup Shares on Smartcards

This section describes how CAT generates a user authentication key and copies it on a smartcard. As an option, at least one backup (consisting of two key backup shares) of the generated key can be generated on two additional smartcards.

If a user authentication key on a smartcard should be generated without the possibility of creating any backup of this key, follow the instructions in [Generating a User Authentication Key on a Smartcard without any Backup \(p. 53\)](#).



Any key you can generate on a smartcard is only designed to help administer or use the CryptoServer. You cannot use that key for any other purpose.



Each user authentication key backup consists of exactly two key shares. Do not confuse this with m-out-of-n key shares that are possible for Master Backup Keys (MBKs), see [Generating an MBK \(p. 75\)](#).

Prerequisites

- Ensure that the delivered PIN pad is connected to the computer whereon CAT is installed.
- Ensure that at least one smartcard is at hand for the key to be generated. If optional backups should be generated, two additional smartcards for each backup are needed.

Procedure

1. Open CAT.
2. Click the **Authentication Token** menu.

3. Select **Smartcard**.
→ The **Smartcard Token Management** dialog box opens. The **Generate with Backup** tab is preselected.
4. Specify whether you want to generate an **RSA** or an **Elliptic Curve (DP: brainpoolP320t1)** (ECDSA) key.
An RSA key to be generated overwrites an already existing RSA key on the smartcard. An ECDSA key to be generated overwrites an already existing ECDSA key.
5. Enter a name for the new key in the **Key-Info** text box.
6. Specify the length for your RSA key in the **RSA Key Length (bits)** field. The default length is 2048 bit.
The definition of a specific key length is not necessary for an ECDSA key. Therefore, the **RSA Key Length (bits)** field is made unavailable in case you have previously selected **Elliptic Curve (DP: brainpoolP320t1)**.
7. In the **Number of Backups** text box, specify how many backups are to be generated from this key. By default, one backup of the key will be created on two smartcards. The backup of the key is stored on the smartcard as RSA backup or respectively ECDSA backup.
8. Click **Generate**.
9. Follow the instructions on the PIN pad.
10. Click **Close**.
→ The **Smartcard Token Management** dialog box closes.



The user authentication key with backup shares on smartcards has been generated successfully.

5.3.2 Restoring a User Authentication Key from a Backup on Smartcards

Prerequisites

- Keep two smartcards whereon the backup of the user authentication key is stored at hand.

- Keep a third smartcard whereon the user authentication key will be restored at hand.
- Connect the delivered PIN pad to the computer whereon CAT is installed.

Procedure

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Smartcard**.
 - The **Smartcard Token Management** dialog box opens.
4. Depending on the key type you want to restore proceed as follows:
 - **Restoring an RSA key**
 - i. Click the **Restore RSA** tab.
 - ii. Click **Restore RSA....**
 - iii. Insert the first RSA backup smartcard into the PIN pad.
 - iv. Press the **OK** key on the PIN pad.
 - v. Enter the PIN of the first RSA backup smartcard.
 - vi. Press the **OK** key on the PIN pad.
 - vii. Insert the second RSA backup smartcard into the PIN pad.
 - viii. Press the **OK** key on the PIN pad.
 - ix. Enter the PIN of the second RSA backup smartcard.
 - x. Press the **OK** key on the PIN pad.
 - xi. Insert the smartcard on which you want to restore the key into the PIN pad.
 - xii. Press the **OK** key on the PIN pad.
 - xiii. Enter the PIN of the smartcard.
 - xiv. Press the **OK** key on the PIN pad.
 - **Restoring an ECDSA key**
 - i. Click the **Restore EC** tab.
 - ii. Click **Restore EC....**
 - iii. Insert the first EC backup smartcard into the PIN.
 - iv. Press the **OK** key on the PIN pad.

- v. Enter the PIN of the first EC backup smartcard.
 - vi. Press the **OK** key on the PIN pad.
 - vii. Insert the second EC backup smartcard into the PIN.
 - viii. Press the **OK** key on the PIN pad.
 - ix. Enter the PIN of the second EC backup smartcard.
 - x. Press the **OK** key on the PIN pad.
 - xi. Insert the smartcard on which you want to restore the key into the PIN pad.
 - xii. Press the **OK** key on the PIN pad.
 - xiii. Enter the PIN of the smartcard.
 - xiv. Press the **OK** key on the PIN pad.
5. Close the dialog confirming the successful key creation by clicking **OK**.
 6. Click **Close**.
 - The **Smartcard Token Management** dialog box closes.



The user authentication key has been restored successfully from a backup on smartcards.

5.3.3 Copying User Authentication Key Backup Shares from One Smartcard to Another Smartcard

An RSA user authentication key backup share and an ECDSA user authentication key backup share stored on a smartcard can be copied to another smartcard. Consider that the RSA key backup share and the ECDSA key backup share are copied at the same time. If the corresponding `c_sadm CopyBackupCard` command is used, only the share specified by the `<keytype>` parameter is copied. For details, see *CopyBackupCard* in the [CryptoServer – csadm Manual](#) (p. 106).

Prerequisites

- Keep the smartcard whereon the backup of the key is stored (source smartcard), and the smartcard to which the key backup should be copied (destination smartcard) at hand.
- Connect the delivered PIN pad to the computer whereon CAT is installed.

Procedure

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Smartcard**.
→ The **Smartcard Token Management** dialog box opens.
4. Click the **Copy** tab.
5. Click **Copy**.
6. Insert the smartcard from which you want to copy the key into the PIN pad.
7. Press the **OK** key on the PIN pad.
8. Enter the PIN of the smartcard.
9. Press the **OK** key on the PIN pad.
10. Insert the smartcard to which you want to copy the key backup into the PIN pad.
11. Press the **OK** key on the PIN pad.



An existing key backup of the same key type on the smartcard will be overwritten. A smartcard can store the following key types at the same time: RSA key, RSA key backup, ECDSA key, ECDSA key backup and Master Backup Key

12. Enter the PIN of the smartcard.
13. Press the **OK** key on the PIN pad.



The authentication key backup shares have been copied successfully from one smartcard to another. A separate dialog box appears to confirm that the key backup has been copied successfully.

5.3.4 Generating a User Authentication Key on a Smartcard without any Backup

This section describes how to generate a user authentication key by the specified smartcard and store this key on the specified smartcard. It is not possible to create any backup of this

key. This user authentication key never leaves this smartcard. An RSA key to be generated overwrites an already existing RSA key on the smartcard. The same applies to EC keys. If a user authentication key should be generated by CAT and stored on the specified smartcard with optional backup shares of this key on additional smartcards, follow the instructions in [Generating a User Authentication Key with Backup Shares on Smartcards](#) (p. 49).



Any key you can generate on a smartcard is only designed to help administer or use the CryptoServer. That key cannot be used for any other purpose.

Prerequisites

- Ensure that the delivered PIN pad is connected to the computer whereon CAT is installed.

Procedure

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Smartcard**.
 - The **Smartcard Token Management** dialog box opens. The **Generate with Backup** tab is preselected.
4. Click the **Generate on Card** tab.
5. Specify whether you want to generate an **RSA** or an **Elliptic Curve (DP: brainpoolP320t1)** (ECDSA) key.

An RSA key to be generated overwrites an already existing RSA key on the smartcard. An ECDSA key to be generated overwrites an already existing ECDSA key.
6. Enter a name for the new key in the **Key-Info** text box.
7. Specify the length for your RSA key in the **RSA Key Length (bits)** field. The default length is 2048 bit.

The definition of a specific key length is not necessary for an ECDSA key. Therefore, the **RSA Key Length (bits)** field is made unavailable in case you have previously selected **Elliptic Curve (DP: brainpoolP320t1)**.
8. Click **Generate**.

9. Follow the instructions on the PIN pad.
10. Click **Close**.
 - The **Smartcard Token Management** dialog box closes.



The user authentication key has been generated successfully on a smartcard without any backup.

5.3.5 Changing the PIN for User Authentication Keys on a Smartcard

This section describes changing the PIN for user authentication keys stored on a smartcard.

Do not confuse this with changing the PIN for Master Backup Key (MBK) shares, which might be stored in parallel on the same smartcard. This is described in [Changing the PIN for MBK Key Shares on Smartcards](#) (p. 85).



You do not have to log in to the CryptoServer to perform the steps described in this section.

Prerequisites

- Ensure that the delivered PIN pad is connected to the computer whereon CAT is installed.

Procedure

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Smartcard**.
 - The **Smartcard Token Management** dialog box opens. The **Generate with Backup** tab is shown by default.
4. Click the **Change PIN** tab.
5. Click **Change PIN**.
6. Insert the smartcard on which you want to change the PIN into the PIN pad and press the **OK** key on the PIN pad.

7. Follow the instructions on the PIN pad.
 - a. Enter the old PIN.
 - b. Enter the new PIN. Only PINs consisting of 6 up to 12 digits are supported.
 - c. Confirm the new PIN.



The PIN was changed successfully and a confirmation window appears.

5.3.6 Showing the Contents of a Smartcard

A smartcard can contain an RSA key, an elliptic-curve cryptography key, an RSA key backup share, an elliptic key backup share and an MBK backup share at the same time.

- **RSA-Key**

An RSA key. The default value is `Utimaco IS GmbH / Init-Dev-1-Key` or `Utimaco IS GmbH / ADMIN-Key` (older default value). Both default keys are the key for the default administrator (ADMIN user name), See *Default Administrator Key* in the [CryptoServer - Administration Manual \(p. 106\)](#) for details.

- **ECC-Key**

An elliptic-curve cryptography key. The default value is `Utimaco IS GmbH / Default_EC_Key`.

- **RSA Key Backup**

An RSA key backup share on the smartcard. For details, see [Generating a User Authentication Key with Backup Shares on Smartcards \(p. 49\)](#).

- **ECC Key Backup**

An elliptic-curve cryptography key backup share on the smartcard. For details, see [Generating a User Authentication Key with Backup Shares on Smartcards \(p. 49\)](#).

- **MBK**

A backup share of a master backup key (MBK).

To show the contents of a smartcard the needed steps are executed locally without a connection to a CryptoServer. Therefore, the state or mode of any underlying CryptoServer is

irrelevant for the command execution, and no authentication at any CryptoServer is necessary.

Procedure

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Smartcard**.
→ The **Smartcard Token Management** dialog box opens.
4. Select the **Info** tab.
5. Click **Show Info**.
6. Insert the smartcard whose contents you want to view into the PIN pad.
7. Press the **OK** key on the PIN pad.
8. Press the **OK** key on the PIN pad again.



The smartcard contents are displayed in a separate window.

Example output:

```
RSA-Key: Utimaco IS GmbH / Init-Dev-1-Key  
ECC-Key: Utimaco IS GmbH / Default_EC_Key  
RSA Key Backup: RsaKey02 #2  
ECC Key Backup: EcKey #2  
MBK: 15: 32 6 AES test 06.03.2017 14:29:15 02 01 BC954D6AD6132A9C
```

5.3.7 Generating a User Authentication Key as a Keyfile



Any key generated as a keyfile is only designed to help administer or use the CryptoServer. That key cannot be used for any other purpose.

1. Start CAT.
2. Click the **Authentication Token** menu.

3. Select **Keyfile**.
→ The **Keyfile Token Management** dialog box opens.
4. In the **Generate** tab, specify the type of the user authentication key to be generated.
You can choose between an **RSA** key and an ECDSA key using the **Elliptic Curve (DP: brainpoolP320t1)**.
5. In the **Keyfile** text box, manually enter a file location and a name for the keyfile or click the search button (...) next to the **Keyfile** text box to select the location to which the key should be saved.
If you have chosen to generate an RSA key, we highly recommend you to keep the default setting 2048 bits for the **RSA Key Length**.



By default, the keyfile will be generated as an encrypted, password-protected keyfile (RSA or ECDSA).



For security reasons, we recommend you only generate encrypted, password-protected RSA and ECDSA keyfiles.

6. Enter the password for the keyfile into the **Password** text box.
7. Confirm your password entry in the **Confirm Password** text box.
8. Click **Generate**.



The user authentication key has been generated successfully as a keyfile. A separate window appears to confirm the successful key generation

5.3.8 Changing the Password for a Keyfile

1. Start CAT.
2. Click the **Authentication Token** menu.

3. Select **Keyfile**.
→ The **Keyfile Token Management** dialog box opens.
4. Select the **Password** tab.
5. Click the search button (...) next to the **Keyfile** text box.
6. Select the keyfile whose password you want to change.
7. In the **Old Password** text box, enter the old password.
8. In the **New Password** text box, enter the new password.
9. Repeat the new password entry in the **Confirm New Password** text box.
10. Click **Change**.
→ A separate window appears to tell you that the smartcard's PIN was changed successfully.
11. Close it by clicking **OK**.
12. Click **Close**.
→ The **Keyfile Token Management** dialog box closes.



The password for the key file has successfully been changed.

5.3.9 Copying a Keyfile to a Smartcard (Backup)

1. Start CAT.
2. Click the **Authentication Token** menu.
3. Select **Keyfile**.
→ The **Keyfile Token Management** dialog box opens. The **Generate** tab is displayed by default.
4. Click the **Copy to Smartcard** tab.
5. Click the search button (...) to select the keyfile you want to copy to the smartcard. Your selection appears in the **Keyfile** text box.
6. If the keyfile is protected with a password, enter this password in the **Password** text box.

7. Click **Backup**.
8. Follow the instructions on the display of the PIN pad. A separate window appears to tell you that keyfile was copied successfully to the smartcard.
9. Click **Close**.
 - The **Keyfile Token Management** dialog box closes.



The keyfile has been copied to the smartcard successfully.

5.4 Managing Databases

5.4.1 Backing up Databases

This section describes how to copy the databases from a CryptoServer and save them to a backup directory.

Prerequisites

- The individual Master Backup Key (MBK) is imported into the CryptoServer and is used to encrypt all data and databases. If the MBK in MBK slot 3 is the autogenerated MBK named **AUTO-GEN**, no database can be backed up.
- As of SecurityServer 6.0.0, a new database backup structure/format has been introduced.
 - For creating and restoring backups, it is recommended to use a SecurityServer/ CAT version that matches the firmware version.
 - Backups with the format earlier than 6.0.0 are still possible to be restored, except in FIPS mode because FIPS does not allow the old format.
 - Restoring a backup with the new format into firmware version < 6.0.0 is not possible. Generally, restoring backups of a newer firmware version into older firmware is not supported.

- As of version 6.0.0, customers must perform a user backup (no database backup) to back up users, because backing up the user database (`user.db`) is not supported anymore.



As of SecurityServer FIPS 140-3 6.0.0, a new firmware and a new backup format are applied. As a consequence, if you have backed up a database using a SecurityServer < 6.0.0 (i.e. using the old firmware with the old backup format), this database backup cannot be restored in one step by SecurityServer FIPS 140-3 >= 6.0.0.

Instead, proceed as follows:

- a. Restore the database backup using SecurityServer non-FIPS >= 6.0.0.
- b. Create a new database backup using SecurityServer non-FIPS >= 6.0.0 (i.e. using the new firmware with the new backup format).
- c. Restore the new database backup using SecurityServer FIPS 140-3 >= 6.0.0 (i.e. using the new firmware with the new backup format).

Procedure

1. Click **Backup/Restore** in the CAT toolbar.
→ The **CryptoServer Database Backup/Restore Wizard** dialog box opens.
2. Click **Backup databases from source CryptoServer to backup directory**.
3. Enter the device address of the source CryptoServer in the **Source CryptoServer** text box.
The device address is the IP address for a CryptoServer LAN, e.g., `PCI:0` for a CryptoServer in a Windows computer, `/dev/cs2.0` for a CryptoServer in a Linux computer or `3001@127.0.0.1` for a CryptoServer Simulator.
4. Enter in the **Backup Directory** text box the directory where the data is to be stored.
5. In the lower part of the dialog box, select the databases to be copied under **Source CryptoServer**. All databases can be selected by clicking **Add All >>**. Databases can be added individually by first selecting them and then clicking **Add >>**. Added databases appear in the **Backup Directory** list.
6. Click **Execute**.
→ The **Login User for Source CryptoServer** dialog box opens.
7. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.

8. Log in to the CryptoServer as ADMIN (or another user with the same authentication status 22000000), see [Logging in a User \(p. 27\)](#).
→ The result of exporting the databases to a backup directory then appears in a **Database Export** window.
9. Click **Close**.



The selected databases have been backed up successfully.

5.4.2 Restoring Databases

This section describes how to copy databases from a backup directory into a CryptoServer.

Prerequisites



The CryptoServer the databases should be copied to must have the same MBK that was used to create the database backup.

As of SecurityServer 6.0.0, a new database backup structure/format has been introduced.

- For creating and restoring backups, it is recommended to use a SecurityServer/CAT version that matches the firmware version.
- Backups with the format earlier than 6.0.0 are still possible to be restored, except in FIPS mode because FIPS does not allow the old format.
- Restoring a backup with the new format into firmware version < 6.0.0 is not possible. Generally, restoring backups of a newer firmware version into older firmware is not supported.
- As of version 6.0.0, customers must perform a user backup (no database backup) to back up users, because backing up the user database (`user.db`) is not supported anymore.



As of SecurityServer FIPS 140-3 6.0.0, a new firmware and a new backup format are applied. As a consequence, if you have backed up a database using a SecurityServer < 6.0.0 (i.e. using the old firmware with the old backup format), this database backup cannot be restored in one step by SecurityServer FIPS 140-3 >= 6.0.0.

Instead, proceed as follows:

1. Restore the database backup using SecurityServer non-FIPS >= 6.0.0.
2. Create a new database backup using SecurityServer non-FIPS >= 6.0.0 (i.e. using the new firmware with the new backup format).
3. Restore the new database backup using SecurityServer FIPS 140-3 >= 6.0.0 (i.e. using the new firmware with the new backup format).

Procedure

1. Start CAT.
2. Click **Backup/Restore** in the CAT toolbar.
→ The **CryptoServer Database Backup/Restore Wizard** dialog box opens.
3. Click **Restore databases from backup directory to target CryptoServer**.
4. Enter in the **Target CryptoServer** text box the device address of the CryptoServer the databases are to be restored to. The device address is the IP address for a CryptoServer LAN, e.g., `PCI:0` for a CryptoServer in a Windows computer, `/dev/cs2.0` for a CryptoServer in a Linux computer or e.g., `3001@127.0.0.1` for a CryptoServer Simulator.
5. Enter in the **Backup directory** text box the directory the databases have been previously stored to.
6. Under **Backup Directory** in the lower part of the dialog box, select the databases that should be copied. All available databases can be selected by clicking **Add All >>**. Databases can be added individually by first selecting them and then clicking **Add >>**. Once you have made your selection, the databases appear in the **Target CryptoServer** list.
7. Click **Execute**.
→ The **Login User for Target CryptoServer** dialog box closes.
8. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
9. Log in to the CryptoServer with an authentication status of at least 22000000, see [Logging in a User \(p. 27\)](#).

10. Click **Close**.



The selected databases are restored successfully. The result of importing the databases from a backup directory into a CryptoServer is displayed in the **Database Import** window



You must restart the CryptoServer (**Manage > Reboot CryptoServer**) so that the restore of the databases gets applied.

5.4.3 Cloning Databases

This section describes how to copy databases from one CryptoServer to another CryptoServer.

Prerequisites

- Ensure that both CryptoServers are running the same version of the SecurityServer package. To show the firmware versions of CryptoServer, click **Show Firmware** in the toolbar of the CAT main window.
- The MBK of the source CryptoServer must be imported into the target CryptoServer, see [Importing an MBK \(p. 79\)](#). This MBK is used to encrypt all database entries before they are copied from the source CryptoServer to the target CryptoServer. An autogenerated MBK named **AUTO-GEN** in MBK slot 3 is not sufficient.
- In case the required MBK is stored on smartcards, make sure that the PIN pad is correctly connected to the computer where CAT is installed on. Furthermore, keep at least m ($m \geq 2$, see [Generating an MBK \(p. 75\)](#)) of the n smartcards, where the required MBK is stored on, at hand before starting.

Procedure

1. Start CAT.
2. Click the **Backup/Restore** button in the CAT toolbar.
→ The **CryptoServer Database Backup/Restore Wizard** dialog box opens.

3. Select **Copy databases from Source CryptoServer to Target CryptoServer**.
4. Enter the device address of the source CryptoServer in the Source CryptoServer text box.
For a CryptoServer LAN, the device address is the IP address. For a CryptoServer in a Windows computer, it is e.g., `PCI:0`, for a Linux computer `/dev/cs2.0`, and for a CryptoServer Simulator e.g. `3001@127.0.0.1`.
5. Enter the IP address of the target CryptoServer in the **Target CryptoServer** text box.
6. Under **Source CryptoServer** in the lower part of the window, select the databases to be copied. All available databases can be selected by clicking **Add All >>**. Databases can be added individually by first selecting them and then clicking **Add >>**.
Selected databases appear in the **Target CryptoServer** list
7. Click **Execute**.
 - CAT first compares the firmware modules of both CryptoServers (source and target) that are involved in this process. The results of this comparison are displayed in an information window.
 - a. If the results show that both CryptoServers have the same firmware modules (OK!), click the **OK** button to close this information window.
 - b. If the results show that the firmware modules or the firmware module status in the s are not identical, click **No** to cancel the operation, or continue by clicking **Yes**.
Comparing the firmware modules and the firmware module status does not actually affect how the databases are copied.
 - The **Login User for Source CryptoServer** dialog box opens.
8. Click **Login/Logoff** in the toolbar.
 - The **Login/Logoff User** dialog box opens.
9. Log in to the CryptoServer with an authentication status of at least 22000000, see [Logging in a User \(p. 27\)](#).
10. Click **Close**.
 - The **Login User for Source CryptoServer** dialog box closes and the **Login User for Target CryptoServer** dialog box opens.
11. Log in to the CryptoServer with an authentication status of at least 22000000, see [Logging in a User \(p. 27\)](#).
12. Click **Close**.
 - The **Login User for Target CryptoServer** dialog box closes and the **CryptoServer Date/Time for Target CryptoServer** dialog box opens. The date and time for the target

CryptoServer can optionally be specified, but have no effect on how the databases are transferred.

13. Select **Apply host time** to transfer the date and time from the host system.
14. Click **Apply**.
→ The changes are saved.
15. Click **OK**.
→ The changes are applied and the **CryptoServer Date/Time for Target CryptoServer** dialog box closes. The **Master Backup Key for Target CryptoServer** dialog box opens. The MBK will encrypt all database entries before they leave the source CryptoServer.



Both CryptoServers involved in this process must have the same Master Backup Key so the databases can be decrypted correctly in the target CryptoServer.

16. In the **Master Backup Key for Target CryptoServer** dialog box, click the **Import** tab. If a **Permission denied** message is shown, verify whether you are logged in with a minimum authentication status of 2 in user group 6 (02000000).
17. For CAT versions < 2.2.5.2 only: Under **MBK Type**, select the type of key you want to import: an **AES (32 byte)** or a **DES (16 byte)** MBK. If the CXI firmware module is part of the loaded firmware, only MBKs of type AES are accepted.
18. Under **m (shares)**, specify the number of parts into which you have split the MBK.
19. Click **Import**.
20. In the **Master Backup Key (MBK): Share Import** dialog box, specify whether the MBK is to be imported from a **Smartcard Token** or from a **Keyfile Token**.
21. Click **OK**.
22. Follow the instructions on the PIN pad and CAT to import all parts of the Master Backup Key into the target CryptoServer.
23. Click **Close**.
→ The **Master Backup Key (MBK): Share Import** dialog box closes.



The databases have been copied from one CryptoServer to another CryptoServer. The results are displayed in a separate information window.

5.5 Managing Logs

5.5.1 Viewing the Boot Log

1. Start CAT.
2. Click the **Show** menu.
3. Select **Boot Log**.
 - You see everything that has been started and initialized by the bootloader when the CryptoServer was booted, e.g. after a reset. Depending on your CryptoServer hardware, specific information is displayed.
 - CryptoServer Se12 or Se52: The message `No Hardware Crypto Engine detected` is displayed. This means that your CryptoServer does not have a cryptographic accelerator chip.
 - CryptoServer Se500 or Se1500: In this case, you see the message `Hardware Crypto Engine detected` because an accelerator chip is present.
 - CryptoServer CSe10 or Se12: the line `CMD5: 1000 TPS` appears in the boot log. In every other model, the line `CMD5: no TPS limit` is displayed.
 - CryptoServer CSe100 Se52, Se500 or Se1500 and the line `CMD5: 1000 TPS` still appears: The reason can be that no license file has been loaded. In this case, the boot log contains the line `No license file found`. Alternatively, it means that the found license file does not match your CryptoServer model that was found. In this situation, check the `Signed License File found: xxx.slf` message to see that the name `xxx` matches the name of the CryptoServer series you are using.
4. Perform a setup.
5. Import the appropriate license file and the corresponding firmware package for your CryptoServer series according to [Installing/Updating the Firmware \(p. 96\)](#).

6. Reboot the CryptoServer.
7. Check once again the corresponding messages in the boot log.



The Boot Log is displayed with the correct information for the signed license file.

5.5.2 Deleting Displayed Log Entries

All data you can display in the CAT main window by clicking the **Show** menu or by clicking **Show Status**, **Show Firmware**, or **Show Files** in the toolbar is only displayed temporarily.

If you want to delete any of the entries in the CAT main window, proceed with these steps:

1. Start CAT.
2. Click the **File** menu.
3. Select **Clear Console Output**.
→ A separate window opens for confirmation if the deletion.
4. Click **OK**.



All information displayed in the CAT main window is cleared.

5.5.3 Saving Displayed Log Entries

In case of an issue with the CryptoServer, the output file of the current log entries in the CAT main windows should be supplied to the customer support of Utimaco IS GmbH for analysis.

To save all information currently displayed in the CAT main window, follow these steps:

1. Click the **File** menu.
2. Select **Save Console Output**.
→ The **CryptoServer Console Output** dialog box opens.

3. In the **File name** text box, assign a unique name for the logfile.
4. Click **Save**.



The logfile is saved successfully in the default directory: `C:\Program Files\Utimaco\SecurityServer\Administration`. The type of the created logfile is by default `Console Output File (*.log)`.

5.5.4 Retrieving and Saving the Audit Log

1. Start CAT.
2. Click the **Show** menu.
3. Select **Audit Log**.
 - The **CryptoServer Audit Log** dialog box opens.

In the **Logged Events** group, you see a list of all events that are written in the audit log. In the **Audit Log Filters** group, you can filter the displayed audit log either by **User** or by **Command/Return Value**.

 - Firmware Management
 - User Management
 - Date/Time Management
 - Startup Messages
 - Audit Log Management
 - MBK Management
 - Failed Login Attempts
 - Backup/Restore
 - Action needed
4. Click **Save Log...**.
 - The **CryptoServer Audit Log File** dialog box opens.
5. Assign a unique name for the audit log file in the **File name** text box.
6. Click **Save**.
 - The audit log file is stored by default in the `C:\Program`

Files\Utimaco\SecurityServer\Administration directory. The type of the created file is by default, *.log.

7. Click **Close**.



The Audit Log has been saved successfully.


5.5.5 Configuring the Audit Log Files

The audit log configuration can be adjusted to match individual requirements. The configuration determines the information to be written into the audit log.

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 22000000,
see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
5. Click the **Manage** menu.
 - a. Select **Audit Log Settings**.
→ The **Audit Log Configuration** dialog box opens.

In this dialog box, you can set up different settings.

Setting	Description
Number of audit log files	Specify the maximum number of audit log files. 3 (default setting) means that three audit log files are recorded on the CryptoServer. Minimum: 2. Maximum: 10.
File size (max. 240)	Specify the maximum size of each audit log file in kilobytes. Default: 200 kb for each audit log file. Minimum: 4 kb.

Setting	Description
When all log files are full	<p>This defines how the audit log files are to be handled when they are full.</p> <ul style="list-style-type: none">• Rotate file The next audit log file is used when the previous audit log file is full. Once all audit log files are full, the oldest audit log file is overwritten (when in Maintenance Mode under special conditions) or the oldest audit log file is deleted and a new audit log file with a not yet existing file name is created, see <i>Audit Log File Names</i> in the CryptoServer – csadm Manual (p. 106).• Stop logging No audit log files are overwritten or created if all audit log files are full. <div><p>If all audit log files are full and Stop logging is selected, all CryptoServer commands generating an audit log file entry will be blocked. In this case, all audit log files must be deleted to be able to administer the CryptoServer again. A CryptoServer user with authentication status 20000000 or 02000000 must be logged in to perform this action.</p></div>

Setting	Description
Events	<p>Specify the events to be recorded in the audit log files. In the default settings for audit log files, only the options Key Management and Successful login attempts are cleared.</p> <ul style="list-style-type: none"> • Firmware management Load, delete and replace firmware modules. • User management Create and delete users, and back up and restore the user database • Date/Time management Set of time and date • Audit log management All aspects of audit log file configuration • MBK management All aspects of MBK management (remote and local) • Key management Key management functions for cryptographic interfaces (for example CXI) • Failed login attempts All unsuccessful attempts to log in to the CryptoServer • Successful login attempts All successful attempts to log in to the CryptoServer • Startup messages All relevant CryptoServer messages during the start phase • Backup/Restore Backup and restore CryptoServer databases. If the CryptoServer databases contain a large number of entries, the volume of data may cause the individual audit log files to overflow. • Action needed This log entry refers to an action that is needed by the SecurityServer administrator (update the host side), even though no error occurred, i.e. the login was successful.

Table 4: Configuration parameters of Audit Log Settings

6. Click **Apply**.
→ All changes are saved and the **Audit Log Configuration** dialog box remains open.
7. Click **OK**.



All changes to the audit log configuration are applied successfully.



The equivalent action can be performed by using audit message class numbers and the csadm tool, see *Auditing* in the [CryptoServer – csadm Manual \(p. 106\)](#).

5.5.6 Deleting an Audit Log



A CryptoServer audit log cannot be restored once it has been deleted. Save the audit log before deleting it, see [Retrieving and Saving the Audit Log \(p. 69\)](#).

To delete an audit log file on the CryptoServer:

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer as a user with at least authentication status 20000000 or 02000000, or as the default user ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
5. Click the **Manage** menu.
6. Select **Audit Log**.
→ The **CryptoServer Audit Log** dialog box opens.
7. Click **Clear Log...**
→ In a separate window the system prompts you to confirm the deletion of the audit log on the CryptoServer.
8. Click **Yes**.



The Audit log has been deleted successfully.



We recommend you to view, save and delete the audit log files regularly especially when the CryptoServer switches quite often between the Maintenance Mode and the Operational Mode. For details about audit log file names, see *Audit Log File Names* in the [CryptoServer – csadm Manual](#) (p. 106).

5.6 Managing Master Backup Keys

The MBK management functions can be performed remotely with CAT. The functions can only be performed locally if the CryptoServer PCIe card is in a CryptoServer LAN and the front panel of the CryptoServer LAN is used.

In this context, remote means that the PIN pad is connected to the host computer from which CryptoServer should be administered. You do not need to be logged in to the CryptoServer to perform the following actions:

- Backing up an MBK
- Changing the PIN of the smartcard the MBK is stored on
- Retrieving information about an MBK

If MBKs should be generated and imported into the CryptoServer, you must log in to the CryptoServer with at least permission 2 in the user group 6 (min. authentication status 02000000).



If an external database is used, make sure not to use the autogenerated MBK. This MBK is shown in the **Name** column of the table at **Manage MBK > Info > MBKs stored in the CryptoServer** as **AUTO-GEN**. If an alarm or an external erase occurs, this MBK is deleted and the external database is inaccessible. Use an MBK instead that you have generated, backed up in keyfiles or on smartcards, see [Generating an MBK](#) (p. 75), and imported into the CryptoServer, see [Importing an MBK](#) (p. 79). If now an alarm or an external erase occurs, reimport the same MBK from the keyfiles or smartcards.

If an external database is accessed from several devices, make sure the same MBK is used in all these devices.

If the MBK used for the encryption of an external database should be changed, perform an MBK rollover. For details, see *Master Backup Key Rollover* in the [CryptoServer – csadm Manual](#) (p. 106).

5.6.1 Generating an MBK

Before the full range of the CryptoServer's functionality can be used, a Master Backup Key (MBK) must be generated and import it into the CryptoServer. This section describes how to generate a Master Backup Key.

Prerequisites

- Determine if the MBK should be stored in keyfiles (outside the CryptoServer) or on smartcards
- Determine how many people the MBK will be distributed to. This specifies the number of key shares the MBK is to be split in. This number is defined as the parameter `n`.
- Determine the minimum number of key shares (people) required to use the MBK. This specifies the number of key shares needed to make the MBK reconstruction possible. This number is defined as the parameter `m`.

`n` defines the number of people to whom the MBK shall be distributed, and `m` defines the minimum number of people required to use the MBK.

The examples below clearly illustrate the relationship between `m` and `n` key shares and show which combinations are useful:

Key Shares	Number	Meaning
n (shares)	4	Four people have a part of the MBK
m (shares)	2	Two of these four people must therefore be present before the MBK can be used

Table 5: Example for an MBK split into 4 key shares

Key Shares	Number	Meaning
n (shares)	2	Two people have a part of the MBK.
m (shares)	2	Two people must be present before the MBK can be used.


Table 6: Example for an MBK split into 2 key shares

- Make sure that the required number `n` of smartcards delivered by Utimaco IS GmbH are present before you start generating the MBK.

- Be able to log in to the CryptoServer with at least permission 2 in the user group 6 (authentication status 02000000) or as the default user ADMIN.
- In case you have decided to use smartcards for the MBK generation, make sure that the PIN pad is correctly connected to the computer CAT is installed on and keep the required number of smartcards at hand.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer as the default administrator ADMIN or as a user with at least permission 2 in the user group 6 (min. authentication status 02000000), see [Logging in a User](#) (p. 27).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click **Manage MBK** in the toolbar.
→ The **Remote Master Backup Key (MBK) Management** dialog box opens. The **Generate** tab is shown by default.
6. In the **MBK Name** text box, enter a name (max. eight characters) for the MBK. Do not name the MBK to be created **AUTO-GEN** because this is the name of the autogenerated MBK. The type of the MBK is predefined (**MBK Type 256 Bit AES Key**) and is unchangeable.
7. Select how many parts you want to split the key into.
 - If XOR is enabled, the key is split into two parts and therefore two people will be needed to use the MBK (two-person rule).
 - If **m out of n** is clicked, any value can be set as the number of parts the MBK is to be split into **n (Shares)** and the number of people needed to use the MBK **m (Shares)**.
In our example, we have selected the **m out of n** option, where **n (Shares) = 3** and **m (shares) = 2**.

8.  Before you import an MBK, verify which backup files have been generated because they might become inaccessible after the import. After having imported an MBK, we recommend to regenerate these backup files. Thus, you have additional backup files, this time made with the new MBK, see *Master Backup Key Rollover* in the [CryptoServer – csadm Manual](#) (p. 106).

If you want the MBK to be imported automatically, select **Automatic MBK Import**. For manual MBK import, see [Importing an MBK](#) (p. 79).

The field **Slot Number** shows the number of the MBK slot on the device the MBK should be imported to. The MBK slot number must be 3 for an AES key (recommended; even mandatory for usage with firmware module CXI) and 0 for a DES key (DES keys are supported for CAT versions < 2.2.5.2 only). the supported value range is 0...255, for SecurityServer/CryptoServer SDK 4.20 or earlier it is 0...3.

Leave the value 3 in the field **Slot number** unchanged unless for certain situations, like an MBK rollover. For details about the MBK rollover, see *Master Backup Key Rollover* in the *CryptoServer – csadm Manual*.

If there is already an old MBK in the MBK slot indicated by **Slot number**, this old MBK is overwritten by the new MBK to be imported. The only exception is the case that **Slot number** is 3 and the old MBK is an autogenerated MBK (shown as the MBK name **AUTO-GEN** in the **Info** tab). In this case, the autogenerated MBK is moved from MBK slot 3 to MBK slot 7 (or to the next free MBK slot > 7 if MBK slot 7 is already occupied by another MBK) and the new MBK is imported into MBK slot 3.

Consider the difference between automatically imported MBKs and an autogenerated MBK. An automatically imported MBK is an MBK the **Automatic MBK Import** check box has been selected for. An autogenerated MBK is an MBK with the name **AUTO-GEN** that has been generated by Utimaco IS GmbH in MBK slot 3 during the production of the device. There is no backup in keyfiles or on smartcards for an autogenerated MBK. To verify which MBK is in a certain MBK slot, click the **Info** tab.

Consider that it is important which MBK is in use in MBK slot 3 by the device because this MBK is used by the actions backing up a user or a database to protect the backup files that are generated by these actions.

It is important to note down which MBK has been used for these backup commands because for a successful restoring of these backup files at a later date it is necessary that the same MBK is in MBK slot 3. Otherwise, for example, after an MBK import or an MBK rollover, the backup files are inaccessible.

9. Click **Generate**.
→ The **Master Backup Key (MBK): Share Storage 1/n** dialog box opens.

10. Specify whether the MBK should be stored on a smartcard (**Smartcard Token**) or as a keyfile (**Key file Token**).



For security reasons, we recommend you store the MBK on a smartcard and keep this in a safe place.

- **Smartcard Token**

The following example requires three smartcards.

- Click **OK** to trigger the generation of an MBK
- Insert the first smartcard into the PIN pad.
- Press the **OK** key on the PIN pad.
- Enter the PIN for the smartcard.
- Press the **OK** key on the PIN pad.
- In a separate CAT window, you now see that you have successfully generated and stored the MBK share on the smartcard. Click **OK** to continue for the next MBK share.
- Keep the **Smartcard Token** option selected and click **OK**.
- Repeat the previous steps for the remaining smartcards n-1 shares.

- **Key file Token**

- In the dialog box **Master Backup Key (MBK): Share Storage 1/<n>**, click the search button (...) next to the **Key Path** text box.
 - The **Set Name and Path for MBK key share 1/<n>** dialog box opens
- Enter the location for the MBK into the **Key Path** text box manually or use the search button (...).
- Click **Save**.
- Specify a password in the **Password** text box to protect the MBK keyfile from unauthorized access.
- Click **OK**.
 - The generation of the MBK is initiated and confirmed in a separated window.

vi. Repeat the previous steps for the remaining two key parts (n-1 shares).

11. Once the MBK is saved either as a keyfile or on a smartcard, click **Close**.



The MBK has been successfully generated and is stored either on a smartcard or as a keyfile.

5.6.2 Importing an MBK

If you have not automatically imported the MBK into the CryptoServer after you have generated it, follow the instructions in this section.

Prerequisites

- Verify which backup files have been generated because they might become inaccessible after the import. After having imported an MBK, we recommend regenerating these backup files to have additional backup files, this time made with the new MBK, see *Master Backup Key Rollover* in the [CryptoServer – csadm Manual \(p. 106\)](#).
- In case you have stored the MBK on smartcards, make sure that the PIN pad is correctly connected to the computer CAT is installed on and keep at least m ($m \geq 2$), see [Generating an MBK \(p. 75\)](#) MBK smartcards at hand before you start.



If you use SecurityServer/CryptoServer SDK 4.10, and you import a new MBK, the external key and key backups become inaccessible. The error message `invalid mac of key blob` (error code: 0xB0680026) is created. This applies as well if you have upgraded to SecurityServer/CryptoServer SDK 4.20 or later after you have imported the original MBK.

If you use SecurityServer/CryptoServer SDK 4.20 and you import a new MBK, the external key and key backups become inaccessible. The error message `key blob encrypted with different MBK` (error code: 0xB0680080) is created.



If the firmware package loaded into your CryptoServer contains the CXI firmware module, you cannot use a DES key as the MBK. The CXI firmware module can only use an AES key as an MBK.

Procedure

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with at least permission 2 in the user group 6 (min. authentication status 02000000) or as the default user ADMIN, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click in the toolbar on **Manage MBK**.
→ The **Remote Master Backup Key (MBK) Management** dialog box opens.
6. Click the **Import** tab. If a **Permission denied** message is shown, verify whether you are logged in with a minimum authentication status of 2 in user group 6 (02000000).
7. For CAT versions < 2.2.5.2 only: Select the key type of the MBK you want to import: **AES (32 bytes)** or **DES (16 bytes)**.
8. Select the number of key shares, **m (shares)**, needed to reconstruct and use the MBK you want to import.
9. The field **Slot Number** shows the number of the MBK slot on the device the MBK should be imported to. The MBK slot number must be 3 for an AES key (recommended; even mandatory for usage with firmware module CXI) and 0 for a DES key (DES keys are supported for CAT versions < 2.2.5.2 only). the supported value range is 0...255, for SecurityServer/CryptoServer SDK 4.20 or earlier it is 0...3.
Leave the value **3** in the field **Slot number** unchanged unless for certain situations, like an MBK rollover. For details about the MBK rollover, see *Master Backup Key Rollover* in the *CryptoServer – csadm Manual*.
If there is already an old MBK in the MBK slot indicated by **Slot number**, this old MBK is overwritten by the new MBK to be imported. The only exception is the case that **Slot number** is **3** and the old MBK is an autogenerated MBK (shown as the MBK name **AUTO-GEN** in the **Info** tab). In this case, the autogenerated MBK is moved from MBK slot 3 to MBK slot 7 (or to the next free MBK slot > 7 if MBK slot 7 is already occupied by another MBK) and the new MBK is imported into MBK slot 3.
Consider the difference between automatically imported MBKs and an autogenerated MBK. An automatically imported MBK is an MBK the **Automatic MBK Import** check box

has been selected for when the MBK has been created. An autogenerated MBK is an MBK with the name **AUTO-GEN** that has been generated by Utimaco IS GmbH in MBK slot 3 during the production of the device. There is no backup in keyfiles or on smartcards for an autogenerated MBK. To verify which MBK is in a certain MBK slot, click the **Info** tab.

Consider that it is important which MBK is in use in MBK slot 3 by the device because this MBK is used by the actions backing up a user or a database to protect the backup files that are generated by these actions.

It is important to note down which MBK has been used for these backup commands because for a successful restoring of these backup files at a later date it is necessary that the same MBK is in MBK slot 3. Otherwise, for example, after an MBK import or an MBK rollover, the backup files are inaccessible.

10. Click **Import**.

→ The **Master Backup Key (MBK): Share Import 1/<m>** dialog box opens.

11. In the **Master Backup Key (MBK): Share Import 1/<m>** dialog box, specify whether the MBK is to be imported from a smartcard or from a keyfile.

- **MBK from Smartcard**

- i. Select the **Smartcard Token** option.
- ii. Click **OK**.
- iii. Insert the smartcard.
- iv. Press the **OK** key on the PIN pad.
- v. Enter the PIN for the smartcard.
- vi. Press the **OK** key on the PIN pad.
- vii. In a separate CAT window, you now see that you have successfully imported the first MBK share. Click **OK** to continue.
- viii. Keep the **Smartcard Token** option selected and click **OK**.
- ix. Repeat the import process for all remaining MBK shares.
- x. In the next CAT window, you now see that you have successfully imported all required MBK shares. Click **OK**.
→ The window closes.

- **MBK from keyfile**

- i. Select the **Key file Token** option.

- ii. Click the search button next to the text field **Key Path** and double-click one of the previously generated MBK shares to select it. By default the MBK shares are keyfiles with the file extension * **.mks** .
 - iii. In case the MBK share keyfile is password-protected, enter the appropriate password into the **Password** text box.
 - iv. Click **OK**.
 - A separate CAT window confirms that the first MBK share was successfully imported.
 - v. Click **OK** to continue.
 - vi. Repeat the import process for all remaining MBK shares.
 - A separate CAT window confirms that all MBK shares were successfully imported.
 - vii. Click **OK**.
 - The window closes.
12. After you have imported the MBK, click **Close**.
 - The **Remote Master Backup Key (MBK) Management** dialog box closes.
13. We recommend regenerating backup files with the new MBK. Thus, you have additional backup files, this time made with the new MBK.



The MBK has been imported successfully into the CryptoServer.

5.6.3 Creating an MBK Backup

This section explains how to create a backup copy of your MBK with CAT.



You do not have to log in to the CryptoServer to create a backup of an MBK.

Prerequisites

- The smartcard holders of all n smartcards, containing all shares of the MBK must be present, keeping their MBK smartcards at hand. A smartcard holder is a person knowing the PIN for accessing the smartcard.
- The smartcard holders of all n smartcards required for creating backup copies of all shares of the MBK must be present, keeping their MBK smartcards at hand.
- The PIN pad must be connected to the computer where CAT is installed on.

Procedure

1. Start CAT.
2. Click **Manage MBK** in the toolbar.
→ The **Remote Master Backup Key (MBK) Management** dialog box opens.
3. Click the **Backup** tab.
4. Under **Source Token**, select whether the MBK backup is to be prepared from **Smartcards** or from a **Keyfile**. If you select the **Keyfile** option, you must enter/select the file location where the MBK share is stored and the filename. In case the MBK keyfile is protected with a password, you must enter the appropriate password into the **Password** text box and confirm it.
5. Under **Destination Token** select whether the backup is to be created on **Smartcards** or as a **Keyfile**. If you select the **Keyfile** option, you must enter/select the file location and the filename for the copy of the MBK share. Optionally, you can enter a password in the **Password** text box and confirm it if the MBK backup keyfile shall be additionally protected with a password.
6. Click **Backup** to confirm your selection for both source and destination tokens.
 - a. **Create a backup from an MBK smartcard to another smartcard**
 - i. Insert the source smartcard containing the first share of the MBK into the PIN pad and press **OK** on the PIN pad.
 - ii. Enter the PIN for the MBK smartcard and press **OK** on the PIN pad.
 - iii. Insert the first destination smartcard into the PIN pad and press **OK** on the PIN pad.
 - iv. Enter the PIN for the destination smartcard and press **OK** on the PIN pad.
→ A separate window appears to confirm the successful creation of the MBK share copy.



If the smartcard containing the copy of the MBK share is protected with the default PIN, change the PIN, see [Changing the PIN for MBK Key Shares on Smartcards \(p. 85\)](#).

- v. Repeat the backup process for all source MBK smartcards containing MBK shares.

b. Create a backup from an MBK smartcard to a protected keyfile:

- i. Insert the source smartcard containing the first share of the MBK into the PIN pad and press **OK** on the PIN pad.
- ii. Enter the PIN for the MBK smartcard and press **OK** on the PIN pad. A dialog box appears to warn you that if there are two different types of MBK – AES and DES stored on the smartcard – one keyfile copy will be created for each.
- iii. Confirm the warning by clicking **YES** to continue.
 - A separate window appears to confirm the successful creation of the MBK share copy.
- iv. Repeat the backup process for all source MBK smartcards containing MBK shares.

c. Create a backup from a protected keyfile to an MBK smartcard

- i. Insert the destination smartcard into the PIN pad and press **OK** on the PIN pad.
- ii. Enter the PIN for the smartcard and press **OK** on the PIN pad.
 - A separate window appears to confirm the successful creation of the MBK share copy.
- iii. Repeat the backup process for all MBK shares.



If the smartcard containing the copy of the MBK share is protected with the default PIN, change the PIN, see [Changing the PIN for MBK Key Shares on Smartcards \(p. 85\)](#).



The MBK backup has successfully been created.

5.6.4 Changing the PIN for MBK Key Shares on Smartcards

This section describes changing the PIN for Master Backup Key (MBK) shares stored on a smartcard.

Do not confuse this with changing the PIN for user authentication keys, which might be stored in parallel on the same smartcard. This is described in [Changing the PIN for User Authentication Keys on a Smartcard \(p. 55\)](#).



You do not have to log in to the CryptoServer to perform the steps described in this section.

Prerequisites

- Ensure that the delivered PIN pad is connected to the computer whereon CAT is installed.

Procedure

1. Start CAT.
2. Click **Manage MBK** in the toolbar.
→ The **Remote Master Backup Key (MBK) Management** dialog box opens. The **Backup** tab is shown by default.
3. Click the **MBK Change PIN** tab.
4. Click **Change PIN**.
5. Insert the smartcard the PIN of which you want to change into the PIN pad and press the **OK** key on the PIN pad.
6. Enter the old PIN for the smartcard and press the **OK** key on the PIN pad.
7. Enter the new PIN of at least six and a maximum of 12 digits for that smartcard and press the **OK** key on the PIN pad.
8. Confirm the new PIN by entering it once again and press the **OK** key on the PIN pad.

9. Change the PIN on every smartcard on which parts of the MBK are stored. You must do this separately for each individual card.



The PIN for the MBK shares on smartcards has been changed successfully.

5.6.5 Retrieving MBK Information



You do not have to log in to the CryptoServer to retrieve information about an MBK.

1. Start CAT.
2. Click **Manage MBK** in the toolbar.
 - The **Remote Master Backup Key (MBK) Management** dialog box opens.
3. Click the **Info** tab.
4. Under **MBKs stored in CryptoServer**, you see more information about the MBK.

The **Slot** column shows the MBK slot number. Supported values: 0...255 (SecurityServer/ CryptoServer SDK 4.20 or earlier: 0...3). The MBK slot number must not be confused with the PKCS#11 slot number.

The **Name** column shows the name of the MBK, or **<NoName>** if no key name is given. The name **AUTO-GEN** indicates an autogenerated MBK.
5. To view information about an MBK that is stored on a smartcard, click **Card Info** and follow the instructions on the PIN pad. All important information about an MBK that is stored on a smartcard is displayed under MBKs stored on Smartcard.
6. Click **Close**.
 - The **Remote Master Backup Key (MBK) Management** dialog box closes.



The MBK information has been retrieved successfully.

6 Monitoring the CryptoServer

6.1 Viewing the Status of the CryptoServer

To view the status of the CryptoServer, click **Show Status** in the CAT toolbar.

The system displays the CryptoServer's status in the CAT main window.

Example Output: Show Status

```
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
```

The following table describes the parameters of the **Show Status** output in more detail.

Parameter	Description
mode	<p>Operating mode of the CryptoServer:</p> <ul style="list-style-type: none"> Operational The regular set of firmware modules (*.msc) is started. All administration and cryptographic functions are available. Operational Mode – Administration-Only The regular set of firmware modules (*.msc) is started. All administration functions are available. All cryptographic functions are blocked. Maintenance Backup set of firmware modules (*.sys) is started (e.g., in alarm state) Bootloader The Bootloader is running. The operating system and the regular set of firmware modules have not been started yet.

Parameter	Description
state	<p>Current operating state of the CryptoServer (should be <code>INITIALIZED</code>):</p> <ul style="list-style-type: none"> ▪ MANUFACTURED This state is only relevant during production process. ▪ INITIALIZED Firmware modules and all system keys (Production Key, Module Signature Key, default Administrator Key <code>ADMIN.key</code> file) are loaded. ▪ DEFECT CryptoServer is defect. Contact the manufacturer, Utimaco IS GmbH.
temp	<p>Current temperature of the CryptoServer (in °C) For detailed information about the CryptoServer's behavior depending on its internal temperature, see <i>Temperature Monitoring</i> in the CryptoServer – Administration Manual (p. 106)</p>
alarm	<p>Current alarm status. It can be either <code>ON</code> or <code>OFF</code>. If <code>ON</code>, the following reasons are possible and shown in case of an alarm state:</p> <ul style="list-style-type: none"> ▪ Power is too low (empty battery) ▪ Power is too high ▪ Temperature too high (> 66°C) ▪ Temperature too low (< -13 °C) ▪ Outer foil is broken (CryptoServer CSe-Series only) ▪ Inner foil is broken (CryptoServer CSe-Series only) ▪ External Erase is executed (manually by a short-circuit of the corresponding pins on the PCIe card) ▪ Invalid/Corrupted Master Key ▪ Communication to sensor controller failed <p>In addition, it is shown if the alarm reason is still present or if it has been removed in the meantime, e.g. an empty battery has been replaced.</p>
bl_ver	Current bootloader version and the model type of the CryptoServer
hw_ver	Version of the hardware for the CryptoServer CSe-Series and CryptoServer Se-Series Gen2
uid	<p>The UID is a "Universal Identification" that uniquely identifies every CryptoServer PCIe card. It is stored on a hardware component and loaded onto the PCIe card during production. <code>UID</code> is an 8-byte binary data field. The UID is displayed when the status information is extracted. It is not stored on the CryptoServer.</p>

Parameter	Description
adm1	<p>adm1 is a readable character string, with a length of 16 characters. The first 8 characters of adm1 contain a short form of the CryptoServer's model type, filled with blank spaces CSe10, Se12, CSe100, Se52, Se500 or Se1500. The second 8 characters represent the unique serial number of the CryptoServer's PCIe card. This serial number is assigned by Utimaco IS GmbH during manufacture and then loaded into the CryptoServer. In case of a real hardware CryptoServer PCIe card, the serial number starts with the letters CS, followed by a 6-digit number. The adm1 character string is displayed when the status information is selected. The 8-character serial number CSxxxxxx is also stored on the CryptoServer PCIe card. In case of the CryptoServer Simulator, the serial number has the format SI<xxxxxx>. SI stands for "simulator" and <xxxxxx> stands for the port number the simulator is listening on, i.e., 003001 for the first simulator instance, 003003 for the second simulator instance etc. Example: SI003001. In case of the PaymentServer Simulator, the serial number is always CS000000.</p>
adm2	<p>adm2 is a readable 16-character string. The contents of the adm2 character string is also assigned by Utimaco IS GmbH and loaded onto the CryptoServer during production. Whilst the CryptoServer is being manufactured, the name of the firmware module package loaded for the customer is also recorded here, according to which CryptoServer model series is being produced. The adm2 character string is displayed when you select the status information. It is not stored on the CryptoServer. This field may be empty.</p>
adm3	<p>adm3 is a readable 16-character string. During production, a default value is recorded here, according to which CryptoServer model is being manufactured. For an CryptoServer CSe-Series and Se-Series Gen2, the INSTALLED value is recorded here.</p>
error state	<p>Error code indicating that a power-on self-test has failed. If these tests succeed, nothing is shown</p>

Table 7: CryptoServer status information

The bit representation of the state field has the following meaning.

Bit(s)		Value	Description
	Device state		
0 ... 6		1	DEFECT
		2	MANUFACTURED
		4	INITIALIZED
		5	OPERATIONAL
	Alarm		
7		0	OFF
		1	ON

Bit(s)		Value	Description
	Sensor		
8		0	The temperature is too low.
		1	No temperature low alarm has been registered.
9		0	The temperature is too high.
		1	No temperature high alarm has been registered.
10 This is only possible for CSe-Series.		0	The inner foil has been broken.
		1	No inner foil alarm has been registered.
11 This is only possible for CSe-Series.		0	The outer foil has been broken.
		1	No outer foil alarm has been registered.
12		-	This bit is not used any more.
13		0	The power is too high (power overdrive).
		1	No power high alarm has been registered.
14		0	The power is too low.
		1	No power low alarm has been registered.
15		0	The external erase has been executed.
		1	No external erase alarm has been registered.
16		0	No alarm is present.
		1	An alarm is still present.
17		0	No alarm has occurred.
		1	An alarm has occurred.
	FIPS140 mode		
18		0	FIPS mode OFF
		1	Some FIPS mode (restricted (CryptoServer Se-Series only) or validated, see bit 26 below)
	Boot mode		
19 ... 20		0	The boot loader is started (not possible here).
		1	*.sys modules are started.
		2	*.msc modules are started.
	...		
	FIPS140 (2)		
26 This bit is only relevant if bit 18 has been set		0	FIPS mode = ON
		1	FIPS Mode = OFF but FIPS restrictions are applied (CryptoServer Se only)
	Administration-only mode		

Bit(s)		Value	Description
27		0	Administration-Only Mode = OFF
		1	Administration-Only Mode = ON

6.2 Viewing the Battery State of the CryptoServer

Viewing the state of the Carrier Battery

The status of the carrier battery on a CryptoServer PCIe card is always displayed in the lower right-hand corner of the CAT main window.



If the status **LOW** is displayed for the carrier battery, this means that the carrier battery is in a critical state and shall be replaced by a new one as soon as possible. Otherwise, it may happen that the supply of power can no longer be guaranteed. This may trigger an alarm that then deletes all sensitive data from the CryptoServer. Instructions on how to replace the carrier battery can be found in the corresponding operating manual provided on the product CD in the `Documentation\Operating Manuals` directory.

Viewing the state of the External Battery

Click the **Show** menu and select **Battery State**. When the external battery of a CryptoServer LAN reaches a critically low power level, it must be replaced as described in the corresponding CryptoServer LAN Operating Manual.



For details about the exact voltage threshold values, see *Power Supply Monitoring* in the *CryptoServer - Administration Manual* (p. 106).

6.3 Viewing Driver Information

The driver information of the CryptoServer can be displayed and is especially useful in case the CryptoServer suddenly stops reacting to any commands and the support needs to be contacted. Have this information at hand if you then need to contact our support team.

The driver information includes details about the CryptoServer driver, the slot number and more information, which can only be interpreted by the manufacturer Utimaco IS GmbH.

To display the driver information, click the **Show** menu and select **Driver Info**.

The driver information of the CryptoServer can be displayed and is especially useful in case the CryptoServer suddenly stops reacting to any commands and the support needs to be contacted.

The driver information includes details about the CryptoServer driver, the slot number and more information, which can only be interpreted by the manufacturer Utimaco IS GmbH.

To display the driver information, click the **Show** menu and select **Driver Info**.

6.4 Listing the Firmware

In the CAT main window, click **Show Firmware** in the toolbar to display all firmware modules that have been loaded into the CryptoServer.

The following tables show output examples. The output examples may differ from the output on your CryptoServer with respect to the listed firmware modules and/or their versions depending on the installed firmware package and its version.

For CryptoServer 4.45 and later, the following applies:

The implementation of cryptographic primitives has been optimized for, and harmonized across, Utimaco's HSM platforms and host components, resulting in a general performance increase of cryptographic operations. The exact improvements depend on algorithm, key size, size of data to be encrypted/signed, and HSM model. The improvements are highest for short-running operations like AES encryption of small blocks of data. This new common cryptographic library is delivered as CRYPT firmware module. In a firmware package, this CRYPT firmware module replaces the following modules that were previously handled as separate modules: AES, HASH, DSA, VRSA, LNA, ECDSA, ECA, POST and ASN.1. The modules AES, HASH, etc. appear as active firmware modules in addition to the new CRYPT module when calling the `csadm ListFirmware` command.

Example output for CryptoServer 4.45 and later:

<i>ID number (hexadecimal)</i>	<i>Module name</i>	<i>Version number</i>	<i>Initialization Status</i>
0	SMOS	5.6.4.1	INIT_OK
4	POST	2.2.1.0	INIT_OK
68	CXI	2.4.11.1	INIT_OK
81	VDES	2.2.1.0	INIT_OK
82	PP	1.4.1.2	INIT_OK

<i>ID number (hexadecimal)</i>	<i>Module name</i>	<i>Version number</i>	<i>Initialization Status</i>
83	CMDS	3.8.4.1	INIT_OK
84	VRSA	2.2.1.0	INIT_OK
85	SC	1.2.0.7	INIT_OK
86	UTIL	3.0.7.1	INIT_OK
87	ADM	3.1.2.0	INIT_OK
88	DB	2.0.0.2	INIT_OK
89	HASH	2.2.1.0	INIT_OK
8a	STUN	0.0.0.1	INIT_OK
8b	AES	2.2.1.0	INIT_OK
8d	DSA	2.2.1.0	INIT_OK
8e	LNA	2.2.1.0	INIT_OK
8f	ECA	2.2.1.0	INIT_OK
91	ASN1	2.2.1.0	INIT_OK
96	MBK	2.5.1.1	INIT_OK
9a	NTP	1.2.1.1	INIT_OK
9c	ECDSA	2.2.1.0	INIT_OK
9f	CRYPT	2.2.1.0	INIT_OK

Table 8: Example for how firmware information is displayed in CAT

Example output for CryptoServer earlier than 4.45:

<i>ID number (hexadecimal)</i>	<i>Module name</i>	<i>Version number</i>	<i>Initialization Status</i>
0	SMOS	5.3.3.0	INIT_OK
68	CXI	2.1.9.2	INIT_OK
81	VDES	1.0.9.1	INIT_OK

ID number (hexadecimal)	Module name	Version number	Initialization Status
82	PP	1.2.5.0	INIT_OK
83	CMDS	3.4.0.0	INIT_OK
84	VRSA	1.3.0.6	INIT_OK
85	SC	1.2.0.2	INIT_OK
86	UTIL	3.0.3.0	INIT_OK
87	ADM	3.9.16.0	INIT_OK
88	DB	1.3.1.1	INIT_OK
89	HASH	1.0.9.0	INIT_OK
8b	AES	1.3.5.1	INIT_OK
8d	DSA	1.2.2.1	INIT_OK
8e	LNA	1.2.3.0	INIT_OK
8f	ECA	1.1.7.3	INIT_OK
91	ASN1	1.0.3.4	INIT_OK
96	MBK	2.2.4.4	INIT_OK
9c	ECDSA	1.1.8.5	INIT_OK

Table 9: Example for how firmware information is displayed in CAT

The firmware module's initialization states have the following meanings:

- **INIT_OK**

The firmware module has been installed successfully and is ready for use.

- **INIT_FAILED**

An error occurred when the firmware module started.

- **INIT_INACTIVE**

This message is output for the HCE firmware module if the CryptoServer does not have a cryptographic accelerator chip. This is the situation for all CryptoServer models excluding Se500 and Se1500, see *Cryptographic Accelerator Chip* and *Firmware Modules* in

the [CryptoServer - Administration Manual](#) (p. 106). For CryptoServer Se500 and Se1500 that have a cryptographic accelerator chip, the `INIT_OK` status is output for the HCE firmware module.

- **INIT_INTERNAL**

This status is usually only displayed during the temporary boot phase and means that the firmware module is initialized internally.

- **INIT_DEP_OK**

This status is usually only displayed during the temporary boot phase and means that all dependencies to other modules have been successfully removed.

- **INIT_SUSPENDED**

This status is displayed if the previous operation (for example, Clear) requires a CryptoServer restart.

If you encounter a problem with one of the firmware modules, which means its initialization status is not `INIT_OK`, make a note of all entries shown in the above table. Then contact Utimaco's customer support, and pass on these details to enable us to identify this module.

6.5 Listing All Files

In the CAT main window, click **Show Files** in the toolbar to display all files resident on the CryptoServer's flash memory (RAM).

All loaded firmware modules (`*.msc`), databases (`*.db`), logfiles (`*.log`) and license files (`*.slf`) can be displayed.

If the signed configuration file `cmds.scf` is used, for example to harden your CryptoServer interfaces or to increase the required permissions for the authentication of specific CryptoServer functions/commands, it also will be listed here. More detailed information about using the `cmds.scf` is provided in *Configurable Role-based Access Control (C-RBAC)* and *Interface Hardening by Disabling Selected Functions* in the [CryptoServer - Administration Manual](#). (p. 106)

7 Maintaining the CryptoServer

This chapter describes the general tasks and maintenance tasks performed on a CryptoServer.

7.1 Installing/Updating the Firmware

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 02000000, see [Logging in a User \(p. 27\)](#).
4. Click the **Manage** menu.
5. Select **Firmware**.
→ The **Setup CryptoServer** dialog box opens. The series of your CryptoServer is shown in the upper part of the **Setup CryptoServer** dialog box in the **Model** text box.
6. Select the appropriate license file in the **License File** text box.
After the installation of the product CD, you find the license files on your computer in the directory `C:\Program Files\Utimaco\SecurityServer\Administration`.



If you have a CryptoServer with a SecurityServer firmware version 3.10 and later, and a firmware module ADM version 3.0.8.0 or later you do not need to import any license file during a setup (firmware package import).

The names of the license files must match the names of the CryptoServer series. Therefore, if e.g. a CryptoServer CSe-Series is used, the appropriate license file for the CSe-Series must be selected according to the following table.

CryptoServer Series	CryptoServer Model	License File
CSe-Series	CSe10	No license file required
CSe-Series	CSe100	<code>cse100.s1f</code>
Se-Series Gen2	Se12	No license file required

CryptoServer Series	CryptoServer Model	License File
Se-Series Gen2	Se52	se52.slf
Se-Series Gen2	Se500	se500.slf
Se-Series Gen2	Se1500	se1500.slf

Table 10: CryptoServer models and the corresponding license files

7. Select the required SecurityServer package file in the **Firmware Package** text box. After the installation of the product CD, you find the SecurityServer packages in the directory `C:\Program Files\Utimaco\SecurityServer\Firmware`. Utimaco IS GmbH provides for each CryptoServer series the SecurityServer package as shown in the following table:

CryptoServer series	SecurityServer packages
CryptoServer CSe-Series	SecurityServer-CSe-Series-x.xx.x.mpkg
CryptoServer Se-Series Gen2	SecurityServer-Se2-Series-x.xx.x.mpkg

Table 11: CryptoServer firmware packages

8. Choose the installation option according to your situation:
New Installation (deletes all files; installs new firmware package)
Update (installs only new firmware)
9. Click **Setup**.
10. Click **Yes**.



The CryptoServer Firmware has been updated successfully. A separate window with a confirmation message is shown.



After the SecurityServer package has been updated, the CryptoServer performs a restart which automatically logs off all users.

7.2 Resetting an Alarm

Every alarm triggered on the CryptoServer must be reset by an administrator. This ensures the alarm will not go unnoticed and also that it will be investigated.

Before an alarm is reset, the source of the alarm should be found. If the alarm is a temporary alarm triggered, e.g. because the main power supply is too low or because the internal temperature is either too high or too low, the cause of the alarm must be resolved before resetting it. If the cause is not resolved, the CryptoServer will return to Maintenance Mode after it is restarted. The CryptoServer will only go into Operational Mode after a restart if you have removed the cause for the alarm.

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
→ The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with an authentication status of at least 20000000 or 02000000, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
→ The **Login/Logoff User** dialog box closes.
5. Click the **Manage** menu.
6. Select **Reset Alarm**.
→ A new message window informs you whether the alarm has been reset successfully. The CryptoServer then performs a restart. This logs off any user who is currently logged in to the device. Therefore, every user must log in again to continue working with the CryptoServer.



If you cannot reset the alarm, contact the manufacturer Utimaco IS GmbH.

7.3 Clearing the CryptoServer

Prerequisites

Before the CryptoServer can be reset to factory settings, an External Erase must be performed directly on the CryptoServer PCIe card or on the CryptoServer LAN, see [Performing an External Erase \(p. 102\)](#). The External Erase triggers an alarm on the

CryptoServer which allows the Clear CryptoServer to Factory Settings command to be executed for as long as this alarm is active.

Consequences of Clearing the CryptoServer

When a **Clear** is performed, it deletes all sensitive data and firmware modules stored on the CryptoServer. The following actions take place:

- The following sensitive data is deleted:
 - Master Key. The deletion and regeneration of the Master Key automatically makes all other keys (including the Master Backup Key) and sensitive data stored on the device unusable because they can no longer be decrypted without the "old" Master Key.
 - HSM Authentication Key (`authkey.db`), if available
 - Firmware Encryption Key, if available
 - The audit log signature key (`auditkey.db`), if available
 - Master Backup Key (MBK), if available
 - All firmware modules (`*.msc` files) except for the bootloader code and the system firmware modules (`*.sys` files)
 - Signed configuration file (`cmds.scf`), if available
 - All users in the user database (`user.db`) using the HMAC password authentication mechanism
- The following items are not deleted:
 - Public parts of the Production Key, Default Administrator Key, Module Signature Key and Alternative Module Signature Key
 - Bootloader code and system firmware modules (`*.sys`)
 - Alarm state file (`alarm.sens`)
 - Audit log file(s) (`audit*.log`)
 - Audit log configuration file (`audit.cfg`)
 - Any Signed License File (`*.slf`), if present
 - Bootloader configuration file (`bl.cfg`)
 - All users in the user database (`user.db`) using a public key authentication mechanism, e.g., RSA signature authentication, RSA smartcard authentication or ECDSA signature authentication

- A second copy of the public part of the Default Administrator Key (`init.key` file). This copy can neither be changed nor deleted, but it is used to restore the default administrator user ADMIN with his Default Administrator Key as an authentication token (using the `csadm Clear = DEFAULT` (ClearFactoryDefaults) command or CAT > **Manage** > **Clear to Factory Settings**).

Consider that the above list differs from the items that are deleted due to an alarm.

When a **Clear to Factory Settings** is performed, it resets the CryptoServer back to delivery conditions. The following actions take place:

- All items that are deleted by a **Clear** are deleted by a **Clear to Factory Settings** as well.
- All users on the CryptoServer user database (`user.db`) are deleted.
- The default administrator ADMIN is set up again and can use the original user authentication key `ADMIN.key` to log in to the CryptoServer.

7.3.1 Performing a Clear



When performing a clear, be aware of the consequences described in [Clearing the CryptoServer \(p. 98\)](#).

1. Start CAT.
2. Click **Login/Logoff** in the toolbar.
 - The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with at least authentication status 02000000, e. g., as the default ADMIN user, see [Logging in a User \(p. 27\)](#).
4. Click **Close**.
 - The **Login/Logoff User** dialog box closes.
5. Click the **Manage** menu.
6. Select **Clear**.

7. Confirm the confirmation prompt with **Yes**.



The CryptoServer has been cleared successfully. A separate window with a confirmation message appears.

The CryptoServer then performs a restart and goes into Maintenance Mode.

This logs off any user who is currently logged in to the device. Therefore, every user must log in again to continue working with the CryptoServer.

To re-create all features of the CryptoServer (Operational Mode), the CryptoServer must be set up again and the firmware modules of the SecurityServer package must be reloaded, see [Setting up the CryptoServer after a Clear/Clear to Factory Settings \(p. 102\)](#).

The CryptoServer does not return to Operational Mode until the firmware modules of the SecurityServer package are reloaded.

7.3.2 Performing a Clear to Factory Settings



When performing a clear to factory settings, be aware of the consequences described in [Clearing the CryptoServer \(p. 98\)](#).

An External Erase must be performed before clearing the CryptoServer as described in [Performing an External Erase \(p. 102\)](#).

1. Start CAT.
2. Click the **Manage** menu.
3. Select **Clear to Factory Settings** that has been activated by the External Erase.
4. Click **YES**.
 - A separate window informs you whether the Clear to Factory Settings command was executed successfully.
5. Click **OK** to close this window.
 - The CryptoServer restarts and goes into Maintenance Mode.
6. Log in to the CryptoServer again, see [Logging in a User \(p. 27\)](#).

7. Reset the alarm that has been activated by the previously performed External Erase, see [Resetting an Alarm \(p. 98\)](#).



The CryptoServer has been cleared to factory settings. It can now be set up again, see [Setting up the CryptoServer after a Clear/Clear to Factory Settings \(p. 102\)](#).

7.3.3 Performing an External Erase

An External Erase can only be performed on the CryptoServer PCIe card during normal operation when the host computer is running. This is the only way to ensure the CryptoServer is supplied with enough power to perform the External Erase. Note that the different CryptoServer series – CryptoServer CS, CSe, Se and Se Gen2 - have different designs.

For details on how to perform an External Erase on the CryptoServer LAN, see *Performing an External Erase* in the [CryptoServer LAN – Administration Manual \(p. 106\)](#).

For details on how to perform an External Erase on the CryptoServer PCIe card, see *External Erase* in the [CryptoServer - Administration Manual \(p. 106\)](#).

7.4 Setting up the CryptoServer after a Clear/Clear to Factory Settings

This section describes how to set up a CryptoServer again after a Clear or Clear to Factory Settings command has been executed.

1. Import the relevant license file and the appropriate firmware package (`SecurityServer-<Series>-<version>.mpkg`) into your CryptoServer as described in [Installing/Updating the Firmware \(p. 96\)](#).
2. Generate an MBK, see [Generating an MBK \(p. 75\)](#) splitting the MBK into several key shares and storing these key shares on smartcards.
3. Import the MBK into the CryptoServer, see [Importing an MBK \(p. 79\)](#) unless already done using the **Automatic MBK Import** option when generating the MBK.



The CryptoServer is fully operational again after a Clear or Clear to Factory Settings has been performed.

7.5 Preparing Diagnostic Information

If a problem occurs while the CryptoServer is running, you can call a range of status information that may help you sort out the problem.

To view the most important status information, perform the following steps:

1. Start CAT.
2. Click the **Show** menu.
3. Select **Diagnostics**.
 - The **Save Diagnostics** dialog box opens. The following diagnostic information is displayed:
 - The current date and time on the host computer when the diagnostics query was sent to the CryptoServer.
 - The CAT version
 - The address of the CryptoServer or the IP address of the CryptoServer LAN
 - The CryptoServer status
 - The boot log
 - Driver information (GetInfo)
 - The battery state of the carrier battery and the external battery
 - All files currently present on the CryptoServer
 - All active firmware modules on the CryptoServer
 - All users set up on the CryptoServer
 - Date and time on the CryptoServer
 - The alarm log (only displayed if bootloader version ≤ 2.5 is loaded on the CryptoServer)
 - Information about the Master Backup Key that is saved on the CryptoServer
4. Click **Save**.
 - A dialogue box opens to determine the file location.

5. Select the location, e.g., on your computer, for saving the file and enter an appropriate file name.
6. Click **Save** to save the `.txt` file.
7. Click **Cancel**.
 - The **Save Diagnostics** dialog box closes.
8. Click the **Show** menu.
9. Select **Audit Log**.
 - The **CryptoServer Audit Log** dialog box opens.
 - You can filter the display containing the log entries by users and by commands.
10. Click **Save Log**.
 - A dialogue box opens to determine the file location.
11. Select the location, e.g., on your computer, for saving the audit log and enter an appropriate file name.
12. Click **Save** to save the `.log` file.
13. Click **Close** to close the **CryptoServer Audit Log** dialog box



The diagnostic information has been retrieved and saved successfully and can be sent to Utimaco for further analysis.



To change the audit log configuration for showing more detailed logging information than provided by default, you must log in to the CryptoServer with at least authentication status 22000000, click the **Manage** menu and select **Audit Log Settings**.

8 Contact Address for Support Queries

If an error occurs that you cannot resolve with the help of the chapter *Troubleshooting* in the [CryptoServer - Administration Manual \(p. 106\)](#), you can contact us.

Please prepare diagnostic information, see [Preparing Diagnostic Information \(p. 103\)](#).

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.com¹
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.

¹ <mailto:support@utimaco.com>

9 References

<i>Title/Company</i>	<i>Document Number</i>
CryptoServer - Administration Manual / Utimaco IS GmbH	M010-0001-en
CryptoServer - csadm Manual / Utimaco IS GmbH	2009-0003
CryptoServer LAN - Quick Start Guide / Utimaco IS GmbH	M014-0001-en
CryptoServer LAN V5 – Administration Manual / Utimaco IS GmbH	2018-0010