CryptoServer

Manual for System Administrators

utimaco®

Imprint

Copyright 2017	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	+49 (0)241 / 1696-200
Fax	+49 (0)241 / 1696-199
Internet	http://hsm.utimaco.com
e-mail	hsm@utimaco.com
Document Version	2.5.5
Date	2017-02-15
Status	Final
Document No.	M010-0001-en

Table of Contents

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.

1.1 About this Manual

This manual provides information about the CryptoServer functions and contains solution-oriented information about how to use the CryptoServer Administration Tool (CAT) to set up, manage and maintain the CryptoServer/CryptoServer LAN all series.

1.1.1 Target Audience for this Manual

This manual is primarily intended for administrators who use the CryptoServer administration tool (CAT) to administer the CryptoServer or CryptoServer LAN all series.

1.1.2 Contents of this Manual

After the introduction, this manual is divided up into two main areas:

Functional description

This part of the manual, which runs in chapters 2 and 3, gives you all the important information about the CryptoServer functions you require in order to operate it correctly and effectively.

Operating instructions

This part of the manual, which covers chapters 4 and 5, provides solution-oriented information about how to use the CAT to set up, manage and maintain the CryptoServer.

1.1.3 Document Conventions

We use the following conventions in this manual:

Convention	*Usage*	*Example*
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	Filenames, folder and directory names, commands, file outputs, programming code samples	You will find the file `example.conf` in the `/exmp/demo/` directory.

Convention	*Usage*	*Example*
Italic	References and important terms	See Chapter 3, "Sample Chapter" in the *CryptoServer LAN/CryptoServer CryptoServer Command-line Administration Tool -csadm -Manual for System Administrators*.

Table 1: Document conventions

We have used icons to highlight the most important notes and information.

Here you find important safety information that should be followed.

Here you find additional notes or supplementary information.

1.1.4 Abbreviations

We use the following abbreviation in this manual:

Abbreviation	*Meaning*
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CAT	CryptoServer administration tool
CNG	Cryptography API: Next Generation
CSP	Cryptographic Service Provider
CXI	Cryptographic eXtended Interface
csadm	CryptoServer command-line administration tool

Abbreviation	*Meaning*
DES	Data Encryption Standard
DRBG	deterministic random bit generator
DRNG	deterministic random number generator
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve DSA
EKM	Extensible Key Management
FIPS	Federal Information Processing Standard
HSM	hardware security module
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
MAC	message authentication code
MBK	Master Backup Key
NTP	Network Time Protocol
P11CAT	PKCS#11 CryptoServer Administration Tool
PCIe	PCI Express Interface
PRNG	pseudo-random number generator
RSA	Rivest, Shamir, Adleman (cryptosystem)
TRNG	true-random number generator

Table 2: List of Abbreviations

1.2 Other Manuals

The CryptoServer is supplied as a PCI Express (PCIe) plug-in card in the following series:

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

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

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

We provide the following manuals on the product CD for the CryptoServer PCIe plug-in cards CSe, Se and Se Gen2 and for the CryptoServer LAN (appliance) CSe, Se and Se Gen2.

Quick Start Guides

You will find these Manuals in the main folder of the SecurityServer product CD. They are available only in English, do not cover all possible scenarios, and are intended as a supplement to the product documentation provided on the SecurityServer product CD.

- *CryptoServer LAN - Quick Start Guide*
  If you are looking for step-by-step instructions on how to bring the CryptoServer LAN into service, how to prepare a computer (Windows 7) for the CryptoServer administration and how to start administrating your CryptoServer with the Java-based GUI CryptoServer Administration Tool (CAT), read this document.
- *CryptoServer PCIe - Quick Start Guide*
  If you are looking for step-by-step instructions on how to bring the CryptoServer PCIe plug-in card into service, how to install the CryptoServer driver on a computer with minimal RHEL 7.0 installation and how to start administrating your CryptoServer with the CryptoServer Command-line Administration Tool (csadm), read this document.

Manuals for System Administrators

You will find these manuals on the product CD in the following folder:
`…Documentation\Administration Guides\`

- *CryptoServer - Manual for System Administrators*
  If you need to administer a CryptoServer PCIe plug-in card or a CryptoServer LAN using the CryptoServer Administration Tool (CAT), read this manual. Furthermore, this manual provides a detailed description of the CryptoServer functions, required for the correct and effective operation of the product.
- *CryptoServer LAN - Manual for System Administrators*
  If you need to administer a CryptoServer LAN (appliance), read this manual. Since a CryptoServer plug-in card is integrated into the CryptoServer LAN, read the *CryptoServer - Manual for System Administrators*, as well.
- *CryptoServer LAN/CryptoServer - Troubleshooting*
  If problems occur while you are using a CryptoServer PCIe plug-in card or a CryptoServer LAN (appliance), read this manual.

- *CryptoServer LAN/CryptoServer*
  PKCS#11 CryptoServer Administration Tool – Manual for System Administrators
  If you need to administer the PKCS#11 R2 interface with the PKCS#11 CryptoServer Administration Tool (P11CAT), read this manual.
- *CryptoServer LAN/CryptoServer*
  CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators
  If you need to administer a CryptoServer PCIe plug-in card or a CryptoServer LAN using the CryptoServer Command-line Administration Tool (csadm), read this manual.

Operating Manuals

You will find these manuals on the product CD in the following folder: `…Documentation\Operating Manuals\`. They contain all the necessary information for using the hardware of the CryptoServer PCIe plug-in card respectively the CryptoServer LAN (appliance).

2 CryptoServer Overview

The CryptoServer, created by Utimaco, is a hardware security module (HSM) that was developed specifically to ensure the efficient and secure performance of the following cryptographic operations:

- Generate key
- Save the key securely
- Generate random numbers (hardware (true) and software (pseudo) random number generator)
- Generate and verify signatures
- Encrypt and decrypt data
- Calculate hash values

CryptoServer protects all the cryptographic operations or keys you use against any form of attack. To do so, it uses technical software solutions, and also shields against physical attacks. The CryptoServer therefore guarantees the trustworthiness and integrity of data within your IT systems.

There are three series of Utimaco's CryptoServer. They provide the same basic functionality but have different types of physical security:

- The *CryptoServer CSe* is designed to meet the most stringent requirements of physical security, as required, for example, by the banking and government authority sectors. Its highly-developed sensors can identify a multitude of mechanical, chemical and physical attacks and actively delete sensitive keys and data from the CryptoServer's internal memory before they can fall into the wrong hands. These mechanisms comply with the FIPS 140-2 Level 4 physical security level.
- The *CryptoServer Se* is designed to fulfill typical security requirements in a commercial environment. The physical external enclosure of the hardware security module guarantees that any unauthorized attempts to access the sensitive keys and data held in the CryptoServer's memory will be repelled. These mechanisms comply with the FIPS 140-2 Level 3 physical security level. The CryptoServer Se-Series may be delivered with a crypto accelerator chip which provides highest performance for RSA operations.
- The *CryptoServer Se Gen2* is the successor for the CryptoServer Se-Series. It fulfills the same security requirements as the CryptoServer Se-Series, and is designed to comply with the FIPS 140-2 Level 3 physical security level. The CryptoServer Se-Series Gen2 may be delivered with a crypto accelerator chip which provides highest performance for RSA and ECC operations.

All CryptoServer series are available in two variants:

- CryptoServer as a plug-in card with a PCIe bus.
  This is referred to below as the CryptoServer or CryptoServer PCIe.
- CryptoServer LAN as a network component (appliance) which can be easily integrated into a network and wherein a CryptoServer PCIe is integrated.
  This is referred to below as the CryptoServer LAN.

Throughout this manual, the term CryptoServer is used to refer to all series and all variants of the CryptoServer.
However, the products are named explicitly when the functionalities of the CryptoServer series differ.

2.1 Administration of the CryptoServer

You can administer the CryptoServer in a number of ways, each of which is introduced briefly in the sections that follow.

2.1.1 The CryptoServer Administration Tool (CAT)

The CryptoServer administration tool is a Java application used to administer CryptoServer plug-in cards as well as CryptoServer LANs. Use the CAT to handle all the typical administration tasks involved in bringing the CryptoServer into operation, monitoring its status and managing the users, firmware and keys.

CAT versions 2.1.0.0 and later do not support administration of the CryptoServer CS-Series (CS2000 and CS Classic). Use the CAT version 2.1.0.0 or earlier to administer those CryptoServer series.

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 host computer, whereon CAT shall be installed, are listed in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` provided on the SecurityServer/CryptoServer SDK product CD in the folder `…\Documentation\Product Details`.

The CAT runs in the following Java runtime environments (JRE):

- Oracle JRE 1.7

- IBM JRE

2.1.2 CryptoServer Command-line Administration Tool (csadm)

The CryptoServer command-line tool csadm is a program that can be called from either a command line or a batch file. You can use csadm to administer both CryptoServer PCIe cards and CryptoServer LANs. With csadm you can handle all the typical administration tasks as mentioned above for CAT, as well as perform additional advanced administration functions primarily of interest for customers who want to extend the standard functionality of the CryptoServer with self-developed firmware modules providing specific cryptographic functions and commands.

All operating systems that are currently supported for the host computer, whereon csadm shall be installed, are listed in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` provided on the SecurityServer/CryptoServer SDK product CD in the folder `…\Documentation\Product Details`.

2.1.3 Menu Options on the CryptoServer LAN

On the front side of the CryptoServer LAN you will see a display and a number of control keys. You can use this display and the control keys to access the menu options needed to perform the most important administration functions. They include commissioning and status monitoring, as well as a limited range of functions for managing firmware and keys. However, you cannot use these menu options to manage user data.

With the menu options on the front side of the CryptoServer LAN you can administer both the CryptoServer LAN and the CryptoServer plug-in card installed within the CryptoServer LAN.

2.2 Smartcards, PIN Pads and Keyfiles

Smartcards, PIN pads and keyfiles are used to administer the CryptoServer.

2.2.1 Smartcards

The smartcards that can be used with the CryptoServer are supplied exclusively by Utimaco IS GmbH. You cannot use any other smartcards for the administration of the CryptoServer. The smartcards are preconfigured by Utimaco before they are shipped.

The CryptoServer LAN is supplied along with ten smartcards.
However, if you purchase a CryptoServer PCIe, smartcards are not included in the deliverables.

Each one of these smartcards is already preloaded with an authentication key for the default administrator ADMIN.

The smartcards are PIN protected. If you enter the incorrect PIN three consecutive times, the smartcard is blocked and can no longer be used. If this happens you must order a new smartcard from Utimaco IS GmbH.

2.2.2 PIN Pads

The PIN pads are smartcard readers to be used with the CryptoServer which have an integrated display and a keypad, and are also supplied exclusively by Utimaco IS GmbH. You cannot use any other PIN pads for the CryptoServer.

The CryptoServer LAN is supplied along with a PIN pad.
However, if you purchase a CryptoServer PCIe, a PIN pad is not included in the deliverables.

Prior to SecurityServer 4.10 the REINERSCT cyberJack PIN pad has been supplied as shown in the following figure:

Figure 1: REINERSCT cyberJack

Additionally, as from SecurityServer 4.10 a new PIN pad of type Utimaco cyberJack One has been introduced.

Figure 2: Utimaco cyberJack One

Both PIN pads provide the same functionality and can be used with the smartcards delivered by Utimaco.

Note that as of SecurityServer 4.10, the CryptoServer LAN is supplied either with the REINERSCT cyberJack or with the Utimaco cyberJack One. To use these PIN pads on a Windows host computer, the appropriate USB PIN pad driver shall be installed as described in chapter 3.3.5. For using the PIN pads on a Linux host computer, the udev rule provided in chapter 3.4.6 must be defined.

2.2.3 Keyfiles

After the installation of the CryptoServer host software from the product CD, the authentication keyfile `ADMIN.key` for the default administrator ADMIN is also stored on the host computer you are going to use for the CryptoServer administration.

Keyfiles can be used either with or without password protection. However, we strongly recommend you always use a password to protect your keyfiles.

2.3 Implementation Environment with a CryptoServer PCIe

A description of a simplified system, with a CryptoServer PCIe that is ready for use, is given below:

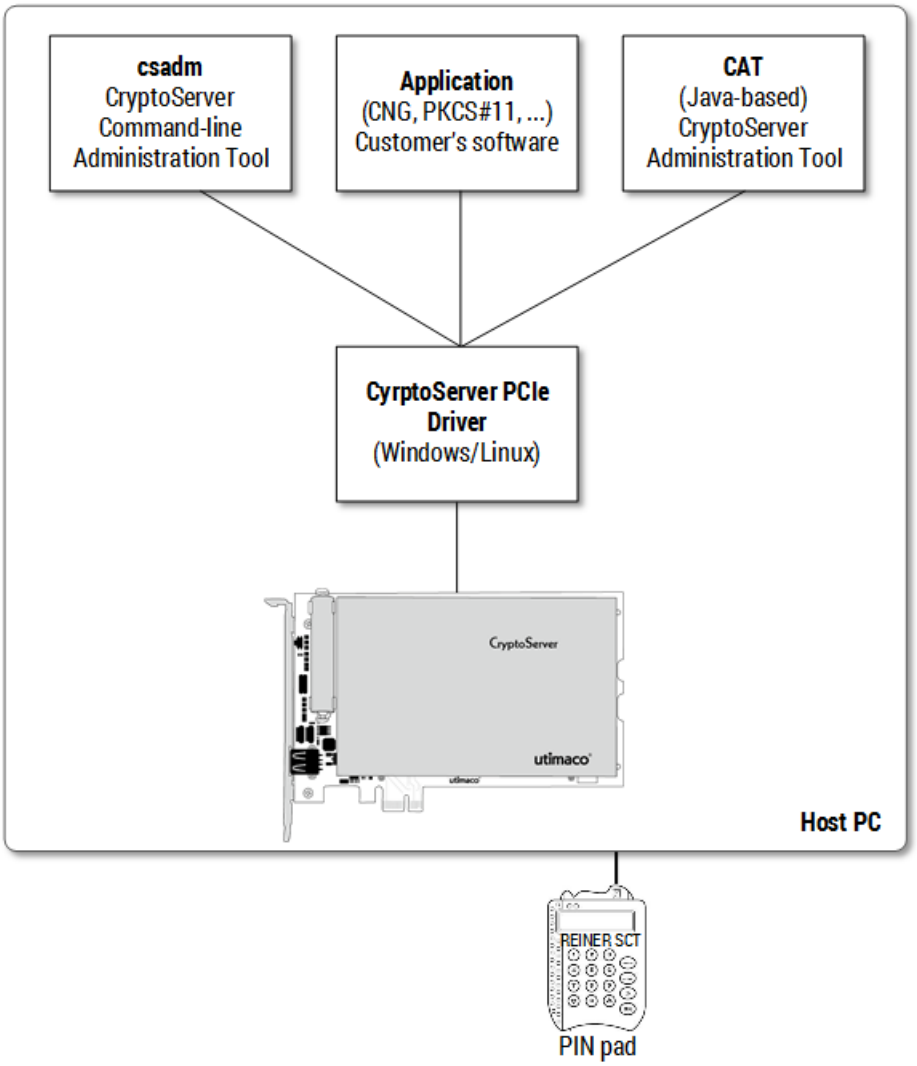


Figure 3: Example for a system with integrated CryptoServer CSe PCIe plug-in card

The CryptoServer PCIe has been installed on a host computer that is running either a Windows or Linux operating system. To enable the operating system of the host computer to communicate with the CryptoServer, the CryptoServer driver for the corresponding operating system, provided on the SecurityServer/CryptoServer SDK product CD, has also been installed on the host computer. If necessary, you can run more than one CryptoServer PCIe in the same host computer. The CryptoServer itself is administered with the administration tools installed on the host computer and also provided on the SecurityServer/CryptoServer SDK product CD.

You find the list of all currently supported operating systems for the host computer in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` on the

SecurityServer/CryptoServer SDK product CD in the folder …\Documentation\Product Details.

Most of the commands used to administer the CryptoServer must be authenticated by users with appropriate permissions. The user can use a keyfile, a passwords or a smartcard as an authentication token. However, the smartcards and the PIN pad serving as a card reader are not included in the CryptoServer PCIe deliverables and must be acquired separately from the manufacturer Utimaco. If you want to use smartcards, the PIN pad is usually connected directly to the host computer via a serial or an USB port. For some security-relevant operations you can also connect the PIN pad directly to the CryptoServer PCIe.

2.4 Implementation Environment with One or More CryptoServer LANs

A description of a simplified system with one or more CryptoServer LANs that is ready for use, is given below.

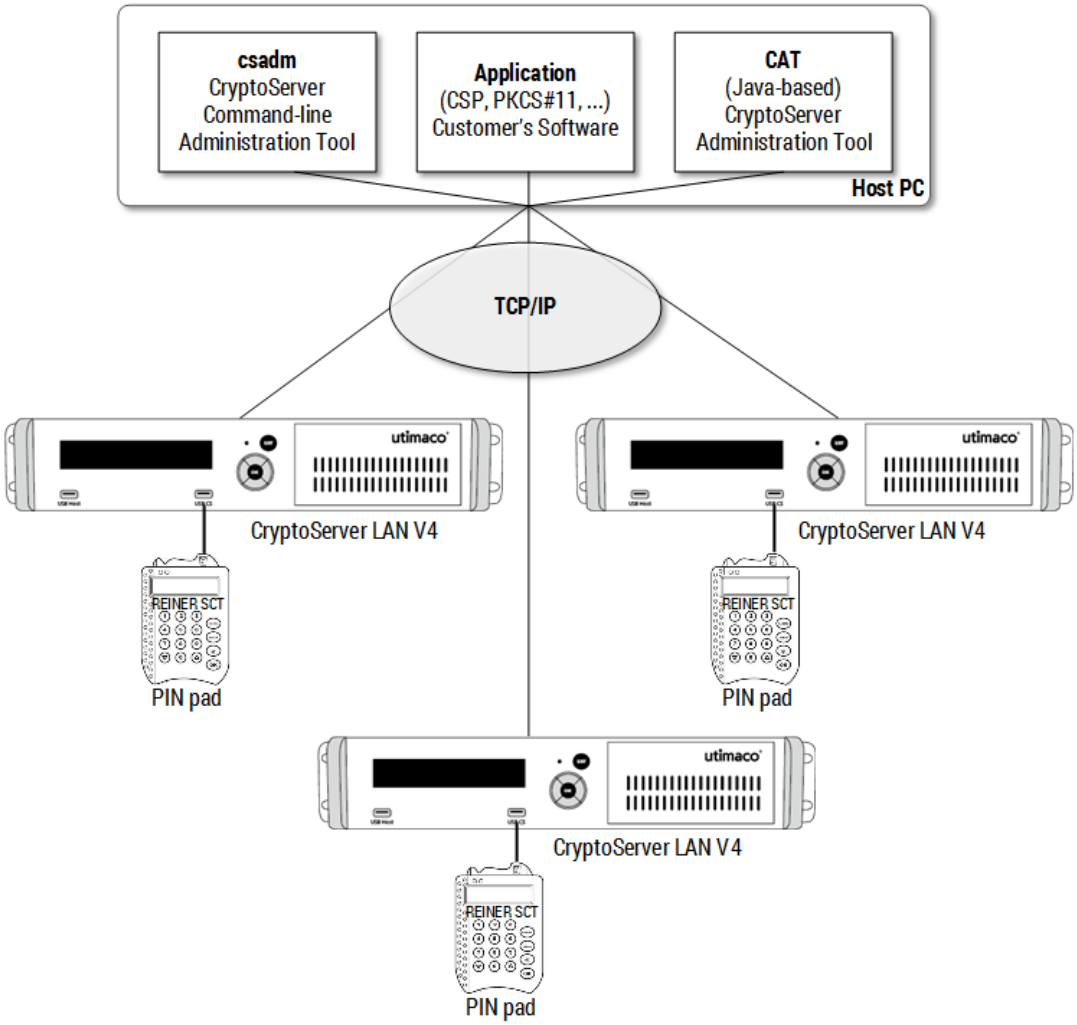


Figure 4: Example for a system with three CryptoServer LANs

The CryptoServer LAN can be administered over a network from a host computer.

The CryptoServer PCIe, which is integrated in the CryptoServer LAN, can be administered either from the host computer or directly on the CryptoServer LAN itself. To enable this, a PIN pad and ten smartcards are included in the CryptoServer LAN deliverables.

The network connection allows you to install the administration tools and the applications on one and the same host computer. However, you can also install them on different host computers. In addition, several CryptoServer LANs can be implemented in the same network and managed from the central host computer.

You find the list of all currently supported operating systems for the host computer in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` on the SecurityServer/CryptoServer SDK product CD in the folder `…\Documentation\Product Details`.

If you want to administer the CryptoServer over the network, connect the PIN pad directly to one of the serial or USB ports on the host computer. If you want to perform administration tasks locally on the CryptoServer LAN, connect the PIN pad directly to the device.

2.5 CryptoServer Simulator

The CryptoServer simulator is a software program provided by Utimaco. It simulates the cryptographic and administrative functions of all series CryptoServer. It is available for Windows and Linux operating systems, and is delivered on the SecurityServer product CD, as can be downloaded over the Utimaco web page **https://hsm.utimaco.com/download-simulator** after successful registration.

The CryptoServer simulator does not provide physical data protection as the real CryptoServer device, and should only be used for test and evaluation purposes but not for data protection in real production environments.

2.6 Hardware

The CryptoServer hardware is comparable to that of a modern minicomputer or smartphone. It includes a central processor, RAM, flash memory modules as mass storage media, a real time clock, and external interfaces. Additional hardware components are arranged specifically to provide the functionality of a hardware security module and are therefore described in greater detail.

2.6.1 Random Number Generator (RNG)

The CryptoServer implements a hardware true random number generator (TRNG) and a software pseudo random number generator (PRNG), which is also called deterministic random bit generator (DRBG).

The hardware random number generator is needed to produce real respectively true random numbers. It is implemented by using a physical noise generator, the output of which is mathematically post-processed and online tested to guarantee the quality of the generated random numbers.

CryptoServer's TRNG complies with class PTG.2 of a TRNG as specified in the BSI specification AIS 20/AIS 31. The generated random numbers can be used for the generation of signature key pairs, random padding bits, etc.

To achieve high-performant random number generation, the TRNG is enhanced by a software random generator (DRBG) which complies with class DRG.4 of DRNG as specified in the BSI specification AIS 20/AIS 31. The algorithm used by this software is specified in NIST 800-90A "Recommendation for Random Number Generation Using Deterministic Random Bit Generators". The generated pseudo random numbers can be used for the generation of keys, padding bits, etc.

2.6.2 Cryptographic Coprocessor

The powerful Se400, Se500, Se1000 and Se1500 models in the CryptoServer Se-Series/CryptoServer Se-Series Gen2 are equipped with a cryptographic coprocessor. They can therefore perform cryptographic calculations extremely quickly.

2.6.3 Physical External Housing

All the hardware components are enclosed in a sturdy metal case and are securely sealed in place. The CryptoServer and the keys and data it contains are therefore fully protected against any attack. Any attempt to break into this physical external enclosure, or to degrade any of its surfaces, will leave unmistakable traces of the attack that cannot be disguised. Any attempt to remove the physical external enclosure will destroy the CryptoServer's internal components.

2.6.4 Sensors

In addition to its physical external enclosure, the CryptoServer is equipped with a range of sensors that constantly monitor some of its critical operating parameters. In particular, these sensors check whether the device is running within the upper and lower threshold values for its operating voltage and operating temperature. If the temperature or the voltage fall below or rise above these threshold values, the sensors react as if the device is being attacked and delete the CryptoServer's internal key memory. This prevents any keys and sensitive data from being read-out as a result of unauthorized operating parameters.

An internal power supply (battery) ensures that, even when the CryptoServer is switched off, it has sufficient power to operate the sensors and to delete sensitive data or memory if necessary.

2.6.5 Tamper-protecting Foil

In the CryptoServer CSe-Series device a tamper-protecting foil is connected to the sensors. If the physical external enclosure was under a mechanical or chemical attack, which damages the tamper-protecting foil, the sensors trigger an alarm which immediately deletes all the keys and sensitive data in the CryptoServer.

When the alarm is triggered, an entry is recorded in the CryptoServer's audit log file.

The alarm triggered by the tamper-protecting foil being damaged or destroyed, is a permanent alarm. The CryptoServer cannot be brought back into operation until the tamper-protecting foil has been repaired or replaced by the manufacturer Utimaco.

After a restart, the CryptoServer goes into Maintenance Mode. This allows you to extract the status information and logfiles to analyze the error in greater detail before sending the CryptoServer device back to Utimaco for repair.

2.6.6 Key Memory

The key memory (*Key-RAM*) is non-volatile memory that is protected by the sensors. It is where the CryptoServer's individual device key is stored. These individual device key is only used within the CryptoServer to encrypt other keys and sensitive data that are stored in the CryptoServer.

If the sensors detect an attack, each individual device key in the *Key-RAM* is actively deleted by the hardware. As a consequence, none of the other keys and sensitive data in the CryptoServer can be decrypted.

2.6.7 Power Supply Monitoring

Whenever the CryptoServer is running, its sensors monitor the power supply to its PCI or PCIe ports. If this power supply falls below or rises above a predefined threshold value, it can no longer be guaranteed that the CryptoServer will run correctly. In such situations, an alarm is triggered to prevent keys or other sensitive data from being read-out by unauthorized means.

However, if the computer or CryptoServer LAN in which the CryptoServer plug-in card is installed is not actually switched on, no power supply is being supplied to the CryptoServer's PCIe port.

In this case, power is supplied to the sensors and the internal memory from a battery and a capacitor. If the power supplied from this battery sinks below a specified threshold value, there is no guarantee that the sensors will continue operating correctly. For this reason, an alarm is triggered and the capacitor's power is used to delete all the keys and sensitive data stored on the CryptoServer.

Every time an alarm is triggered, an entry is recorded in the CryptoServer's audit log file.

The alarm triggered by the power supply monitoring sensors is a temporary alarm. Once the mains power returns to within the limits of the predefined threshold values, the reason for triggering this alarm is no longer present. CryptoServer can then be brought back into operation.

2.6.8 Temperature Monitoring

The sensors monitor the CryptoServer's internal temperature whilst it is in operation. The following table shows the permitted temperature ranges and also how the CryptoServer reacts if the temperature falls below or rises above the threshold values.

Temperature	*Behavior of the CryptoServer*
Below -13 °C (8.6 °F)	Alarm is triggered, all keys and sensitive data in the CryptoServer are deleted, and the CryptoServer is restarted. After the restart the processor of the CryptoServer is suspended, commands are not executed any longer.
–13 °C to 3 °C (8.6 °F to 37.4 °F)	The processor of the CryptoServer is suspended; a new entry is written into the audit log file; commands are not executed any longer. No alarm is triggered, i.e., no keys and sensitive data stored in the CryptoServer are deleted. After being back to the normal operational temperature (4 °C to 62 °C) the CryptoServer has to be restarted in order to be operational again.
4°C to 62°C (39.2 °F to 143.6 °F)	Permitted temperature range

Temperature	*Behavior of the CryptoServer*
63°C to 66°C (145.4 °F to 150.8 °F)	The processor of the CryptoServer is suspended; a new entry is written into the audit log file; commands are not executed any longer. No alarm is triggered, i.e., no keys and sensitive data stored in the CryptoServer are deleted. After being back to the normal operational temperature (4 °C to 62 °C) the CryptoServer has to be restarted in order to be operational again.
Above 66°C (150.8 °F)	An alarm is triggered, all sensitive data in the CryptoServer are deleted and the security module is restarted. After the restart the processor of the CryptoServer is suspended, commands will not be executed any longer.

Table 3: Temperature ranges and CryptoServer behavior

The temperature ranges given in this table are only approximate and may vary slightly due to the tolerances of individual components.

An entry is recorded in the CryptoServer audit log file both when the device goes into sleep mode and when an alarm is triggered.

If the CryptoServer is in sleep mode, it can be reset to Operational Mode once its internal temperature returns to the permitted temperature range. To do this, you must perform a hardware reset on the CryptoServer. As no keys or other data are deleted when the CryptoServer goes into sleep mode, it returns to Operational Mode once the restart procedure is completed.

The alarm triggered by the temperature monitoring sensors is a temporary alarm. Once the temperature returns to within the limits of the predefined temperature range, the reason for triggering this alarm is no longer present. CryptoServer can then be brought back into operation.

2.7 An Alarm and Its Consequences

When an alarm is triggered, the following sensitive data is actively deleted from the CryptoServer:

- The individual device key.
  This automatically makes all the other keys (including the MBK) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the individual device key.
- All the users from the user database who use a password-based mechanism to authenticate themselves:

However, all the users who log in to the CryptoServer with a signature-based mechanism (RSA Signature, RSA Smartcard or ECDSA signature) are not deleted.

After the alarm, the CryptoServer is no longer in Operational Mode and will go into Maintenance Mode after a restart.

The alarm must be reset by an administrator who has the appropriate authentication status before the CryptoServer returns to Operational Mode.

After triggering the alarm, the CryptoServer is no longer in Operational Mode and will go into Maintenance Mode after a restart. Before you, as the administrator, reset an alarm, you should find out why it was triggered. At this point you must note the following:

- If the alarm is a temporary alarm, and the event that triggered it is no longer present, (i.e. the power supply and the internal temperature of the CryptoServer are once again within the permitted threshold values), the CryptoServer returns to Operational Mode after a reset of the alarm and the restart.
- If the alarm is a temporary alarm and the event that triggered it is still present (i.e. the power supply or the CryptoServer's internal temperature are still not within the permitted threshold values), CryptoServer goes into Maintenance Mode after the restart. The CryptoServer will not return to Operational Mode after a restart until you resolve the event that triggered the alarm and reset the alarm.
- If the alarm is a permanent alarm, i.e. the tamper-protecting foil in a CryptoServer CSe-Series has been damaged or destroyed, the CryptoServer returns to Maintenance Mode after the restart. Any attempt to reset the alarm will not succeed. You cannot bring the CryptoServer into operation again until it has been repaired by Utimaco IS GmbH.

2.8 The Software of the CryptoServer

Different software components work together in the CryptoServer at different times. This section gives a brief introduction to these software components and describes their functionality.

2.8.1 Bootloader

The bootloader is a base software stored in the CryptoServer's FLASH memory. It runs every time the CryptoServer (re)starts, before the actual operating system and the other firmware modules are booted.

If you are working as a CryptoServer administrator, you will never come into contact with the bootloader in "normal" operations. For this reason, the bootloader is only described in brief here. More detailed information is provided in the sections about the special situations in which the bootloader plays a critical role.

2.8.2 Firmware Modules

The CryptoServer's firmware has a modular structure. In addition to the actual SMOS (*Security Module Operating System*) operating system there are a number of other firmware modules each performing specific functions, for example, generating random numbers, signature generation and data encryption (RSA, elliptic curves cryptography, DES, AES, etc.), performing hash functions, access to the internal real time clock, database for storing keys and other data, communications with the PIN pad and smartcard, etc.

All these firmware modules are loaded, updated and deleted more or less independently of each other. When you upgrade a firmware module it is ensured that any keys and data already present, are transferred automatically and therefore do not need to be imported from scratch.

The firmware modules included, by default, in version 4.00.0 and later of SecurityServer firmware packages are listed below:

- SMOS (Security Module Operating System)
- CMDS (Command Scheduler) command processing and user management
- ADM Administration of firmware modules
- UTIL (utilities) access to the real time clock and random number generator
- CXI (Cryptographic eXtended Interface); Utimaco’s proprietary cryptographic HSM interface which is used by the host libraries for the CXI API, PKCS#11 (CXI module version 2.0.0.0 or later), CSP/CNG, JCE, OpenSSL and EKM.
- VDES (DES algorithm); used for key generation, encryption/decryption, MAC
- AES (AES algorithm); used for key generation, encryption/decryption, MAC
- VRSA (RSA algorithm); incl. key pair generation
- LNA (Long Number Arithmetic)
- ECA (Elliptic Curve Algorithm)
- ECDSA (Elliptic Curve Cryptography, ECDSA signature generation/verification, key pair generation)

- DSA (Digital Signature Algorithm)
- HASH various hash algorithms
- DB database used to store keys and other data
- MBK (Master Backup Key (MBK) Management) incl. generation, export and import of MBK
- ASN1 (Abstract Syntax Notation One)
- NTP Time management using an NTP (Network Time Protocol) client
- HCE (Hardware Crypto Engine): interface for accessing the crypto accelerator chip, Broadcom, of the CryptoServer Se400 and Se1000, and Exar of the CryptoServer Se500 and Se1500 (Se-Series Gen2).

  The HCE module will only start if the Broadcom hardware crypto accelerator chip is built into the CryptoServer Se or the Exar hardware crypto accelerator chip is built into the CryptoServer Se-Series Gen2. If this is not the case, the initialization state of HCE and BCM, for a CryptoServer Se, and HCE and EXAR, for a CryptoServer Se-Series Gen2, will be set to INIT_INACTIVE, and no services of HCE, BCM resp. EXAR firmware modules are available.
- BCM: Driver for the Broadcom crypto accelerator chip of the CryptoServer Se; this firmware module can only provide its full functionality if the HCE firmware module is available and fully functional.
- EXAR: Driver for the Exar crypto accelerator chip of the CryptoServer Se-Series Gen2; this firmware module can only provide its full functionality if the HCE firmware module is available and fully functional.
- PP (PIN Pad Driver)
- SC (Smartcard Driver)

2.8.3 Firmware Package

The SecurityServer product CD supplied along with every CryptoServer device contains all firmware modules, provided as firmware packages. You can easily identify these packages by their `.mpkg` file extension in the folder `\Firmware\SecurityServer-<CryptoServer-Series>`.

For the different series of CryptoServer, Se-Series, Se-Series Gen2, CS- and CSe-Series, as well as for the CryptoServer simulator and the FIPS 140-2 Level 3 certified CryptoServer Se, the corresponding SecurityServer firmware packages are provided.

2.9 System Keys

These keys play an important role in the CryptoServer's security concept:

- The default authentication key `ADMIN.key` for the default administrator ADMIN.
- The individual device key used to encrypt all the keys and data in the CryptoServer.
- The Master Backup Key (MBK) used to encrypt the backup copies of the key and/or user data stored in the CryptoServer. This ensures that this data can also be stored securely outside the CryptoServer.

2.9.1 Default Authentication Key

The authentication key `ADMIN.key` is an RSA key with a key length of at least 1024 bit. It is generated by the manufacturer Utimaco before the CryptoServer is delivered to you. The private part of the key is made available to you (to every customer) on the smartcards, and as a keyfile on the SecurityServer product CD in the folder `\Software\All_Supported_Operating_Systems\Administration\key`. The public part of the key is loaded into the CryptoServer device by the manufacturer Utimaco before it has been delivered to you.

The default administrator ADMIN who already has been set up on the CryptoServer must then use this authentication key to authenticate initial administration tasks. It can also be used to authenticate other specific CryptoServer users.

Since the ADMIN.key is a default key that does not provide any individual protection, we strongly recommend to replace it by your own authentication key as soon as possible. For detailed instructions on how to generate a new authentication key on a smartcard, read chapter 5.6.1. Chapter 5.6.6 contains detailed instructions on how to generate a new authentication key as a keyfile.

2.9.2 Individual Device Key

The individual device key (CryptoServer's Master Key) is generated randomly every time the CryptoServer is brought into operation. It cannot be readout, exported, or imported, saved, or restored, and is therefore inaccessible to everyone, even to the CryptoServer owner. It is implemented exclusively within the CryptoServer itself.

The individual device key is used to encrypt all the other keys and sensitive data stored in the CryptoServer.

2.9.3 Master Backup Key (MBK)

The CryptoServer provides secure storage for secret data and private keys. This includes, for example, the keys used by the PKCS#11, CSP/CNG, JCE and other interfaces. As any perceived attack will cause the CryptoServer to permanently delete all the sensitive data and

private keys stored on it, we strongly recommend you to back up this data and keys so they can be reimported (restored) once the alarm has been resolved. To ensure that each backup copy of sensitive data or private keys is stored securely even outside the CryptoServer, it is protected with the Master Backup Key (MBK).

The purpose of an MBK is therefore to protect the backups and externally stored secret data and private keys from unauthorized access.

As an alarm will also cause the MBK to be permanently deleted, a backup copy of this key has to be stored in a different location (not on the CryptoServer).

If the MBK is stored on a smartcard or in a keyfile, it is always split into several, at least two parts (shares), approval according to the two-person rule. Splitting the MBK into several key shares is one of CryptoServer's most important security functions because it enforces the MBK to be used by several people (at least two), who then share responsibility for its use.

The MBK is always split into minimum two shares. Each of these shares can be stored outside the CryptoServer in two different ways:

- On a smartcard protected by a PIN
- As a keyfile protected by a password

The MBK firmware module provides the following functions for MBK management:

- Generation and storage of an MBK
  This function generates a 256-bit (32-byte) AES key as an MBK within the secure environment of the CryptoServer. To ensure the highest possible levels of quality and "randomness" the hardware random number generator of the CryptoServer is used for the MBK generation. The generated MBK is then split into shares and stored on smartcards or in keyfiles, but it is not stored yet on the CryptoServer. The MBK must be imported into the CryptoServer in a separate step.
- Import of an MBK
  This function imports an MBK from the smartcards or keyfiles to the CryptoServer. For backward compatibility purposes, the import of 128-bit (16-byte) DES keys is supported additionally.

For detailed step-by-step instructions on managing an MBK with CAT, see chapter 5.8 in this manual. For details on managing an MBK with the command-line tool csadm, see the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*.

There are two methods for managing an MBK:

- Local MBK Management
  In this case, the PIN pad is connected directly to the CryptoServer. As the CryptoServer writes the MBK shares directly to the smartcards, they are neither stored in the host computer's RAM nor transferred via a network. However, if you use this method, you cannot store the MBK in a keyfile.

Local MBK management can be performed by both the csadm command-line tool and the CryptoServer LAN menu.

- Remote MBK Management
  In this situation, the MBK can be managed over a network on a CryptoServer LAN. After the MBK has been generated in the CryptoServer, its shares are transferred to the host computer, where the administration tools have been installed. Afterwards, they are stored on smartcards or in keyfiles. If the MBK shares are stored on smartcards, the PIN pad is connected to the host computer.

2.9.4 Tenant Backup Keys

As from SecurityServer/CryptoServer SDK 4.10 the Master Backup Key can be additionally used to derive individual backup keys, called Tenant Backup Keys (TBK). The TBKs ensure that key backups and keys stored outside a CryptoServer, and used for example by the PKCS#11, CSP/CNG or CXI API, are protected in an individual way. For example, in a cloud environment the CryptoServer serves as the root of trust for more than one PKCS#11 applications simultaneously. Each application uses a single PKCS#11 slot on the CryptoServer for its individual key management. The CryptoServer considers each of these applications as a tenant. Thus, the key backup of a slot is protected with the slot-individual TBK and can only be accessed by the authorized users of that PKCS#11 slot.

The database backup functionality in CAT and csadm always uses the CryptoServer's MBK. The individual protection of external keys and key backups by using TBKs is only provided by P11CAT, p11tool2 and the CXI tool, and requires individual configuration.

TBKs are not used by default. The CryptoServer can be configured on demand to use them. This is done by setting dedicated configuration attributes. Further individualization of the TBKs can be achieved by defining individual passphrases for their derivation.

The usage of TBKs can be enabled globally for the CryptoServer or only for specific CryptoServer PKCS#11 slots/CXI key groups:

- The global use of TBKs means that TBKs are used for every key and each PKCS#11 slot/CXI key group. To enforce this, the CryptoServer requires one or more authenticated CryptoServer users with user management rights (min. authentication status 20000000) or the ADMIN to set the following global configuration attribute:
  - For PKCS#11 applications: Set `CKA_CFG_SLOT_BACKUP` to `CK_TRUE` by using the p11tool2 (command `SetGlobalConfig`) or P11CAT.

- For applications using Utimaco's CXI interface: Set `SecureGroupBackup` to `true` by using the CXI tool, for example:

```
cxitool LogonSign=ADMIN,C:\Utimaco\keys\ADMIN.key SetConfig=SecureGroupBackup,true
```

- The slot/key group-specific use of TBKs means that TBKs can be used only for selected PKCS#11 slots/CXI key groups on the CryptoServer. To enforce this, the CryptoServer requires the corresponding PKCS#11 slot/CXI key group administrator(s), so-called Security Officer(s) (SO), with permissons in the user group 2 (min. authentication status 00000200) to set the configuration attributes mentioned above for the specific PKCS#11 slot(s)/CXI key group.

For further details on how to configure the CryptoServer to use TBKs, read the *CryptoServer PKCS#11 Administration Tool Release 2 Reference Manual* respectively the *PKCS#11 CryptoServer Administration Tool – Manual for System Administrators*.

For configuring the passphrase, the `SecureSlotPass` command has been introduced in the command-line tools p11tool2 and the CXI tool. For details on how to use the command to configure your PKCS#11 application, see the corresponding chapter in the *CryptoServer PKCS#11 Administration Tool Release 2 Reference Manual*. For details on setting the passphrase with the CXI tool, refer to the cxitool in-tool help.

If a passphrase shall be used for the derivation of TBKs, it has to be defined prior to enabling the usage of TBKs. The usage of TBKs in turn must be configured before the corresponding PKCS#11 slot/CXI group on the CryptoServer gets operational. Otherwise, existing external keys and key backups become inaccessible.

2.10 Operating States

The CryptoServer has two operating states, which are described briefly in this section.

2.10.1 INITIALIZED Operating State

When the CryptoServer is started correctly, it goes into the INITIALIZED operating state.

2.10.2 DEFECT Operating State

The bootloader performs a self-test every time the CryptoServer starts to check whether particular hardware and software components are functioning correctly. If this self-test detects an error, booting is interrupted and the CryptoServer switches to the DEFECT operating state.

If it is still possible to call the CryptoServer's status whilst it is in the DEFECT operating state, you will see its operating state displayed as DEFECT.

In this operating state the CryptoServer accepts either only very few or no administration commands.

If a significant hardware defect is present, it may not even be possible to start the bootloader itself. If the bootloader cannot be started, the operating state DEFECT will not be displayed. In this situation, the CryptoServer's register displays an undefined value.

2.11 Operating Modes

When the CryptoServer's operating state is INITIALIZED it can be in either one of two basic operating modes.

- Operational Mode
- Maintenance Mode

These modes are described in greater detail in the following sections.

2.11.1 Operational Mode

The Operational Mode means that the CryptoServer is functioning correctly. The complete set of loaded firmware modules (`.msc`) has been started successfully.

2.11.1.1 Administration-Only Mode

You can configure the startup mode of the CryptoServer, by using the csadm administration tool, in a way that the automatic activation of cryptographic interfaces after a restart is blocked. This is indicated as the *Operational Mode – Administration-Only* which is first provided with the release 4.00.0 of the SecurityServer product CD.

It is an operating mode that provides access to all CryptoServer administration functions, and blocks all cryptographic (key management and key usage) functions.

- The Operational Mode – Administration-Only can be activated as default startup mode. Therefore, a dedicated csadm command specified in chapter "SetStartupMode" of the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*, shall be executed. It has to be authenticated by one or more users with system administration rights, and defines that on the next restart of the CryptoServer all cryptographic interfaces will be disabled.
  For example, if an attacker would be able to steal both, the CryptoServer device and the

authentication credentials of a key manager or key user, booting into Operational Mode – Administration-Only will prevent the attacker from misusing the stolen CryptoServer.

- The Operational Mode – Administration-Only can also be activated temporarily.
  This means that all cryptographic functions can be blocked on-demand by users with system administration permissions. For example, during CryptoServer maintenance, for avoiding delays or interruptions by long-lasting key generations in the middle of a maintenance window. Another dedicated csadm command, as described in chapter "SetAdminMode" of the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*, shall be used for that. No restart of the CryptoServer is required.

2.11.2 Maintenance Mode

The Maintenance Mode means that the CryptoServer is no longer ready for normal operation, and only the backup-set of firmware modules (`.sys`) is running. This mode provides an interface for performing administration tasks, but no cryptographic services are available. The following events will cause the CryptoServer to go into Maintenance Mode:

- The CryptoServer's sensors have triggered an alarm, and all the keys and sensitive data have been deleted from the device.
- The CryptoServer's operating system, SMOS, cannot be started or loaded without an error occurring.

The following actions will cause the CryptoServer to go into Maintenance Mode.

- An *External Erase* has been performed and this has triggered an alarm.
- The `Clear` command has been used to delete the entire contents of the CryptoServer.

The CryptoServer's functionality is very restricted in Maintenance Mode. The administrator can perform all functions required to make the CryptoServer operational again. Applications like, e.g., PKCS#11, JCE, CSP/CNG, etc., cannot access the CryptoServer when it is running in this mode. For information about how to switch from Maintenance Mode to Operational Mode, read chapter "Checking the Operativeness and the State of the CryptoServer" in the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*.

2.12 External Erase

An External Erase is accompanied by an alarm and actively deletes the following sensitive data from the CryptoServer:

- The individual device key
  This automatically makes all the other keys (including the MBK) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the individual device key.

- All the users from the user database who use a password-based mechanism to authenticate themselves

However, all the users who log in to the CryptoServer with RSA Signature, RSA Smartcard or ECDSA are not deleted.

After the External Erase the CryptoServer is no longer in Operational Mode and returns to Maintenance Mode after a restart.

The alarm triggered by an *External Erase* must be reset by an administrator who has the appropriate authentication status before the CryptoServer returns to Operational Mode.

The alarm triggered by an *External Erase* is the prerequisite for performing a *Clear to Factory Settings* on the CryptoServer.

However, you must ensure that the alarm triggered by the *External Erase* is not reset so that the *Clear to Factory Settings* function can also be performed.

2.13 Clear

Use the `Clear` command to manually delete all the sensitive data and firmware modules from the CryptoServer. The following actions are triggered after you enter this command:

- The firmware modules are deleted.
  Only the system firmware modules `.sys` required for base administration remain on the CryptoServer.
- All the users using a password to log in to the CryptoServer are deleted.
- A new individual device key is generated for the CryptoServer.
  This automatically makes all the other keys (including the MBK) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the "old" individual device key.

However, all the users who log in to the CryptoServer with RSA Signature, RSA Smartcard or ECDSA signature are not deleted.

After the `Clear` the CryptoServer is no longer in Operational Mode and returns to Maintenance Mode after a restart.

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

You should only use the `Clear` command if you want to set up or reinstall the CryptoServer again.

2.14 Clear to Factory Settings

If ever you can't find the authentication key for the default administrator, ADMIN, and can therefore no longer administer the CryptoServer, you can also perform an *External Erase* directly on the CryptoServer and on the CryptoServer LAN.

However, if you do perform this *External Erase* directly on the CryptoServer or the CryptoServer LAN, this will trigger an alarm which enables you to perform a *Clear to Factory Settings*.

The *Clear to Factory Settings* command can only be implemented if the alarm triggered by the *External Erase* is still present.

When you run the *Clear to Factory Settings* command, it resets the CryptoServer to the state it was in when it was first supplied. The *Clear to Factory Settings* command triggers the following actions:

- The firmware modules are deleted.
  Only the system firmware modules required for base administration remain on the CryptoServer.
- All the users in the CryptoServer user database are deleted.
- The default administrator ADMIN is set up again and can use the original authentication key `ADMIN.key` to log in to the CryptoServer.
- A new individual device key is generated for the CryptoServer. This automatically makes all the other keys (including the MBK) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the "old" individual device key.

After the *Clear to Factory Settings* the CryptoServer is no longer in *Operational Mode* and returns to *Maintenance Mode* after a restart.

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

2.15 Users, User Groups and Authentication

The commands given to the CryptoServer can only be authenticated by authorized users. The CryptoServer provides user management functions for this purpose.

2.15.1 Users

Every user is identified by a unique name. In addition, every user is also assigned a number of other properties that are described in the following table.

Property	*Meaning*
Name	Used as a unique identification for a user
Permission	User's permissions for the different user groups
Authentication mechanism	Defines how the user is to authenticate themselves
Authentication token	Keyfile or password depending on the authentication mechanism
Flags	Two flags that define whether the user has to authenticate the corresponding command for opening a Secure Messaging session or not.
Attributes	Additional data used to specify particular properties or restrictions, such as that a user may only access specific keys

Table 4: CryptoServer User properties

All this data is stored in a user database in the CryptoServer. These properties and their meanings are described in greater detail in the sections that follow.

2.15.2 User Groups

The CryptoServer's user management functionality has eight user groups, numbered from group 0 to group 7. Some user groups are reserved by Utimaco IS GmbH for applications and their corresponding role-based user profiles.

Group	*Application*	*Role-based user profile*
0	All cryptographic Interfaces	Cryptographic User und PKCS#11 User
2	PKCS#11	PKCS#11 Security Officer (SO)
5	NTP Administration	NTP Manager
6	System Administration	System Manager
7	User Management	User Manager

Table 5: User groups and role-based user profiles reserved for specific applications

2.15.3 Permissions and Authentication Status

A user has a particular permission in each of the eight user groups. This permission is represented by the numbers 0 to 0xF (15). The next table shows the meaning of this permission.

Permission	*Meaning*
0	The user has no permissions in that particular user group.
1	Two-Person rule: although the user can authenticate commands to the CryptoServer, a second user is also required to do this.
2	The user is entitled to authenticate commands on his own.
3 to 0xF	Not required by the CryptoServer firmware functions by default. Might be required by functions with custom permissions defined in a signed configuration file `cmds.scf` (see chapter 2.16 for detailed information).

Table 6: User permissions

Authentication status from the view point of the CryptoServer

From the CryptoServer's point of view, the authentication status defines which permission must be present before it can perform a particular command.

Authentication status for user management

User group 7 is reserved for user management. Permission 2 in user group 7 is required to authenticate the corresponding commands. Therefore, the user management can only be performed by users who have reached on their own or in pairs (two-person rule) the authentication status 20000000 at the CryptoServer.

User group	7	6	5	4	3	2	1	0
Authentication status	2	0	0	0	0	0	0	0

Authentication status for administering firmware modules

User group 6 is reserved for the administration of firmware modules (loading, replacing or deleting firmware modules). Permission 2 in user group 6 is required to authenticate the corresponding commands. Therefore, the firmware module administration can only be done

such users who have reached on their own or for example in pairs (two-person rule) the authentication status 02000000 at the CryptoServer.

User group	7	6	5	4	3	2	1	0
Authentication status	0	2	0	0	0	0	0	0

Authentication status from the user's point of view

From the user's point of view, the authentication status defines which permission(s) can be reached effectively by one or more authentications. After an authentication has been performed successfully, the authentication status is increased by the user's (or users', if they are more than one) permission, starting from authentication status 00000000. The examples below illustrate this relationship.

The CryptoServer has four users who have the following permissions.

User group	7	6	5	4	3	2	1	0
ADMIN	2	2	0	0	0	0	0	0
Admin1	0	1	0	0	0	0	0	0
Admin2	0	1	0	0	0	0	0	0
User3	0	0	0	0	0	0	1	0

No user has been authenticated.

Authentication status:	0	0	0	0	0	0	0	0

ADMIN has been authenticated.

Authentication status:	2	2	0	0	0	0	0	0

The commands used to administer firmware modules and those involved in user management can now be performed because authentication status 2 has been reached in groups 6 and 7.

Only Admin1 has been authenticated.

Authentication status: 0 1 0 0 0 0 0 0

The commands used to administer firmware modules cannot be performed because authentication status 2 has not been reached in group 6.

Admin1 and Admin2 have been authenticated.

Authentication status: 0 2 0 0 0 0 0 0

The commands used to administer firmware modules can now be performed because authentication status 2 has been reached in group 6. However, the commands involved in user management cannot be performed because neither of the two administrators has the appropriate permission in group 7.

Admin1 and User3 have authenticated themselves.

Authentication status: 0 1 0 0 0 0 1 0

Despite the fact that two authenticated users are now present, the commands used to administer firmware modules still cannot be performed because authentication status 2 has not been reached in group 6.

Authentication status and permissions

The following table provides an overview of the functions which can be performed once the authentication status 20000000 and 02000000 has been reached.

Authentication status	*Permissions*
20000000	Create a user
	Delete users
	Create a backup of user data
	Restore user data
	Reset alarm
02000000	Load, replace and delete firmware modules
	Set time
	Reset alarm

Authentication status	*Permissions*
	Clear CryptoServer
	Import Master Backup Key
	Delete audit log

Table 7: Permissions for authentication status 20000000 and 02000000

2.15.4 Permissions for New Users

The permissions within applications have already been defined at the programming stage. Once an application has been loaded into CryptoServer you can no longer change its assignment to a user group or the permission. When you assign new permissions within the individual user groups, you must also take into account the fact that several user groups have already been predefined by Utimaco IS GmbH. The following table shows which user groups have been predefined by the Utimaco IS GmbH for applications and the corresponding role-based user profiles and which are unused:

User Group	*Application*	*Role-based user profile*
0	All cryptographic interfaces	Cryptographic User und PKCS#11 User
1		
2	PKCS#11	PKCS#11 Security Officer (SO)
3		
4		
5	NTP Administration	NTP Manager
6	System Administration	System Manager
7	User Management	User Manager

Table 8: CryptoServer user groups and their permissions

In principle, it is possible to assign new permissions to a user group that has already been predefined. As a result, the new permissions in a predefined user group are automatically given the predefined permission. Therefore, a new permission in group 5 (NTP Administration) can also administrate NTP.

As the predefined user groups 6 and 7 have already been assigned wide-ranging administration rights for the CryptoServer, we recommend you do not assign any other permissions to these groups.

2.15.5 Authentication Mechanisms

CryptoServer can authenticate a user in a number of different ways. These mechanisms are described in greater detail in the sections that follow.

Authentication with electronic signature

Authentication with an electronic signature provides every user with a pair of keys, one public and one private.

This authentication mechanism is then described as an RSA Signature or ECDSA Signature depending on which algorithm you select.

In this method, the private part of the RSA or ECDSA key is stored on a smartcard or in a keyfile which the user must keep in a safe place. The corresponding public part is stored as `authentication data` in the CryptoServer's user database.

Every command which is sent to the CryptoServer will be signed by user's private key.

A random number provided by CryptoServer is included in the signature calculation process. This prevents a signed command from being intercepted and entered again later.

The CryptoServer then uses the corresponding public key to check this signature. The signature authenticates the command and checks whether the command is genuine, i.e. no transfer errors have occurred and there is no sign of data manipulation.

As this procedure does not transfer any confidential authentication data it is particularly suitable for remote authentication to the CryptoServer LAN when the network connection is not completely under your control.

Authentication with an electronic signature can be used with all the CryptoServer administration tools and for local administration tasks on the CryptoServer LAN, as long as the user's private key is stored on a smartcard.

If the private part of the key is stored in a keyfile, this procedure cannot be used for local administration tasks on the CryptoServer LAN.

Authentication with an RSA smartcard

A special variant of the electronic signature authentication process described above is authentication with an RSA smartcard. In this procedure the user's private RSA key is only stored on a smartcard and not in a keyfile. The corresponding public part is stored as authentication data in the CryptoServer's user database.

If you use this authentication mechanism, the PIN pad must be connected directly to a port on the CryptoServer.

You cannot use the ECDSA algorithm with this procedure.

In contrast to the first procedure described above, the electronic signature is not calculated before the command is sent to the CryptoServer. The command is sent first to the CryptoServer and then the CryptoServer requests a signature via the RSA smartcard.

You should use authentication with an RSA smartcard if you want to make sure that an authorized user authenticates a command locally on the CryptoServer.
Remote authentication is not an option here because the PIN pad must be connected directly to the CryptoServer in this case.

The electronic signature authentication can be implemented with all the CryptoServer administration tools.

Authentication with user name and password

The authentication mechanism involving the user name and password is by far the most well-known. Unfortunately, this mechanism is not as secure as the authentication using an RSA smartcard.

The CryptoServer supports HMAC password mechanism for user authentication. The password is transferred to the CryptoServer in a protected form: A random number is added to each authentication. This prevents the authentication from being intercepted and performed again at a later point in time. Thus, the HMAC password authentication procedure is also suitable for remote authentication to the CryptoServer LAN.

The HMAC password is stored as authentication data in the CryptoServer's user database `user.db`.

All CryptoServer administration tools support authentication with a user name and an HMAC password.However, since you cannot enter a password using the CryptoServer LAN menu options, this authentication mechanism cannot be used if you are administering the CryptoServer LAN locally, by using its front panel.

2.15.6 Authentication Mode

Every security-relevant command must be authenticated by an authorized user before it is send to the CryptoServer.

If you administrate the CryptoServer with the command-line tool csadm, you shall authenticate every command individually, with the csadm `LogonSign` or `LogonPass` command, depending on the user's authentication mechanism.

If you administrate the CryptoServer with the Java-based administration tool CAT, a Secure Messaging connection to the CryptoServer is established every time a user logs in to the CryptoServer. This connection is set to a maximum duration of 14 minutes and 59 seconds and resets to 14 minutes and 59 seconds every time the user sends a command to the CryptoServer, or when another user 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, all the users currently logged on to the CryptoServer are logged off simultaneously. This is because the Secure Messaging connection, which is being used by these multiple users, is terminated.

2.15.7 ADMIN, the Default Administrator

We have already set up the default administrator, ADMIN, on the CryptoServer to ensure you can administer the CryptoServer after it has been delivered.

The administrator ADMIN not only has the authentication key (smartcard or keyfile), but also has full permissions in user groups 6 and 7 that are reserved for administration tasks and can authenticate any command on their own. However, the default administrator ADMIN has no permissions in user groups 0 to 5.

Anyone who has the authentication key on the smartcard or as a keyfile can log in to the CryptoServer as the default administrator ADMIN and manage the device on their own.

The user rights in the default administrator ADMIN's user groups 6 and 7 cannot be changed on the CryptoServer. You can only change the authentication key used by the default administrator ADMIN to log in to the CryptoServer.

If the following criteria have been met, it is also possible to delete the default administrator we set up on the device:

- You create one or more new users as administrators who have the same rights in total in user groups 6 and 7 as the default administrator ADMIN already set up on the CryptoServer.
- However, only these authentication mechanisms are permitted for the new administrator(s):
  - RSA signature on a smartcard or stored in a keyfile
  - Password (HMAC)

The new administrator(s) cannot use a Clear Password as the authentication mechanism in user groups 6 and 7.

This therefore enables you to implement a two-person rule for the CryptoServer's administration tasks. You create two new administrators who in total have the same rights in user groups 6 and 7 as the default administrator ADMIN previously had on their own. The corresponding role-based user profiles have been set up in the CAT for this purpose.

After this you can delete the default administrator we supplied with the CryptoServer. From that point onwards, two people will be required (two-person rule) to perform the CryptoServer administration tasks.

Permissions

The default administrator with authentication status 22000000 is permitted to perform these functions on the CryptoServer:

- Create a user
- Delete users
- Create a backup of user data
- Restore user data
- Load, replace and delete firmware modules
- Set time
- Reset alarm
- Clear CryptoServer
- Import Master Backup Key

- Delete audit log

2.15.8 Cryptographic User

A Cryptographic User with permission 2 in the user group 0 (authentication status 00000002) has been set up in CAT by default. The Cryptographic User has all the permissions in user group 0 and can authenticate all the commands on its own. The Cryptographic User has been created to enable you to administer all the cryptographic interfaces.

- CXI (Cryptographic eXtended Interface)
- JCE (Java Cryptography Extension)
- CSP/CNG (Microsoft CryptoAPI and Cryptography Next Generation)
- Open SSL (Cryptographic Token Interface), only if the CryptoServer is connected directly via an ENGINE interface
- EKM (Extensible Key Management)

The permissions assigned to the Cryptographic User in user group 0 have been defined in the CXI firmware module and cannot be changed.

2.16 Configurable Role-based Access Control (C-RBAC)

With release 4.0 of the SecurityServer product CD the CryptoServer provides the possibility to increase the required permissions for the authentication of specific CryptoServer functions.

The increased permission requirements can be individually configured by the customer for all external functions specified in the signed configuration file `cmds.scf`. During command execution, the currently reached permission for the function is compared to the required permission in the configuration file. If they are equal or no permission restrictions list exists, the command is executed normally performing the default (unchanged) permissions check for the command.

For detailed information about signed configuration files and their use, read chapter "Signed Configuration Files" in the *CryptoServer Command-line Tool –csadm – Manual for System Administrators*. There you will also find a list of all firmware functions for which you might define enhanced permission requirements.

2.17 Secure Messaging

The CryptoServer supports Secure Messaging for communications between the host and itself. Commands from the host to the CryptoServer and the CryptoServer's replies to the host can be encrypted and the integrity of the data can be protected by a MAC (Message Authentication Code).

In Secure Messaging between the CryptoServer and the host, a new random session key is generated for each connection. This prevents recorded data packets belonging to an earlier connection from being imported into a new connection. No valid data packets can be present once the imported data packet has been decrypted with the current session key.

In addition, the CryptoServer generates a start value for a sequence counter and a session ID for every new session key. The sequence counter increases every time a command is sent and is also included in the MAC calculation or integrity check. This ensures that no commands are recorded within the same connection and sent to the CryptoServer again. The unique session ID guarantees that every session key is uniquely identifiable. All the commands that use the same session key and session ID are part of the same session (connection).

A session key automatically becomes invalid if it is not used for 15 minutes.
The SecurityServer/CryptoServer SDK 4.10 and later support a maximum of 4096[1] session keys (connections) active at the same time. If another session key is requested for a connection, exceeding the maximum of 4096, the oldest connection is closed and the session key, associated with it, becomes invalid.

The benefits of sending messages with Secure Messaging are obvious. Once a session key has been requested, and a secure connection has been established between the host and the CryptoServer, all the commands exchanged within this session are authenticated, encrypted and secured against being tampered by a MAC.

Additionally, starting with SecurityServer/CryptoServer SDK 4.10 the CryptoServer can be configured to authenticate itself towards host applications at the beginning of a Secure Messaging session. For that purpose a new key, the HSM Authentication Key (a 3072-bit RSA key), has been introduced that can be used to verify the authenticity of a Secure Messaging session originating from the HSM.

[1] The SecurityServer/CryptoServer SDK 4.01 and earlier support a maximum of 256 session keys which are active at the same time and used by different host applications (each key identified by its session ID). If a host application requests a new session key while the maximum of 256 sessions are already active, the oldest session is closed and the session key session key, associated with it, becomes invalid.

The new security feature is disabled in the default configuration of the CryptoServer. It can be enabled on demand by using the csadm administration tool as explained in Chapter "Enabling Mutual Authentication" of the manual *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*. There you will also find a detailed description of the concept in the Chapter "Mutual Authentication" and of the newly introduced csadm command `GetHSMAuthKey` in the corresponding chapter.

2.18 Logs

In the CryptoServer, every action that involves a security issue (for example, creating a new user) or event (especially the triggering of an alarm) is saved in logs. There are two types of log: the boot log and the audit log.

2.18.1 Boot Log

Every time the CryptoServer starts up, i.e. after being switched on, and after a reset, every individual step and its results are recorded in the boot log. These include:

- The version number of the loaded operating system (SMOS)
- The version number of the internal sensor switch
- Information about whether a license file is present and which system settings have been made on the basis of this license file
- For every firmware module that was loaded and started by the operating system: a short description and unique ID to identify it, whether it could be initialized successfully or which errors occurred during the initialization process.

If any problems occur during the boot process, you can use the boot log to analyze the errors.

The boot log is stored as a text file in the CryptoServer and is therefore available in a readable format after you import it.

2.18.2 Audit Log

The audit log is where all the events and actions involving security issues that occur or are performed whilst the CryptoServer is running are recorded. It records if the following occurs:

- The sensor triggers an alarm
- The permitted upper limit for the CryptoServer's internal temperature has been exceeded and the CryptoServer has therefore changed into sleep mode (power down mode)
- An alarm is reset
- The CryptoServer is completely deleted
- The date/time in the CryptoServer's real time clock (RTC) is reset

- Firmware modules or packets have been loaded, deleted or replaced
- Users have been created, changed or deleted or their "properties" have been changed
- The audit log is deleted
- A few other infrequently used commands

Every entry in the audit log has the following structure:

```
DD.MM.YY hh:mm:ss [user] event data [returncode] <CR-LF>
```

The individual fields in this type of entry have the following meaning:

Field	*Meaning*
DD.MM.YY	Date on which the event occurred in day.month.year format. The date is taken from the CryptoServer's internal real time clock.
hh:mm:ss	Time at which the event occurred in hour:minute:second format. The time is taken from the CryptoServer's internal real time clock.
[user]	ID of the user who performed the action. However, if an "external" event occurs, i.e. alarm or restart, the user ID is missing.
event	Description of the event in a readable format
data	Additional information about the event in a readable format
[returncode]	Return value of the function that has been performed. A return value of 0 means that the function has been performed successfully. A return code other than 0 shows the returned error number.
<CR-LF>	Carriage return - line feed

Table 9: Meaning of the audit log entry fields

The square brackets […] displayed for `user` and `returncode` in the previous table do not mean that these fields are optional. In each case the relevant user ID or return code is effectively enclosed in square brackets.

2.19 Backing up, Restoring and Cloning Databases

If you are using version 2.30.2 or later of the SecurityServer package for the CryptoServer, the following functions are available in CAT:

- Store a copy of the CryptoServer databases on a computer (backup).
  For step-by-step instructions on how to prepare a backup of the CryptoServer databases, read chapter 5.10.
- Import a copy of the databases from a backup directory to the CryptoServer (restore).
  For step-by-step instructions on how to restore the CryptoServer databases, read chapter 5.11.
- Copy the databases from one CryptoServer and then import them to a different CryptoServer (clone).
  For step-by-step instructions on how to clone the CryptoServer databases, read chapter 5.12.

Before you can use these new functions, the following must be applied:

- Version 2.30.2 or later of a SecurityServer package must have been installed in the CryptoServer.
- The MBK must have been imported to the CryptoServer. The MBK is used to encrypt all the data that is stored outside of the CryptoServer.

If you want to transfer the databases from one CryptoServer to another (cloning), both these CryptoServer must have the same MBK.

2.20 The Cryptographic Interfaces

This section gives a brief introduction to the CryptoServer's most important cryptographic interfaces. The corresponding libraries for these interfaces are provided on the SecurityServer product CD.

2.20.1 Cryptographic eXtended Interface (CXI)

The Cryptographic eXtended Interface (CXI) is a proprietary interface developed by Utimaco IS GmbH. CXI provides all the CryptoServer cryptographic functions via a user-friendly interface which has a low protocol overhead and is easy to integrate into customer-specific applications.

You can use the Cryptographic User user to administer all the other cryptographic interfaces described later on in this chapter via this CXI interface. You can control all the other cryptographic interfaces and their functions within the CryptoServer via the CXI interface. In this respect the CXI interface plays a more prominent role than the other cryptographic interfaces.

In the CryptoServer itself, CXI functions are provided by the CXI firmware module which is a component of the SecurityServer firmware package. You can use the CAT administration program to create a Cryptographic User which functions both as a CXI user and as a user for all the other cryptographic interfaces. The CAT provides the appropriate permission profile for the Cryptographic User.

2.20.2 PKCS#11

PKCS#11 is the standard used to define a programming interface for security tokens such as smartcards or hardware security modules. From the PKCS#11 viewpoint, a security token is a device that stores objects and can perform cryptographic functions. These objects may be keys or certificates. In addition, the objects can each have different attributes which not only define how you handle them but may also limit the areas in which they can be used.

With version 3.20 and later of the SecurityServer/CryptoServer SDK product CD only the PKCS#11 R2 implementation is supplied for which a dedicated administration tool P11CAT and a separated manual are available.

The PKCS#11 functions in the CryptoServer are provided by the CXI firmware module which is also a part of the SecurityServer firmware package.

2.20.3 Microsoft CryptoAPI and Cryptography API: Next Generation (CNG)

Software developers can use the Microsoft cryptographic application programming interface (CryptoAPI) to call powerful cryptographic functions from their Windows-based applications. These functions are provided by what is known as the Cryptographic Service Provider (CSP).

The CryptoAPI contains all the functions necessary for encrypting and decrypting data (with both symmetrical and asymmetrical keys) and for using and managing digital certificates for authentication purposes.

Cryptography API: Next Generation (CNG) is Microsoft's latest cryptographic platform. In CNG the provider concept has been extended further than in CryptoAPI. CNG also supports newer cryptographic algorithms, for example elliptic curves. At present, both CryptoAPI and CNG are being supported, to enable existing applications to be upgraded step-by-step.

The CSP/CNG cryptographic interface is accessed via the CXI firmware module. Depending on the CryptoServer CSP version different configuration settings are necessary:

- For CryptoServer CSP 1.x provided on SecurityServer and CryptoServer SDK product CD up to 4.01, you do not need to set up a Cryptographic User for CSP/CNG on the CryptoServer. If you have installed the device or the machine via the Control panel applet, a user is created on the CryptoServer automatically. This machine, or the CSP/CNG user, has the same authentication status as the Cryptographic User in the CXI firmware module.

- For CryptoServer CSP 2.x provided on SecurityServer and CryptoServer SDK product CD version 4.10 and later, the CSP and CNG interfaces are configured via a dedicated configuration file, and a CSP/CNG user, with the same permissions as the Cryptographic User (min. 00000002) must be created manually.

The CryptoAPI and CNG functions are made available to the applications that call them by a CryptoServer Cryptographic Service Provider (CSP) which serves both these interfaces. Depending on the version of the SecurityServer and the CryptoServer SDK product CD, not only the CryptoServer CSP itself is provided, but also a control panel applet CSP Configuration or a dedicated configuration file, `cs_cng.cfg`, that can be used to configure the CSP/CNG cryptographic interface. Additionally, two key management tools are available: The GUI-based CSP tool for creating, editing and deleting key container and keys with CSP, and the command-line utility CNG tool for managing CNG cryptographic keys.

2.20.4 Java Cryptography Extension (JCE)

The Java Cryptography Extension (JCE) is a collection of Java packages that implement cryptographic procedures for Java applications. These include, among other things, encrypting and decrypting data and generating keys. These functions are made available by the JCE provider.

In the CryptoServer, these JCE functions are made available by the CXI firmware module which is a component of the SecurityServer firmware package. You can use the CAT administration tool to create a Cryptographic User that is also a user for JCE. The CAT provides the appropriate authorization profile for the Cryptographic User.

2.20.5 OpenSSL

OpenSSL is a free implementation of the SSL/TLS protocol for Open Source environments which also offers a range of more specialized functions for certificate management and for different cryptographic functions. These various different functions are grouped together in the OpenSSL command-line tool.

The integration of OpenSSL into the CryptoServer is done indirectly via an OpenSSL PKCS#11 wrapper. If you want to integrate OpenSSL indirectly via a PKCS#11 wrapper, use the PKCS#11 administration tool P11CAT to initialize a PCKS#11 token or slot.

2.20.6 Extensible Key Management (EKM)

An SQL Server provides functions for data encryption and EKM (Extensible Key Management). Here, the Microsoft Cryptography API service provider is used for encryption and key generation. Encryption keys for encrypting data and keys are created in temporary key containers, and must be exported by the service provider before they can be saved in the database.

This approach enables SQL Server to be used for key management with an encryption key hierarchy and key security.

In CryptoServer, the EKM functions are provided by the CXI firmware module which is an element of the SecurityServer firmware package.

Use the CAT administration program to create a Cryptographic User which is also a user for EKM. The CAT provides the appropriate authorization profile for the Cryptographic User.

2.21 Interface Hardening by Disabling Selected Functions

With release 4.0 of the SecurityServer/CryptoServer SDK product CD the CryptoServer offers the possibility to disable selected functions. The firmware functions to be disabled are defined in a custom signed configuration file `cmds.scf`. The configuration file is read and evaluated on every startup of the CryptoServer. If a function is listed in this configuration file, it is blocked. For detailed information about signed configuration files and their use read chapter "Signed Configuration Files" in the *CryptoServer Command-line Tool –csadm – Manual for System Administrators*. There you will also find a list of all firmware functions that can be disabled.

2.22 Clustering for Load Balancing and Failover

Several CryptoServer LANs can be organized in a cluster either for load balancing or for failover purposes.

Configured to support failover, the CryptoServer cluster ensures high system availability and reliability.

In a load balancing cluster CryptoServer LAN devices are configured to optimize the use of resources to reach higher system performance, and to avoid overloading a single device. A load balancing cluster also implicitly offers high availability in case some CryptoServer in the cluster fails, yet at the cost of reduced system performance compared to the performance of a fully functional cluster.

2.22.1 Concept Overview

Load Balancing

Load balancing defines the ability to distribute connections over several CryptoServer LANs which are all active (rather than one active and the others passive).

All CryptoServer LANs in the cluster must be configured identically. Connections are established by the client-side software based on the "Least Connections" principle, i.e. a new connection is opened on the CryptoServer LAN with the least number of existing connections. For example, let us assume that each of the N CryptoServer LANs as shown in the figure

below has currently exactly one open connection (Connection 1 to N). When later on connection 2 is closed and subsequently the connection N+1 should be established, this connection will be opened on the CryptoServer LAN 2, which has the least number of connections at that time, namely no connections at all.

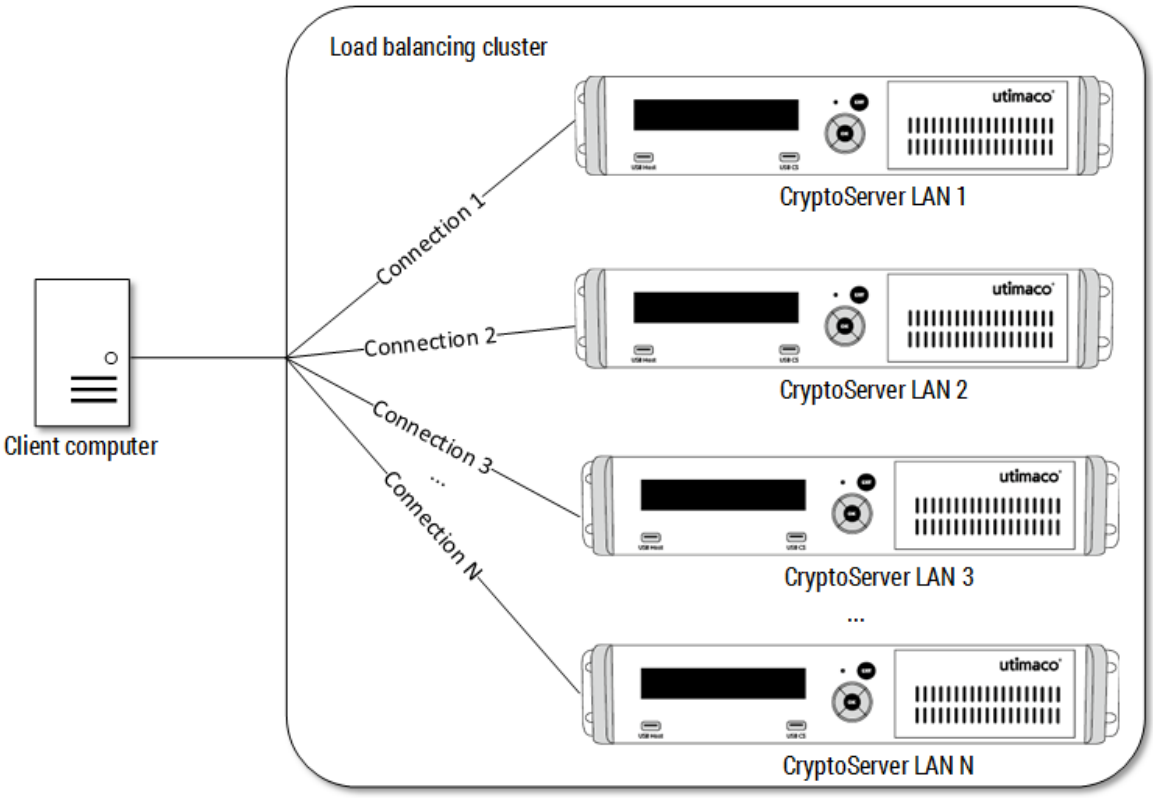


Figure 5: Example of a load balancing cluster with N CryptoServer LANs

Load balancing has been tested with clusters of four CryptoServer LANs. This is not due to limitations of CryptoServer or load balancing functionality. You may build clusters with more than four CryptoServer without any concerns.

Currently, load balancing is only supported by the CXI and PKCS#11 interfaces of the CryptoServer Se- and CSe- Series.

Failover

Failover defines the ability to automatically switch processing to a redundant or standby unit in a cluster, i.e. only the primary CryptoServer is active while other cluster members are passive. Usually, a cluster of two CryptoServer LANs is deployed as a failover solution (see the

figure below). When the primary CryptoServer LAN fails, the active connection(s) is (are) automatically routed to the passive CryptoServer LAN which continues to operate in the same manner as the failed device. The failover mechanism tries to re-connect to the primary CryptoServer in regular time intervals (fallback interval). In this context the primary CryptoServer can be the same device as before and which has become operable again; or it can be a passive CryptoServer which is used as a replacement for the defect primary CryptoServer. On success the connections are switched back to the primary CryptoServer resp. transferred to the passive CryptoServer.

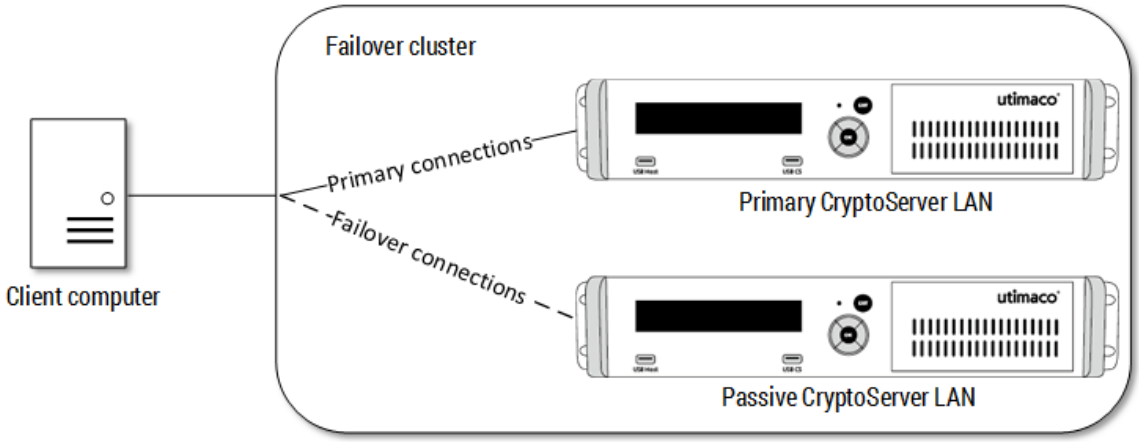


Figure 6: Example for a failover cluster with two CryptoServer LANs

A cluster of more than two CryptoServer LAN appliances can be also deployed as a failover solution.

When choosing the fallback interval suitable for your system environment consider the following aspects to minimize the downtime of your failover cluster:

- If the passive CryptoServer LAN is available and pre-configured (identically to the primary CryptoServer LAN) in the same rack or in the local network, and just has to be switched on to be ready for use, a fallback interval of few minutes might be reasonable.
- If the passive CryptoServer LAN is locally available, but not in the same rack, and has to be configured identically to the primary CryptoServer LAN before connections can be rerouted to it, a fallback interval of few hours might be reasonable.
- If the passive CryptoServer is not locally available, can be delivered per express delivery and has to be configured identically to the primary CryptoServer before connections can be rerouted to it, a fallback interval of few days might be reasonable.
- If the primary CryptoServer has to be send back to the manufacturer Utimaco per RMA request, and no passive CryptoServer is available, a fallback interval of several days might be reasonable.

The use of CryptoServer PCIe plug-in cards is only of limited use since normally for the replacement of a defect CryptoServer PCIe plug-in card the host computer must be shut down, and therefore the application and the CryptoServer cluster are completely out of operation.

Error Handling

Error-handling mechanisms for load balancing and failover are designed to minimize the possibility of disrupting the service availability of the CryptoServer cluster. The load balancing and failover mechanisms react to errors in a similar way:

- If an error indicates that the execution of the failed command might succeed on another device, e.g. in case of a timeout error, then a connection to the next CryptoServer is established, and the command is sent to that CryptoServer.
- If an error indicates that the execution of the failed command most likely will not succeed on another CryptoServer either, an error message is returned to the requesting application. This would be the case, e.g., if a key could not be found. The existing connection remains.

If a connection to a CryptoServer cannot be established, or a connection breaks and cannot be re-established, or any other error or problem dealing with load balancing and failover mechanism occurs, it is reported in the audit log.

2.22.2 Preconditions

Before you start configuring and using the load balancing and failover features make sure that the following requirements are fulfilled for the CryptoServer devices which should belong to the same cluster.

Mandatory Preconditions

- Make sure that all CryptoServer are accessible for the client computer to the same network.
- You have loaded exactly the same firmware modules (versions and functionality in case of self-developed firmware modules) into all devices.
- You have loaded the same MBK into all CryptoServer in the cluster.
  Read chapter 5.8 of this manual for detailed information. In case you prefer using the command-line administration tool csadm, read the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*.
- You have synchronized the user databases of all CryptoServer in the cluster, i. e. the same user account(s) and user credentials (password, keyfile, attributes) required for

authentication/Secure Messaging are available on every CryptoServer LAN in the cluster. You find detailed information on how to create users, backup and restore a user database with CAT in chapter 5.7 of this document. In case you prefer using the command-line administration tool csadm, read the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*.

The usage of keys stored on smartcards for user authentication on CryptoServer devices organized in a cluster is not supported.

Consider to synchronize user accounts between all CryptoServer in a cluster after creation of new users, deletion of existing user accounts as well as any changes on existing user accounts on a CryptoServer in the cluster.

- If an internal key storage is used, you have synchronized all keys between all CryptoServer in the cluster, e.g., by using the CryptoServer's backup and restore functions as described in Chapter 5.10, 5.11, and 5.12. In case you prefer using the command-line administration tool csadm, read the *CryptoServer Command-line Administration Tool - csadm - Manual for System Administrators*.

When using internal key storage, and keys are created, deleted or modified by the application accessing the cluster, these changes must be synchronized between all CryptoServer in the cluster using some mechanisms external to the load balancing/failover implementation.

Optional Preconditions

- The time in all CryptoServer belonging to the CryptoServer cluster is synchronized by using NTP.
- The audit log configuration file is synchronized between all devices in the cluster.

2.22.3 Use of External and Internal Key Storage

The load balancing and failover mechanisms support both internal and external key storage.

- Internal key storage
  All keys are stored in the key database, `CXIKEY.db`, inside the CryptoServer.

The load balancing and failover implementation does not provide an integrated key replication algorithm for internal key storage.

Do not create any new objects (keys or users) while using load balancing or failover with internal key storage. To create additional objects, disable load balancing/failover in the corresponding configuration file, create the new objects, replicate the information on all devices in the cluster, and enable load balancing/failover in the configuration file again.

- External key storage
  All keys are stored in a database outside the CryptoServer

The following table gives an overview of the advantages and disadvantages to be considered when you decide to use either internal or external key storage in combination with load balancing or failover.

Key Storage	*Advantages*	*Disadvantages*
Internal	■ High security level since all keys are stored inside the CryptoServer, i.e., additional protection by the HSM sensory, authenticated access ■ High performance	■ Manual key synchronization between all cluster members is required ■ Limited number of keys (several thousands, depending on the key size)
External	■ No manual key synchronization between cluster members is required ■ High security level due to MBK (AES-256) protection of the external key storage	■ Slightly lower performance than internal key storage

Table 10: Internal/External key storage – advantages and disadvantages

2.22.4 Configuration Settings

Currently, the load balancing mechanism is available only for the PKCS#11 API and for the C++ interface of the CXI API. The failover mechanism is provided for the PKCS#11 API and for both C++ and Java interfaces of the CXI API.

Configuration Settings for the Use with CXI

- For detailed information on how to configure failover and load balancing for the C++ interface of the CXI API, read the HTML documentation provided on the SecurityServer product CD under `…\Documentation\Crypto_APIs\CXI`.
- For detailed information on how to configure failover for the Java interface of the CXI API, read the HTML documentation provided on the SecurityServer product CD under `…\Documentation\Crypto_APIs\CXI_Java`.

Configuration Settings for the Use with PKCS#11

Before you can use load balancing and failover in your PKCS#11 environment some settings in the configuration file `cs_pkcs11_R2.cfg` are required. For details, read the *PKSC#11 Developer Guide* provided on the SecurityServer product CD in the folder `…\Documentation\Crypto_APIs\PKCS11_R2\`.

2.23 Deliverables

The individual device key

An individual device key has already been generated and then stored in the CryptoServer.

As none of the options for administering this key are present, even Utimaco IS GmbH cannot know the key value. You can decide whether you want to keep this individual device key as it is, or completely reset the CryptoServer to generate a new individual device key.

ADMIN, the default administrator

The default administrator ADMIN has already been set up on the CryptoServer. He has the permission 2 in the user groups 7 and 6 (22000000).

The authentication with electronic signature procedure has already been defined as the authentication procedure for the default administrator ADMIN. The RSA algorithm is used as the cryptographic algorithm here. The public part of the RSA key has already been loaded into the CryptoServer's user database as authentication data.

You will find the private part of the RSA key, which is needed for authentication, on the product CD. It is the `ADMIN.key` keyfile in the following folder:

`Software\All_Supported_Operating_Systems\Administration\key`

You do not need a password to open the file.

You will also find the private part of the RSA key on any smartcard that you have received as part of the standard deliverables or as a result of an additional order.

To use the private RSA key from the smartcard, you must enter the PIN `123456`.

Serial numbers and descriptors

Every CryptoServer has a number of serial numbers that identify component parts. Some of these serial numbers will be displayed on the CryptoServer. This status information and additional descriptors are displayed when the CryptoServer's status is queried or called.

All the serial numbers and descriptors have already been loaded and stored on the device when the CryptoServer is supplied.

3 Installing the CryptoServer Host Software

In this chapter we describe how you install the software you need to run the CryptoServer on a host computer with Windows and Unix/Linux operating systems. This includes:

- The CryptoServer administration tools already mentioned above, csadm and CAT. These tools can be used to administer both the CryptoServer PCIe and the CryptoServer LAN.
- The CryptoServer Crypto APIs (JCE, CXI, CSP/CNG, PKCS#11)
- The CryptoServer simulator
- The complete documentation of the CryptoServer and the CryptoServer LAN appliance.

Before you install the software for administering the CryptoServer, you first have to carry out a few preparations.

3.1 System Requirements

- CPU: Intel x86/x64, AMD x86/x86-64
- Hard disk capacity: at least 120 Mbit
- RAM: more than 12 Mbit
- A free PCIe expansion slot, if you are using a CryptoServer PCIe Se-Series, CSe-Series or Se-Series Gen2
- Network card: Ethernet 10/100/1000 Mbit/s for the connection to the CryptoServer LAN
- Operating systems:
  You find the current and complete list of supported operating systems in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` on the SecurityServer/CryptoServer SDK product CD in the folder `…\Documentation\Product Details`.
- CD-ROM disc drive
- Current Java versions for Windows/Linux

3.2 Prepare for Installation

If you are using a CryptoServer LAN, you must first have integrated this into your network. In addition, you must have assigned an IP address for this device. You can find detailed instructions on how to bring your CryptoServer LAN into service in the *CryptoServer LAN V4 Operating Manual* provided on the SecurityServer product CD.

If you are using a CryptoServer plug-in card, you must already have installed this along with the corresponding driver.

The following manuals describe how to install the driver for the plug-in card:

- *CryptoServer PCIe - Operating Manual – CSe-Series*
- *CryptoServer PCIe - Operating Manual – Se-Series*
- *CryptoServer PCIe - Operating Manual – Se-Series Gen2*

3.3 Performing the Installation for Windows

This chapter describes how to install the CryptoServer host software on a computer that is running a Windows operating system.

The CryptoServer host software and the CryptoServer Simulator support the operating systems listed in the document `CS_PD_SecurityServer_SupportedPlatforms.pdf` provided on the SecurityServer/CryptoServer SDK product CD in the folder `…\Documentation\Product Details`.

Before you start the installation, check that you have installed the current version of the Java SE Runtime Environment on your computer. We recommend you uninstall the old version of the Java SE Runtime Environment from your computer first. Restart your computer before you install the current version of the Java SE Runtime Environment.

3.3.1 Installing the Host Software and CryptoServer Simulator

To install the CryptoServer software, perform the following steps

1. Insert the product CD in the computer's CD-ROM drive.
2. If the installation does not start automatically, double-click the file `CryptoServerSetup-<version number>.exe`.
   The installation wizard starts. The **Welcome to the CryptoServer Setup Wizard** dialog box opens.

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

3. Click the **Next >** button.
   The **Select Destination Location** dialog box opens.
4. Use the **Browse…** button to select a different directory for installing the software or confirm the default installation directory.

5. Click **Next >**.
   The **Select Components** dialog box opens.
6. Select the components you want to install. By default, the **CryptoServer Administration Tools** and **CryptoServer Documentation** are selected.

To install the CryptoServer simulator for Windows, select the corresponding check box here.

7. Click **Next >** to continue the installation process.
   The **Select Start Menu Folder** dialog box opens. Here you can select the directory in which the shortcut used to start the program is to be stored.
8. Confirm the default directory or click the **Browse** button to change the folder for the shortcut.

*If you click **Don't create a Start Menu folder**, no shortcut is created in the Windows **Start** menu.*

9. To continue with the installation, click the **Next >** button.
   The **Select Additional Tasks** dialog box opens. Here you can decide whether to create a desktop icon or not. By default, **Create a desktop icon** is selected.
10. Click **Next >**.
    The **Ready to Install** dialog box opens. Here you can see what you have selected or specified in the previous dialog boxes.
11. Click the **Install** button to start the installation of the software.

During installation a special setup window opens in which you are prompted to download the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from the Oracle web site. These files are required to work with the Utimaco CryptoServer JCE Provider.

12. To use the JCE interface, click the **Yes** button in the **Setup** window.
    The system continues the installation.

    After completing the installation, the **Completing the CryptoServer Setup Wizard** dialog box opens. Here you can specify whether the CAT should be launched automatically after

successful software installation. By default, the option **Launch CryptoServer Administration** is selected.

13. Click the **Finish** button to complete the software installation.

You have now finished installing the CryptoServer software. CAT starts now by default and the **Settings** dialog box is displayed.

3.3.2 Using the CryptoServer Simulator

To use the CryptoServer Simulator on a host computer running a Windows operating system, proceed as follows:

1. Start the CryptoServer Simulator:
   - By using the Windows **Start** menu and clicking **Start** > **All Programs** > **Utimaco** > **CryptoServer** > **CryptoServer Simulator**
   - By double-clicking the desktop icon for the CryptoServer Simulator shown to the right. The desktop icon is available if you kept the default setting for desktop links during the installation of the host software.

   - By using a command prompt window:

     a) Open a command prompt in the product CD installation folder for the CryptoServer Simulator
     `<product CD installation folder>\Simulator\sim5_windows\bin`.
     b) Type `cs_sim.bat` and press ENTER.
     Alternatively, type `bl_sim5.exe -h -o` and press ENTER.

   This starts the **Utimaco CryptoServer SDK5 – Simulator** command-line application. Do not close this application until you have finished using the simulator.

2. Double-click the **CryptoServer Administration** desktop icon to start the CAT. The CAT main window opens.
3. In the toolbar, click **Devices**.
   This opens the **CryptoServer Devices** dialog box.
4. Enter the address `3001@127.0.0.1` in the **New Device** text box.
5. Click the **Add to List** button.
6. Click the **Test** button to check whether a connection can be established. The test result is displayed in a separate window.
7. Click **OK** to close this window.
8. Close the dialog box CryptoServer Devices by using the **Close** button.

The successfully established connection is now confirmed in the info field of the CAT main window. Furthermore, information about the date and time as well as the current status of the CryptoServer Simulator is displayed.

You can use the CryptoServer Simulator as described in the sections that follow this one.

3.3.3 Starting Multiple CryptoServer Simulator Instances

As from SecurityServer 4.01 the simultaneous start and use of multiple CryptoServer Simulator instances is possible. This might be very useful, for example, if you want to configure and simulate your own CryptoServer load balancing cluster for evaluation and test purposes.

Prerequisites:

You have installed the CryptoServer host software provided on the SecurityServer/CryptoServer SDK product CD 4.01 and later as described in chapter 3.3.1.

Proceed as follows:

1. Start the CryptoServer Simulator as described in step 1 of Chapter 3.3.2, “Using the CryptoServer Simulator”.
2. Configure it according to your individual requirements, for example, create specific users as explained in Chapter 5.7.1, “Creating a User”.
3. Close the CryptoServer Simulator after you have finished the configuration.
4. Open a command prompt window.
5. Change to the CryptoServer product CD installation folder:

```
cd <product CD installation>\Software\Windows\Simulator\sim5_windows\bin
```

6. Start, for example, three CryptoServer Simulator instances by typing `cs_multi.bat 3` and pressing ENTER.

   Three identically configured CryptoServer Simulator instances are started. They have the following device addresses:

   - First instance – 3001@localhost
   - Second instance – 3003@localhost
   - Third instance – 3005@localhost

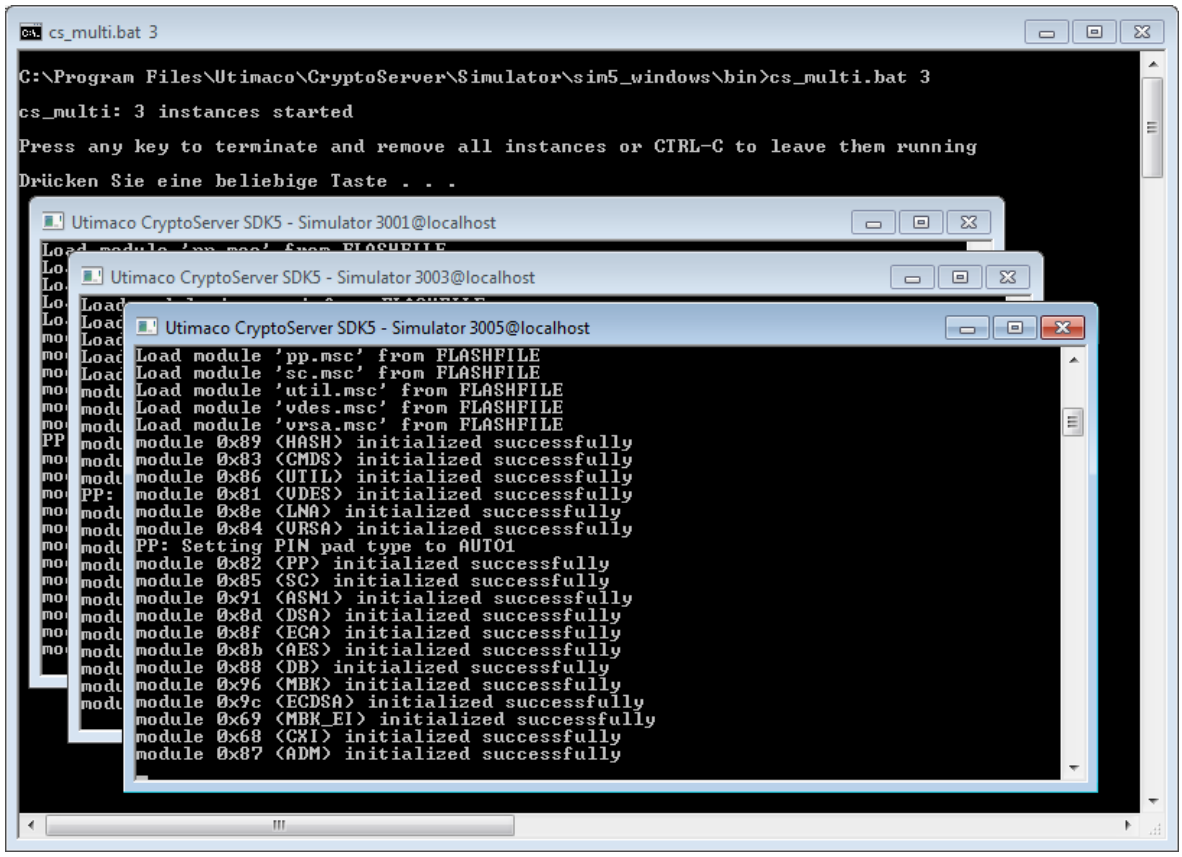


Figure 7: Example for running three CryptoServer Simulator (Windows) instances simultaneously

To close all CryptoServer Simulator instances, change to the command prompt window and press any key. When the instances are closed, all your changes are lost. The next time you start multiple CryptoServer Simulator instances they will have the same configuration as the one you have previously configured in step 2.

3.3.4 Setting up Java Cryptography Extension (JCE) for Windows

If you want to use the JCE interface you need the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

Download the appropriate Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the Java version installed on your computer.

Before you download the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files, check which Java version is installed on your computer by typing java –version in a terminal.

1. Load the appropriate ZIP file `jce_policy-x.zip` onto your computer.
2. Extract `jce_policy-x.zip` on your computer.

   From the `jce_policy-x.zip` file you require the following files:

   - `local_policy.jar`
   - `US_export_policy.jar`
3. Copy them into the following folder:
   `C:\Program Files\Java\jrex\lib\security`

   This completes the installation of the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

3.3.5 Installing the PIN Pad Driver

To be able to use the delivered PIN pad for the CryptoServer administration, the appropriate driver, provided by Utimaco, must be manually installed on the host computer where the host software has already been installed.

Prerequisites:

- You have uninstalled any previous PIN pad driver versions on the host computer.

In case the PIN pad REINER SCT cyberJack (as shown in Figure 1, chapter 2.2.2) was delivered to you and there is a version of Utimaco's USB PIN pad driver already installed on the host computer and listed in the Windows Device Manager as LibUSB Devices, then no driver update or new driver installation is required.

- You have inserted the delivered product CD in the computer's CD-ROM drive.

Under no circumstances install the "Base components" USB driver for Windows from the company REINER SCT.
If your Windows operating system already has REINER SCT's "Base Components" driver installed, it is essential that you remove it before you install the Utimaco IS GmbH driver. The official REINER SCT "Base Components" driver and the driver from Utimaco IS GmbH cannot be used in parallel.

Under no circumstances run the "cyberJack Device Manager" from the REINER SCT Base components, and perform a firmware update of the PIN pad driver.
Installing a firmware update on the PIN pad renders this PIN pad unusable with CryptoServer administration tools and cryptographic libraries. After a firmware update, it is not possible to revert to the PIN pad firmware as shipped by Utimaco.

1. Connect the USB plug of the PIN pad with the host computer.

   You are prompted in a separate dialog box to download the PIN pad driver from the Internet or to let Windows install it automatically.
2. Close this dialog box without selecting any of these options.
3. Double click the **Other Devices** entry in the displayed list.
4. Depending on the PIN pad you are using, proceed as follows:
   - If the REINERSCT cyberJack PIN pad shown in Figure 1 has been supplied to you, double-click **cyberJack e-com(a)**.
   - If the Utimaco cyberJack One PIN pad shown in Figure 2 has been supplied to you, double-click **cyberJack ONE**.

   The **<PIN pad type> Properties** dialog box opens.
5. Click the **Update Driver** button.
6. The **Update Driver Software - <PIN pad type>** dialog box opens.
7. Click **Browse my computer for driver software**.
8. In the dialog box that opened, click **Browse** and select the PIN pad driver provided on the product CD.

   You find the driver software on the product CD delivered by the Utimaco IS GmbH here:
   - For a 32-bit system:
     `\Software\Windows\x86-32\Tools\cyberJack\Driver\`
   - For a 64-bit system:
     `\Software\Windows\x86-64\Tools\cyberJack\Driver\`
9. Click **Next**.
10. Confirm the **Windows Security** warning with **Install**.

    The PIN pad driver is now being installed. When completed, the successful driver installation is confirmed in a separate dialog box.
11. Click **Close** to close the installation confirmation dialog box.
12. Click **Close** to close the **<PIN pad type> Properties** dialog box.

The USB PIN pad is now displayed with its name – cyberJack e-com(a) or cyberJack ONE - in the Windows Device Manager as a subentry of the Universal Serial Bus devices entry.

3.4 Performing the Installation for Linux

This chapter describes how to install the CryptoServer host software on a computer that is running a Linux operating system.

3.4.1 Installing csadm

To install csadm, follow these steps:

1. If there is no `~/bin` folder present on your system, create it in your user directory:

```
mkdir ~/bin
```

2. Copy the csadm relevant for your operating system (32-bit or 64-bit) into the `~/bin` folder.

   An example for Linux 64-bit:

```
cp <mount point of the product CD>/Software/Linux/x86-64/Administration/csadm ~/bin
```

3. Add the `~/bin` folder to the path in the user configuration file in the shell that is being used.

   In our example we have used a bash as the shell:

4. Open the `~/.bashrc` file, and then add the following line to it:

```
export PATH=$PATH:~/bin
```

5. Save the changes and close the `~/.bashrc` file.

3.4.2 Installing CAT

CAT can be used on Linux 32-bit and 64-bit systems.

To be able to use the CAT, install first the appropriate Sun Java Runtime Environment for the Java version available on your computer. Use the package manager for your Unix/Linux system to install the Oracle Java Runtime Environment.

To install the CAT, follow these steps:

1. Copy the `cat.jar` file into your user directory.

```
cp <path to the Product
CD>/Software/All_Supported_Operating_Systems/Administration/cat.jar ~/
```

2. Start CAT with the following command:

```
java -jar ~/cat.jar
```

3.4.3 Installing and Using the CryptoServer Simulator

The CryptoServer Simulator supports the following Linux (32-bit and 64-bit) operating systems:

- Red Hat Enterprise Linux 6.4/6.5/6.6/7.0/7.1/7.2
- SUSE Linux Enterprise Server (SLES) 11
- Debian 7 "Wheezy" and Debian 8 "Jessie"

Prerequisites:

If you are using a 64-bit Linux operating system, you must have installed `gcc-multilib` on it. To perform the installation, you need `root` permissions.

Operating system	*Installation command*
Debian 8	`apt-get install gcc-multilib`
SLES/openSUSE	`zypper install glibc-32bit`
RHEL/CentOS	`yum install glibc.i686 glibc-devel.i686 libstdc++-devel.i686`

Table 11: Examples for installing the gcc-multilib

Installation and Execution

To install the CryptoServer Simulator, proceed as follows:

1. Create a new directory in your `home` directory, for example:

```
mkdir -p ~/Utimaco/CryptoServer/Simulator
```

2. Copy the CryptoServer Simulator files provided on the SecurityServer product CD to the new directory.

```
cp -r /<mount point of SecurityServer product CD>/Software/Linux/Simulator/*
~/Utimaco/CryptoServer/Simulator
```

3. Define the environment variable `CRYPTOSERVER` which is needed for the use of the CryptoServer Simulator:

```
export CRYPTOSERVER=3001@localhost
```

Add this command to your ~/.bashrc, ~/.profile or ~/.zshrc according to your shell to call it automatically.

4. Change the permission for the CryptoServer Simulator executable `bl_sim5` and for the script `cs_sim.sh`, provided on the product CD, to allow the files to be executed.

```
cd ~/Utimaco/CryptoServer/Simulator/sim5_linux/bin
chmod +x bl_sim5 cs_sim.sh
```

5. Start the CryptoServer Simulator:

```
~/Utimaco/CryptoServer/Simulator/sim5_linux/bin/cs_sim.sh
```

This starts the Utimaco CryptoServer SDK5 – Simulator command-line application. Do not close this application until you have finished using the simulator.

3.4.4 Starting Multiple CryptoServer Simulator Instances

As from SecurityServer 4.01 the simultaneous start and use of multiple CryptoServer Simulator instances is possible. This might be very useful, for example, if you want to configure and simulate your own CryptoServer load balancing cluster for evaluation and test purposes.

Prerequisites:

You have installed the CryptoServer Simulator for Linux provided on the SecurityServer/CryptoServer SDK product CD 4.01 and later as described in chapter 3.4.3.

Proceed as follows:

1. Start the CryptoServer Simulator as described in step 5 of Chapter 3.4.3, “Installing and Using the CryptoServer Simulator”.
2. Configure it according to your individual requirements, for example, create specific users as explained in Chapter 5.7.1, “Creating a User”.
3. Close the CryptoServer Simulator after you have finished the configuration.
4. Open a terminal.
5. Change to the CryptoServer product CD installation folder:
   `<product CD>\Software\Linux\Simulator\sim5_linux\bin`
6. Start, for example, three CryptoServer Simulator instances by typing `cs_multi.sh 3` and pressing ENTER.

   Three identically configured CryptoServer Simulator instances are started. They have the following device addresses:

   - First instance – 3001@localhost

- Second instance – 3003@localhost
- Third instance – 3005@localhost

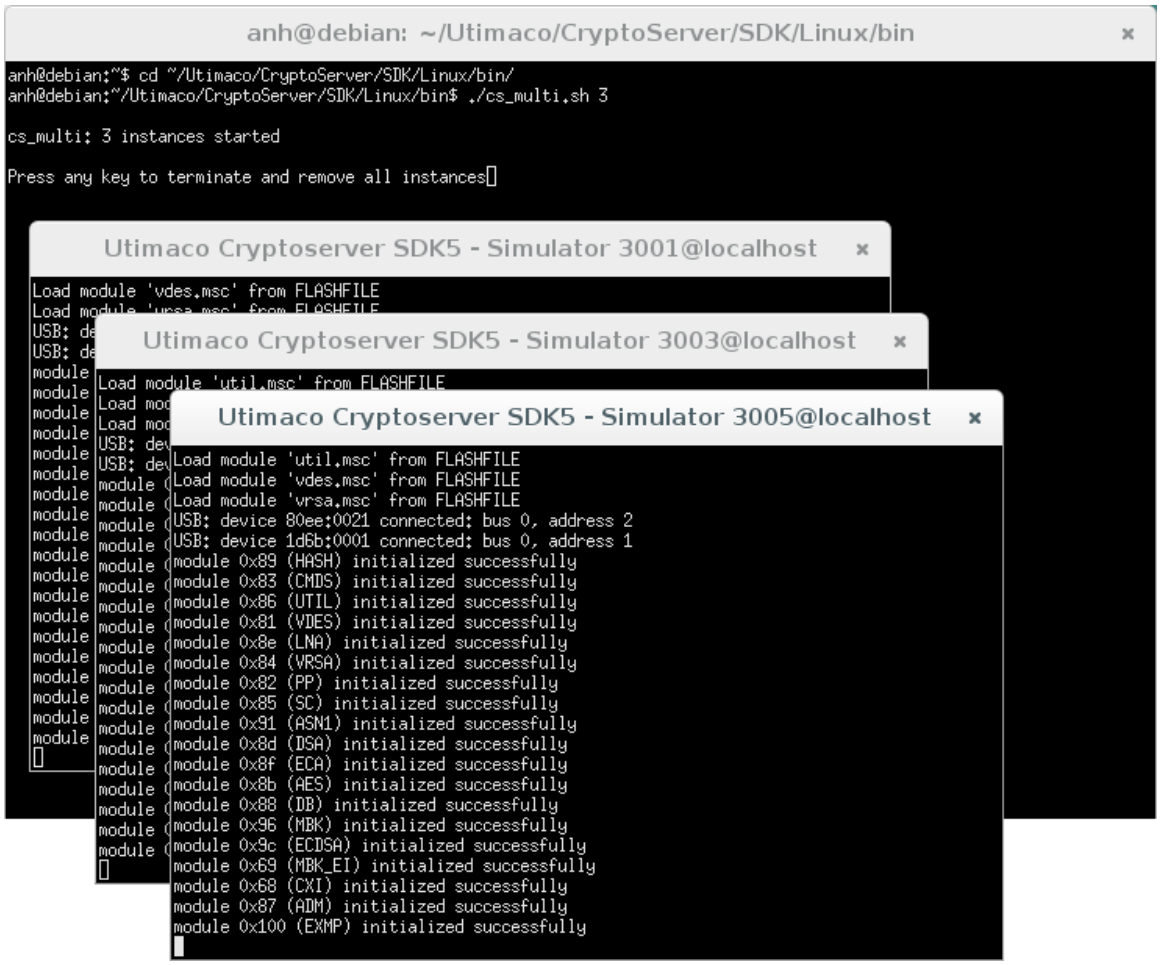


Figure 8: Example for running three CryptoServer Simulator (Linux) instances simultaneously

To close all instances, press any key in the terminal. When the instances are closed, all your changes will be lost. Next time you start multiple CryptoServer Simulator instances they will have the same configuration as the one you have previously configured in step 2.

3.4.5 Setting up Java Cryptography Extension (JCE) for Linux

If you want to use the JCE interface, you need the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files that can be downloaded from the Oracle website. These files are required for working with the Utimaco's CryptoServer JCE Provider.

Check the Java version installed on your computer before you start downloading the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

1. Load the appropriate ZIP file `jce_policy-x.zip` onto your computer.
2. Extract `jce_policy-x.zip` on your computer.

   From the `jce_policy-x.zip` file you require the following files:

   - `local_policy.jar`
   - `US_export_policy.jar`

   The following example shows the path for Java 6 on a computer with a Linux operating system and 64-bit architecture.

   ```
   /usr/lib/jvm/java-6-openjdk-amd64/jre/lib/security/US_export_policy.jar
   /usr/lib/jvm/java-6-openjdk-amd64/jre/lib/security/local_policy.jar
   ```

3. Copy the policy files shown above to the appropriate folder on your Linux system.

3.4.6 Configuring the PIN Pad

There is no PIN pad driver installation required for host computers with a Linux operating system. However, for using an USB PIN pad delivered by Utimaco on a Linux host computer, the definition of a special udev rule is necessary.

- For using the REINERSCT cyberJack PIN pad (see Figure 1 in chapter 2.2.2):

```
echo 'SUBSYSTEM=="usb", ATTRS{idVendor}=="0c4b", ATTR{idProduct}=="0400",
MODE="666" > /lib/udev/rules.d/z80_cyberjack.rules
```

- For using the Utimaco cyberJack One PIN pad (see Figure 2 in chapter 2.2.2):

```
echo 'SUBSYSTEM=="usb", ATTRS{idVendor}=="0c4b", ATTR{idProduct}=="0600",
MODE="666" > /lib/udev/rules.d/z80_cyberjack.rules
```

- For using both PIN pads:

```
echo 'SUBSYSTEM=="usb", ATTRS{idVendor}=="0c4b", MODE="666" >
/lib/udev/rules.d/z80_cyberjack.rules
```

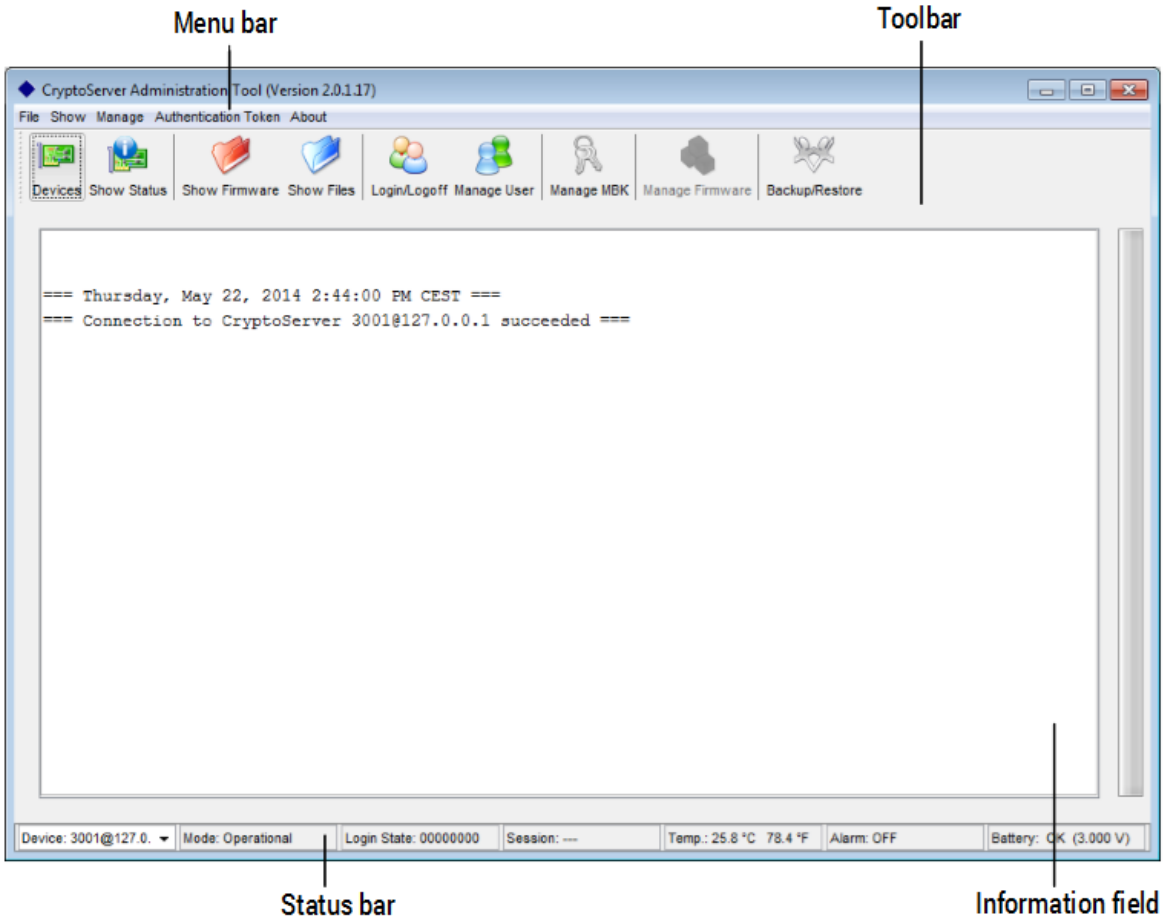
2

4 Administering the CryptoServer with CAT

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

4.1 CAT - Overview of the Graphical User Interface (GUI)

In the following you get an overview of the GUI elements in CAT and their meaning.



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 enables you to access all functions for CryptoServer administration.

- Toolbar

  The toolbar is located under the menu bar. It makes it possible for you to quickly access the most often used administration functions of CAT, like for example, setting up a new

device, getting the current CryptoServer status, the 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 you can retrieve by clicking Show on the menu bar, as well as by using the buttons Show Status, Show Files, Show Firmware in the toolbar.

- Status bar

  The status bar is located on the bottom border of the CAT main window.

  Here you can select the device you want to administer by using the combo box Device at the left window border.

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

  - Operating Mode (Mode:)

    If the CryptoServer is running correctly, and is ready for use, you will see Operational here.

  - Current authentication status (Login State:)

    This displays the current login 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 is displayed here. In this case, you would see authentication status 42000000.

  - Current remaining time until the existing Secure Messaging session is terminated (Session:)

    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 the 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.

  - Current temperature of the CryptoServer in °C and in °F (Temp.:)

- Alarm state (**Alarm:**)

  This shows whether an alarm is present. You see either **OFF** if no alarm has been triggered or **ON** if an alarm has occurred.

- Status of the CryptoServer Carrier Battery (**Battery:**)

  The status and the power of the carrier battery (in V) is displayed here. The status can be either **OK** or **LOW**. If you see the status **LOW**, this means the carrier battery is in a critical state. If you are running the CryptoServer in 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 the data from the CryptoServer.

4.2 Setting Up a New Device

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

CAT versions 2.1.0.0 and later do not support administration of the CryptoServer CS-Series (CS2000 and CS Classic). Use the CAT version 2.1.0.0 or earlier to administer those CryptoServer series.

To set up a new device in CAT, proceed as follows:

1. Start CAT.
2. Click the **Devices** button in the toolbar.
   The dialog box **CryptoServer Devices** opens.

*CAT starts automatically after finishing the installation of the CryptoServer host software provided on the SecurityServer product CD, and the dialog box **CryptoServer Devices** opens. You have to enter the address of the device you want to administer in this dialog box.*

3. Enter the address of the device you want to use in the **New Device** text box.

   Possible address entries:

Device	*Entry*
CryptoServer PCIe plug-in card integrated in the host computer where CAT is installed.	PCI:0
CryptoServer LAN	IP address of CryptoServer LAN
CryptoServer Simulator	3001@127.0.0.1

Table 12: Possible device address entries

If you are going to use a CryptoServer LAN, first configure the CryptoServer LAN's IP address and the IP address of the default gateway with the menu control options on the front panel of the CryptoServer LAN. For step-by-step instructions consult the CryptoServer LAN Quick Start Guide or the CryptoServer LAN Manual for System Administrators.
From CSLANOS version 4.2.0 and later the Internet Protocols IPv4 and IPv6 are supported.

4. Click the Add to List button to confirm the entry.
5. Click the Test button 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 to close the CryptoServer Devices dialog box.

If the connection has been established successfully, this is confirmed in the information field of the CAT main window. Additionally, information about the date and the time of connection is displayed.

4.3 Switching between Devices

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

CAT versions 2.1.0.0 and later do not support administration of the CryptoServer CS-Series (CS2000 and CS Classic). Use the CAT version 2.1.0.0 or earlier to administer those CryptoServer series.

4.4 Setting up a PIN Pad under Windows

Once you have configured the device address of your CryptoServer in CAT (see chapter 4.2), connected the supplied PIN pad to the host computer and installed the PIN pad driver as described in chapter 3.3.5, you have to set up the PIN pad in CAT. Proceed as follows:

1. Click the **File** menu and select **Settings**.
   This opens the **Settings** dialog box.
2. 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, you can select here alternatively the option corresponding to the name of your PIN pad: REINERSCT cyberJack (shown in Figure 1) or Utimaco cyberJack One (shown in Figure 2).

3. Select the **Port** to which you have connected the PIN pad. By default, **USB Port** is selected.
4. Click **OK** to confirm your selection and then click the **Timeout** tab.
5. Here is where you 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.
6. Once you have finished editing the data in the **Settings** dialog box, click **OK**.
   The settings you have made are saved.

4.5 Setting up a PIN Pad under Linux

Once you have configured the device address of your CryptoServer in CAT, connected the supplied PIN pad to the host computer and configured the required udev rule as described in chapter 3.4.6, you have to set up the PIN pad in CAT. Proceed as follows:

1. Click the **File** menu and select **Settings**.
   This opens the **Settings** dialog box. By default, the **PIN pad** tab is displayed.
2. Select **Autodetection** in the **Type** box.
   The PIN pad is automatically detected by the CryptoServer.

In case the PIN pad could not be recognized automatically by the CryptoServer, you can select here alternatively the option corresponding to the name of your PIN pad: REINERSCT cyberJack (shown in Figure 1) or Utimaco cyberJack One (shown in Figure 2).

3. Select the **Port** to which you have connected the PIN pad. By default, **USB Port** is selected.
4. Click **OK** to confirm your selection and then click the **Timeout** tab.
5. Here is where you 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.
6. Once you have finished editing the data in the **Settings** dialog box, click **OK**.
   The settings you have made are saved.

4.6 User Login

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.

To log in to the CryptoServer, proceed as follows:

1. Start CAT.
2. Click the **Login/Logoff** button in the toolbar.
   The **Login/Logoff User** dialog box opens. It contains a list of all users created by you and the default user ADMIN.
3. Select the user you require (e.g. ADMIN) and click the **Login** button.
   The dialog box **Choose User Token for Login** opens.
4. Select the appropriate authentication mechanism.

   - **Smartcard Token**
     If the user is using an RSA or an ECDSA authentication key stored on a smartcard, click **Smartcard Token** and then click **OK** in the **Choose User Token for Login** dialog box. Follow the instructions on the PIN pad.
   - **Keyfile Token**
     If the user is using an RSA or ECDSA authentication key stored in a keyfile, click **Keyfile Token**, and proceed as follows:

     c) Click the search button next to the **Key Path** text box.
     The **Set Name and Path for User Keyfile Token** dialog box opens.

d) Select the keyfile you require, e.g., `ADMIN.key`.
e) Click **Open**.
f) In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.

5. Click **OK** in the **Choose User Token for Login** dialog box.
The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.

4.7 Setting the Time in the CryptoServer

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.

You can set the time shown by the RTC in the CryptoServer.

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 by you and default users (e.g., ADMIN).
3. Select the user you require (e.g., ADMIN) and click the **Login** button.
The **Choose User Token for Login** dialog box opens.
4. Select the appropriate authentication mechanism.

   - **Smartcard Token**
   If you have selected **Smartcard Token**, click **OK** in the **Choose User Token for Login** dialog box and follow the instructions on the PIN pad.
   - **Keyfile Token**
   If you have selected **Keyfile Token**, proceed as follows:

     a) Click the search … button next to **Key Path** the text box.
     The **Set Name and Path for User Keyfile Token** dialog box opens.
     b) Select the keyfile you require, e.g., `ADMIN.key`.
     c) Click the **Open** button.

d) In case the keyfile is protected with a password, enter the password in the **Password** text box of the **Choose User Token for Login** dialog box.

5. Click the **OK** button in the **Choose User Token for Login** dialog box.
   The dialog box closes. If the user login succeeded, a green check mark appears on the left hand side of the user item.
6. Click **Close** to close the **Login/Logoff User** dialog box.
7. On the **Manage** menu, click **Date/Time**.
   The **CryptoServer Date/Time** dialog box opens. Here you can choose between two options to set up the date and time of the CryptoServer.

   - **Apply host time**
     Select this option to transfer the date and time from the host system and use it for 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.

8. Click the **Apply** button.
   The settings you have performed are saved.
9. Click **OK**.
   The **CryptoServer Date/Time** dialog box closes.

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

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

4.8 Generating an MBK

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

Before you start generating an MBK:

- Answer the following questions:

- Do you want to store the MBK in keyfiles (outside the CryptoServer) or on smartcards?
- How many people shall the MBK 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.
- What is 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 13: 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 14: Example for an MBK split into 2 key shares

- Make sure that you have the required number n of smartcards delivered by Utimaco at hand before you start generating the MBK.

To generate the MBK, you must log in to the CryptoServer with at least permission 2 in the user group 6 (authentication status 02000000) or as the default user ADMIN.

To generate an MBK execute the following steps:

1. Start CAT.

2. Click the Login/Logoff button in the toolbar.
   The Login/Logoff User dialog box opens.
3. Log in to the CryptoServer as the default administrator ADMIN.
   You find further details on how to log in to the CryptoServer in chapter 4.6 in this manual.
4. Click Close to close the Login/Logoff User dialog box.
5. Click the Manage MBK button 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.

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 you enable XOR, the key is split into two parts and therefore two people will be needed to use the MBK (two-person rule).
   - If you click m out of n, you can select any value 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. Click Automatic MBK Import.
9. Click Generate.
   This opens the Master Backup Key (MBK) Share Storage 1/n dialog box.
10. In this dialog box, specify whether you want to store the MBK on a smartcard MBK Smartcard Token or as a keyfile MBK File Token.

    - MBK Smartcard Token

    In our example we need three smartcards.

    a) Insert the first smartcard into the PIN pad.
    b) Press the OK button on the PIN pad.
    c) Enter the PIN for the smartcard.
    d) Press the OK button on the PIN pad.
    e) Repeat the steps a) to d) for the remaining smartcards n-1 shares.

    - MBK File Token

a) Enter the location for the MBK into the **Key Path** text box manually or use the search button (…).
b) Specify (optionally) a password in the **Password** text box to protect the MBK keyfile from unauthorized access.
c) Click **OK**.
The generation of the MBK is initiated and confirmed in a separated window.
d) Repeat the steps a) to c) for the remaining two key parts n shares.

11. Once you have saved the MBK either as a keyfile or on a smartcard, close the **Remote Master Backup Key (MBK) Management** dialog box by clicking **Close**.

4.9 Changing the Authentication Key

The default administrator ADMIN has an authentication key (stored as a keyfile and on a smartcard) which is known to the manufacturer Utimaco IS GmbH (see chapter 2.9.1, "Default Authentication Key"). For this reason, it is imperative you change this authentication key. You can generate the new authentication key as a keyfile or on a smartcard. Here we show you how to generate the key on a smartcard.

First generate a new authentication key and then assign this key to the default administrator ADMIN. To do so you need at least three smartcards.

1. In the **Authentication Token** menu, click **Smartcard**.
The **Smartcard Token Management** dialog box opens. The **Generate** tab is shown by default.
2. As you are the default administrator ADMIN you are obliged to use the RSA signature method and therefore you must select the **RSA** option.
3. In the **Key-Info** text box, enter a key name.
4. Select the key size 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)**.*

5. 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.
6. Click **Generate**.
7. Follow the instructions on the PIN pad.

A confirmation window opens confirming the successful generation of the new authentication token.

8. Close the Smartcard Token Management dialog box with Close.

After you have generated the new key you must assign it to the default administrator ADMIN.

9. Click the Manage User button in the toolbar.
   This opens the User Management dialog box.
10. Select the ADMIN user.
11. Click the Change Token/Password button.
    This opens the Choose User Token for Login dialog box.
12. Use the "old" 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 user AMIN.
13. Click OK to close it and to be able to continue.

    The dialog box Choose new User Token opens.
14. Select Smartcard Token and click OK.
15. Insert the smartcard with the new authentication key into the PIN pad.
16. Click the OK button on the PIN pad.

Once the authentication key for the default administrator ADMIN has been successfully changed, the system will confirm this to you in a separate window.

4.10 Changing the PIN for Smartcards

If you purchased a smartcard from us for administering the CryptoServer, we recommend that you change the predefined default PIN for these cards.

You can change the following PINs on the smartcards:

- The smartcard PIN for the authentication key
- The smartcard PIN for the MBK

4.10.1 Changing the PIN for the Authentication Key

1. Click the Authentication Token menu and select Smartcard .
   The Smartcard Token Management dialog box opens. The Generate tab is shown by default.
2. Click the Change PIN tab.
3. Make sure that the PIN pad is connected to the host computer.
4. Click the Change PIN button in the Smartcard Token Management dialog box.

5. Follow the instructions on the PIN pad. First enter the old PIN, and then enter the new PIN. Confirm the new PIN. A message window appears to tell you that the PIN was changed successfully.

4.10.2 Changing the PIN for the MBK Smartcards

You do not have to log in to the CryptoServer if you only want to change the PIN of the smartcard on which the MBK is stored.

1. Click the **Manage MBK** button in the toolbar.
   This opens the **Remote Master Backup Key (MBK) Management** dialog box. The **Backup** tab is shown by default.
2. Click the **MBK Change PIN** tab.
3. Make sure that the PIN pad is connected to the host computer.
4. Click the **Change PIN** button. First enter the old PIN and then enter the new PIN. Confirm the new PIN. A message window appears to tell you that the PIN was changed successfully.
5. Change the PIN on every smartcard on which parts of the MBK are stored. You must do this separately for each individual card.

4.11 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, read the manual *CryptoServer CSP and CryptoServer CNG Key Storage Provider 1.x. and 2.x.* The document is provided on the SecurityServer/CryptoServer SDK product CD in the folder `\Documentation\Crypto_APIs\CSP-CNG`.

4.12 Setting up JCE

In the CryptoServer, JCE functions are provided by the CXI firmware module. A Cryptographic User has been created in this firmware module.

This Cryptographic User is also the JCE user. You must set up the Cryptographic User in the CryptoServer before you can use JCE. The CAT provides the appropriate authorization profile for the Cryptographic User.

The `CryptoServer.cfg` configuration file has been provided for JCE. You must modify the device address and the user name for the `DefaultUser` in this file.

You must load the MBK into the CryptoServer before you can use JCE.

4.12.1 Setting up a User for JCE

1. Start CAT.
2. Click the Login/Logoff button in the toolbar and log in to the CryptoServer with at least authentication status 20000000.
3. Click Close to close the Login/Logoff User dialog box.
4. Click the Manage User button in the toolbar.
   The User Management dialog box opens.
5. In this dialog box, click the Add User… button.
   This opens the Add User dialog box.
6. In the Name of New User field, enter the name `Cryptographic User`.

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

7. In the drop-down check box User Profile select the option Cryptographic User.
8. Select under Authentication Mechanism the authentication mechanism you want to use.
9. You can also enter an Attribute if you want to.

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**.

When you enter an **Attribute**, note the following:

- Set under **Attributes** an attribute in the following 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.*

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

- If you do not set an attribute, the cryptographic user will not be able to access any key on the CryptoServer.

10. Click the **OK** button to confirm your selection and, depending on which authentication mechanism you selected, follow the instructions on the CAT or on the PIN pad.

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 time.

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

The `CryptoServer.cfg` configuration file has been provided for JCE.

You must modify this file to suit the particular CryptoServer hardware you are using (CryptoServer PCI-/PCIe plug-in 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. You must also modify this name.

You will find this CryptoServer.cfg file in this directory:

C:\Program Files\Utimaco\CryptoServer\Software\JCE\

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
```

   In the example above several devices are setup (Device =). After installation a CryptoServer PCI or PCIe plug-in card is used by default, Device = PCI:0 (no # in front of Device). If required, modify it to suit your situation. For example, if you are using a CryptoServer LAN, remove the # in front of the entry #Device = 192.168.4.183, and enter the IP address of your CryptoServer LAN. All device entries you are not currently using must have the # in front. If you want to use the CryptoServer Simulator, enter 3001@127.0.0.1.

2. Modify the name of the DefaultUser from JCE to Cryptographic User.

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

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

4.13 Setting up CXI

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

You must load the Master Backup Key (MBK) into the CryptoServer before you can use CXI.

To be able to use CXI you have to create a CXI user, e. g.by using CAT.

1. Start CAT.
2. Click the **Login/Logoff** button in the toolbar and log in to the CryptoServer with at least authentication status 20000000.
3. Close the **Login/Logoff User** dialog box by clicking **Close**.
4. On the toolbar, click the **Manage User** button.
   The **User Management** dialog box opens.
5. In the **User Management** dialog box, click the **Add User** button.
   The **Add User** dialog box opens.

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.*

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

7. Under **Authentication Mechanism**, select the authentication mechanism you require. If you have decided to use **Password (HMAC)**, you must assign a password.

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

8. You can now enter an **Attribute** if you want.

   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**.

   When you enter an **Attribute**, note the following:

   - Set under **Attributes** an attribute in the following 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.*

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

   - If you do not set an attribute, the CXI cryptographic user will not be able to access any key on the CryptoServer.

9. Exit the **Add User** dialog box by clicking **OK**.

4.14 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

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

You must load the Master Backup Key (MBK) into the CryptoServer before you can use EKM.

4.14.1 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 in the CryptoServer before you can use EKM. The CAT provides the appropriate authorization profile for the Cryptographic User.

1. Click the **Login/Logoff** button in the toolbar and log in to the CryptoServer at least with the authentication status 20000000.
2. Click **Close** to close the **Login/Logoff User** dialog box.
3. Click the **Manage User** button in the toolbar.
   The **User Management** dialog box opens.
4. In the **User Management** dialog box, click the **Add User** button.
   The **Add User** dialog box opens.
5. In the **Name of New User** field, enter a unique name for the Cryptographic User. In our example, this is `Paul`.

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

6. Select the predefined `Cryptographic User` profile under **User Profile**.
7. Under **Authentication Mechanism**, select **Password (HMAC)**.
8. Under **Attributes** enter optionally the attribute you require.

   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**.

When you enter an **Attribute**, note the following:

- If you want EKM to have the ability to process clients, you must set the following, under **Attributes**, here: `CXI_GROUP=<Name of the group>`
  We use `PaulGroup` for our example.
  `CXI_GROUP=PaulGroup`

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=).*

- If you do not want EKM to have the ability to process clients, you do not need to enter a value under **Attributes**.

9. Exit the **Add User** dialog box by clicking **OK**.
   This opens the **Set Password of new User** dialog box.
10. Enter a unique password for the Cryptographic User (e.g. `Paul`), confirm it, and click **OK** to close the **Set Password of new User** dialog box.

4.14.2 Modifying the Device Address in the File cssqlekm.cfg

The `cssqlekm.cfg` configuration file has been created for EKM.

You must modify this file to suit the particular CryptoServer hardware you are using (CryptoServer PCI, CryptoServer PCIe or CryptoServer LAN).

You will find the `cssqlekm.cfg` configuration file on your SQL Server, in this folder:

`C:\Program Files\Utimaco\CryptoServer\Software\EKM`

From CSLAN version 4.2.0 and later 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.

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:/Program Files/Utimaco/CryptoServer/Lib/cssqlekm.log

# loglevel
LogLevel = 3

# maximum logsize in bytes
LogSize = 1000000

# path to the EKM Keystore
KeyStore = C:/Program Files/Utimaco/CryptoServer/Lib/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
```

2. Adjust the following part of the configuration file:

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

# remote CryptoServer
#Device = 192.168.1.2
```

3. Save the `cssqlekm.cfg` file and close your text editor.

4.14.3 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.

Note that you need to enter the user name and the password of the user Cryptographic User on the CryptoServer.

Also, note that the value of the Attribute that you have entered when you were 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 PaulCred WITH IDENTITY='Paul@PaulGroup',
SECRET='password'
FOR CRYPTOGRAPHIC PROVIDER utimaco
```

5 Maintaining the CryptoServer

This chapter describes the general maintenance tasks you will need to perform for your CryptoServer.

5.1 Resetting an Alarm

As already mentioned earlier in this manual, 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 you reset an alarm you should find out why it was triggered in the first place. If the alarm is a temporary alarm triggered, for example, because the mains power supply is too low, or because the internal temperature is either too high or too low, you must resolve the cause of the alarm before resetting it.

If you do not resolve the cause, the CryptoServer will return to *Maintenance Mode* after you restart it. The CryptoServer will only go into *Operational Mode* after a restart if you have removed the cause for the alarm.

To reset an alarm on the CryptoServer, you must log in with the appropriate authentication status.

1. Start CAT.
2. Click the Login/Logoff button 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.
4. Click Close to close the Login/Logoff User dialog box.
5. Click the Manage menu and select Reset Alarm.

   A new message window opens to tell you when the alarm has been reset successfully. The CryptoServer then performs a restart. This logs off any user who is currently logged onto 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.

To recreate the full functional availability of the CryptoServer (*Operational Mode*) you must set up the CryptoServer again and reload the firmware modules of the SecurityServer package. Use the CryptoServer Setup Wizard to do this.

5.2 Updating the Firmware of the CryptoServer

This chapter describes how to perform an update of the CryptoServer firmware package.

1. Click the Login/Logoff button in the toolbar.
   The Login/Logoff User dialog box opens.
2. Log in to the CryptoServer with at least authentication status 02000000.
3. Click the Manage menu and select Firmware.
   This opens the Setup CryptoServer dialog box.
   The series of your CryptoServer is shown in the upper part of the Setup CryptoServer dialog box in the Model text box. You must select the appropriate license file and firmware package for the CryptoServer device you are using.

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 don't need to import any license file during a setup (firmware package import).

If your version of the SecurityServer firmware is older than version 3.10 and the version of the firmware module ADM is older than version 3.0.8.0 you must import the appropriate license file during a setup (firmware package import).

4. Select the appropriate license file for your CryptoServer in the License File text box.
   After the installation of the product CD, you find the license files on your computer in the following folder:
   `C:\Programm Files\Utimaco\CryptoServer\Administration`

The names of the license files must match the names of the CryptoServer series. Therefore, if you have purchased, for example, a CryptoServer CSe-Series, you must select the appropriate license file for the CSe-Series here. See the table below.

CryptoServer series	*Appropriate license file*
CS10 with bootloader version < 2.5	No license file required
CS50 with bootloader version < 2.5	`cs50.slf`

CryptoServer series	*Appropriate license file*
CS10 with bootloader version ≥ 2.5	No license file required
CS50 with bootloader version ≥ 2.5	`cs50bl25.slf`
Se10	No license file required
Se50	`se50.slf`
Se400	`se400.slf`
Se1000	`se1000.slf`
Se12	No license file required
Se52	`Se52.slf`
Se500	`Se500.slf`
Se1500	`se1500.slf`
CSe10	No license file required
CSe100	`cse100.slf`

Table 15: List of CryptoServer series and the corresponding license files

Utimaco IS GmbH provides for each CryptoServer series the appropriate SecurityServer package as shown in the following table:

CryptoServer series	*SecurityServer Packages*
CryptoServer CS-Series	`SecurityServer-CS-Series-x.xx.x.mpkg`
CryptoServer CSe-Series	`SecurityServer-CSe-Series-x.xx.x.mpkg`
CryptoServer Se-Series	`SecurityServer-Se-Series-x.xx.x.mpkg`
CryptoServer Se-Series Gen2	`SecurityServer-Se2-Series-x.xx.x.mpkg`

Table 16: Available CryptoServer firmware packages

After the installation of the product CD, you find the SecurityServer packages on your computer in the following folder:

`C:\Programm Files\Utimaco\CryptoServer\Firmware`

5. Select the required SecurityServer package file in the Firmware Package text box.

6. Click the option **Update (installs only new firmware)**.
7. Click the **Setup** button.
8. Respond **Yes** to the following security prompt.
   A separate window appears to tell you if the SecurityServer package has been installed successfully.

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

5.3 Performing a Clear

The `Clear` command allows you to delete all the sensitive data and firmware modules stored on the CryptoServer. The following actions are triggered after you execute this command:

- All firmware modules are deleted.
  Only the system firmware modules required for base administration remain on the CryptoServer.
- All users using a password to log in to the CryptoServer are deleted.
- A new individual device key is generated for the CryptoServer.
  This automatically makes all the other keys (including the Master Backup Key) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the "old" individual device key.

To perform the `Clear` command, you must be logged onto the CryptoServer with at least authentication status 02000000 or as the default ADMIN.

However, all the users who log in to the CryptoServer with an RSA Signature, an RSA smartcard or an ECDSA signature are not deleted.

1. Start CAT.
2. Click the **Login/Logoff** button in the toolbar and log in to the CryptoServer with at least authentication status 02000000.
3. Click **Close** to close the **Login/Logoff User** dialog box.
4. Click the **Manage** menu and select **Clear**.
5. Confirm the confirmation prompt with **Yes**.
   A separate window appears to tell you if the `Clear` command has been performed successfully.

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

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

To recreate the full functional availability of the CryptoServer (*Operational Mode*) you must set up the CryptoServer again and reload the firmware modules of the SecurityServer package.

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

5.4 Performing Clear to Factory Settings

When you execute the *Clear to Factory Settings* command, it resets the CryptoServer back to delivery conditions.

- The firmware modules are deleted.
  Only the system firmware modules required for base administration remain on the CryptoServer.
- All the users in the CryptoServer user database are deleted.
- The default administrator ADMIN is set up again and can use the original authentication key `ADMIN.key` to log in to the CryptoServer.
- A new individual device key is generated for the CryptoServer.
  This automatically makes all the other keys (including the Master Backup Key) and sensitive data stored in the CryptoServer unusable, because they can no longer be decrypted without the "old" individual device key.

Before you can execute a *Clear to Factory Settings*, you must first perform an *External Erase* directly on the CryptoServer plug-in card or on the CryptoServer LAN.

The *External Erase* triggers an alarm in the CryptoServer which allows the *Clear CryptoServer to Factory Settings* command to be executed for as long as this alarm is active.

5.4.1 Performing an External Erase

You can only perform an *External Erase* on the CryptoServer plug-in card (PCIe) 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. In this situation, note that the different CryptoServer series – CryptoServer CS, CSe, Se and Se Gen2 - have different design.

You will find detailed information on how to perform an External Erase on the CryptoServer LAN in the CryptoServer LAN – Manual for System Administrators.

CryptoServer Se-Series

The figure below shows two contacts labeled *External Erase* in the white square.

1. Short-out these two contacts.

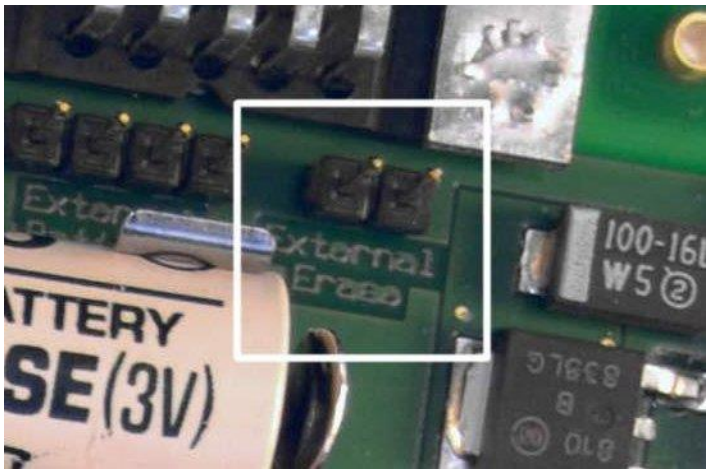


Figure 9: Performing External Erase on a CryptoServer Se-Series plug-in card

   This action is only effective if this card has been plugged in a computer and this computer has been switched on.

2. Click the ShowState button in the CAT administration tool to check whether the CryptoServer is now in Maintenance Mode.

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

CryptoServer CS-Series

The figure below shows two contacts labeled GND and IN in the white square.

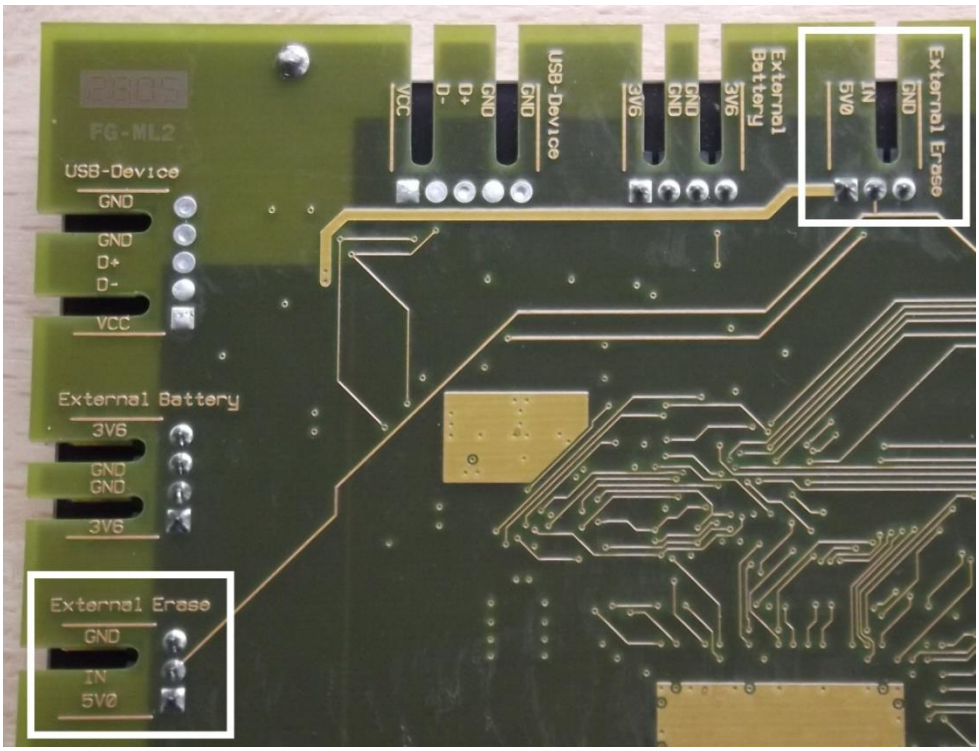


Figure 10: Performing External Erase on a CryptoServer CS-Series plug-in card

1. Short-out the two contacts, labeled GND and IN to perform an *External Erase* on a CryptoServer CS-Series.

   This action is only effective if this card has been plugged in a computer and this computer has been switched on.

2. Click the ShowState button in the CAT administration tool to check whether the CryptoServer is now in Maintenance Mode.

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

CryptoServer CSe-Series

You can perform an *External Erase* directly on the slot plate of a CryptoServer CSe-Series. There is a special Erase pushbutton under the aperture A (see next figure).

Figure 11: Performing External Erase on a CryptoServer CSe-Series plug-in card

3. Push the pushbutton under the aperture labeled with A by using an appropriate screwdriver.

   This action is only effective if this card has been plugged in a computer and this computer has been switched on.

4. Click the ShowState button in the CAT administration tool to check whether the CryptoServer is now in Maintenance Mode.

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

CryptoServer Se-Series Gen2

You can perform an *External Erase* directly on the slot plate of a CryptoServer Se-Series Gen2. There is a special Erase pushbutton under the aperture B (see next figure).

Figure 12: Performing External Erase on a CryptoServer Se-Series Gen2 plug-in card

1. Push the pushbutton under the aperture labeled with B by using an appropriate screwdriver.

   The LED flash light C flashes up red to confirm the activation of the Erase push-button B.

You can perform this action as well if the Cryptoserver PCIe plug-in card is not plugged in a computer or the computer is switched off.

2. Click the ShowState button in the CAT administration tool to check whether the CryptoServer is now in Maintenance Mode.

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

5.4.2 How to Perform a Clear to Factory Settings?

1. Start CAT.
2. Click the Manage menu and select Clear to Factory Settings that has been activated by the *External Erase*.
3. Respond YES to the following security prompt.
   A separate window appears to tell you if the *Clear to Factory Settings* command was executed successfully.
4. Click OK to close this window.
   The CryptoServer performs a restart and goes into Maintenance Mode.
5. Log in to the CryptoServer again.
6. Reset the alarm that has been activated by the previously performed External Erase as described in chapter 5.1 in this manual.
7. Set up the CryptoServer again as described in the following chapter 5.5 in this manual.

5.5 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.

CAT versions 2.1.0.0 and later do not support administration of the CryptoServer CS-Series (CS2000 and CS Classic). Use the CAT version 2.1.0.0 or earlier to administer those CryptoServer series.

1. Import the relevant license file and the appropriate firmware package (`SecurityServer-<Series>-<version>.mpkg`) into your CryptoServer.
2. Generate an MBK, import the MBK into the CryptoServer, split this into several parts, and define how many parts of the MBK are required to allow the MBK to be used. Save the private part of the MBK to the smartcards.

5.5.1 Importing the SecurityServer Package into the CryptoServer

1. Click the **Login/Logoff** button in the toolbar.
   The **Login/Logoff User** dialog box opens.
2. Log in to the CryptoServer with at least authentication status 02000000 or as the default administrator ADMIN.
3. Click the **Manage** menu and select **Firmware**.
   This opens the **Setup CryptoServer** dialog box.
   The series of your CryptoServer is shown in the upper part of the **Setup CryptoServer** dialog box in the **Model** text box.
4. Select the appropriate license file for your CryptoServer in the **License File** text box.

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 don't need to import any license file. Otherwise, you must import the appropriate license file into your CryptoServer.

5. After the installation of the product CD, you find the license files on your computer in the following folder:
   `C:\Programm Files\Utimaco\CryptoServer\Administration`

The names of the license files must match the names of the CryptoServer series. Therefore, if you have purchased a CryptoServer CS-Series, you must select the appropriate license file here. See Table 15 in chapter 5.2 for a list of the CryptoServer series and the corresponding license files.

Utimaco IS GmbH provides for each CryptoServer series the appropriate SecurityServer package as shown in Table 16 in chapter 5.2.

After the installation of the product CD, you find, by default, the SecurityServer packages on your computer in the following folder:

```
C:\Programm Files\Utimaco\CryptoServer\Firmware
```

6. Select the required SecurityServer package file in the **Firmware Package** text box.
7. Click the option **New Installation (deletes all files; installs new firmware package)**.
8. Click the **Setup** button.
9. Respond **Yes** to the following security prompt.
   A separate window appears to tell you if the SecurityServer package has been installed successfully.

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

5.5.2 Generating and Importing an MBK

Before generating an MBK, you should check how many smartcards are available. This is important because the MBK is stored on smartcards and you can split the MBK into a number of parts. You will need the corresponding number of smartcards for this.

To generate and import an MBK, you must be logged onto the CryptoServer with at least authentication status 02000000 or as the default administrator ADMIN.

1. Click the **Manage MBK** button in the CAT toolbar.
   The Remote **Master Backup Key (MBK) Management** dialog box opens.
2. Enter a name for the MBK in the **MBK Name** text box.
3. You then need to decide how many parts you want to "split" the key into.
   - If you enable **XOR**, the key is split into two parts and therefore two people will be needed to use the MBK (two-person rule).
   - If you click **m out of n**, you can select into how many parts you want to split the MBK **m (Shares)**, and how many key parts/persons are required **n (Shares)** to be able to use the MBK.
4. Select the option **Automatic MBK Import** to automatically import the MBK into the CryptoServer.
5. Click the **Generate…** button.
6. In the next dialog box, select whether you want to save the MBK as **MBK Smartcard Token** or as **MBK File Token**.
7. After you have made your selection, click **OK** to initiate the generation of an MBK.

8. If you want to save the new MBK as an **MBK Smartcard Token**, follow the instructions on the PIN pad and on the CAT.
9. To save the new MBK as an **MBK File Token**, follow the instructions on the CAT.
10. Once you have saved the MBK either as **MBK Smartcard Token**, or as **MBK File Token**, close the **Remote Master Backup Key (MBK) Management** dialog box by clicking the **Close** button.

5.6 Managing Smartcards and Keys

CAT provides a wide range of key and smartcard token management functions, which are described in the sections below.

5.6.1 Generating a Key on a Smartcard

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.

Connect the delivered PIN pad to the computer whereon CAT is installed.

You need at least two additional smartcards for a single backup of the generated key. These smartcards have to be at hand at the time of the key generation.

1. Click the **Authentication Token** menu and select **Smartcard**. The **Smartcard Token Management** dialog box opens.
2. Specify whether you want to generate an **RSA** or an **Elliptic Curve (DP: brainpoolP320t1)** (ECDSA) key.
3. Enter a name for the new key in the **Key-Info** field.
4. Specify the length for your RSA-key in the **RSA Key Length (bits)** field. 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 grayed out in case you have previously selected the option **Elliptic Curve (DP: brainpoolP320t1)**.

5. Under **Number of Backups** 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 ECC-Backup.
6. Click the **Generate** button, and follow the instructions on the PIN pad. The new RSA or ECDSA key will overwrite the default RSA key and ECC key stored on each of the ten delivered smartcards.
7. Close the **Smartcard Token Management** dialog box by clicking the **Close** button.

5.6.2 Restoring a Key from a Backup on Smartcards

Keep the smartcards whereon the backup of the key is stored at hand.

Connect the delivered PIN pad to the computer whereon CAT is installed.

To restore an RSA or ECDSA key from a backup stored on smartcards proceed as follows:

1. Click the **Authentication Token** menu and select **Smartcard**. The **Smartcard Token Management** dialog box opens.
2. Depending on the key type you want to restore proceed as follows:
   - If you want to restore an RSA key:
     a) Go to the **Restore RSA** tab.
     b) Click the **Restore RSA...** button.
     c) Insert the first RSA backup smartcard into the PIN pad and press the **OK** button on the PIN pad.
     d) Enter the PIN of the first RSA backup smartcard and press the **OK** button on the PIN pad.
     e) Insert the second RSA backup smartcard into the PIN pad and press the **OK** button on the PIN pad.
     f) Enter the PIN of the second RSA backup smartcard and press the **OK** button on the PIN pad.
     g) Insert the smart card on which you want to restore the smartcard key into the PIN pad and press the **OK** button on the PIN pad.
     h) Enter the PIN of the smartcard and press the **OK** button on the PIN pad.

- If you want to restore an ECDSA key

  a) Go to the **Restore EC** tab.
  b) Click the **Restore EC...** button.
  c) Insert the first EC backup smartcard into the PIN pad and press the **OK** button on the PIN pad.
  d) Enter the PIN of the first EC backup smartcard and press the **OK** button on the PIN pad.
  e) Insert the second EC backup smartcard into the PIN pad and press the **OK** button on the PIN pad.
  f) Enter the PIN of the second EC backup smartcard and press the **OK** button on the PIN pad.
  g) Insert the smart card on which you want to restore the smartcard key into the PIN pad and press the **OK** button on the PIN pad.
  h) Enter the PIN of the smartcard and press the **OK** button on the PIN pad.

3. Close the dialog confirming the successful key creation by clicking **OK**.
4. Exit this **Smartcard Token Management** dialog box by clicking the **Close** button.

5.6.3 Copying a Key Backup from One Smartcard to another Smartcard

You can copy an RSA-key backup or an ECC-key backup stored on a smartcard to another smartcard.

Connect the delivered PIN pad to the computer whereon CAT is installed.

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.

1. Click the **Authentication Token** menu and select **Smartcard**. The **Smartcard Token Management** dialog box opens.
2. Go to the **Copy** tab.
3. Click the **Copy** button.
4. Insert the smartcard from which you want to copy the key into the PIN pad and press the **OK** button on the PIN pad.
5. Enter the PIN of the smartcard and press the **OK** button on the PIN pad.

6. Insert the smartcard to which you want to copy the key backup into the PIN pad and press the OK button on the PIN pad.

An existing key backup of the same key type on the smartcard will be overwritten.

7. Enter the PIN of the smartcard and press the OK button on the PIN pad.

   A separate dialog box appears to confirm that the key backup has been copied successfully.

5.6.4 Changing the PIN for a Smartcard

To change the PIN for a smartcard, perform the following steps:

1. Click the Authentication Token menu and then select Smartcard. The Smartcard Token Management dialog box opens.
2. Click the Change PIN tab and then the Change PIN button.
3. Insert the smartcard on which you want to change the PIN into the PIN pad and press the OK button on the PIN pad.
4. Enter the old PIN for that smartcard and press the OK button on the PIN pad.
5. Enter the new PIN (of at least six and maximum 12 digits) for that smartcard and press the OK button on the PIN pad.
6. Confirm the new PIN and press the OK button on the PIN pad.

   A separate window appears to tell you that the smartcard's PIN was changed successfully.

5.6.5 Displaying the Contents of a Smartcard

To get detailed information about the keys currently stored on a smartcard, proceed as follows:

1. Click the Authentication Token menu and select Smartcard. The Smartcard Token Management dialog box opens.
2. Select the Info tab.
3. Click the Show Info button.
4. Insert the smartcard whose contents you want to view into the PIN pad and press the OK button on the PIN pad.
5. Press the OK button on the PIN pad again.

   The smartcard content is shown in a separate window.

5.6.6 Generating a Key as a Keyfile

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

1. Click the **Authentication Token** menu and select **Keyfile**. The **Keyfile Token Management** dialog box opens.
2. In the **Generate** tab, specify the type of the key you want to generate. You can choose between an **RSA** key and an ECDSA key using the **Elliptic Curve (DP: brainpoolP320t1)**.
3. 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.
4. 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 to only generate encrypted, password-protected RSA and ECDSA keyfiles.

5. Enter the password for the keyfile into the **Password** text box.
6. Confirm your password entry in the **Confirm Password** text box.
7. Finally, click the **Generate** button.

   A separate window appears to confirm the successful key generation.

5.6.7 Changing the Password for a Keyfile

If you want to change the password used to protect an encrypted keyfile, proceed as follows:

1. Click the **Authentication Token** menu and then select **Keyfile**. The **Keyfile Token Management** dialog box opens.
2. Select the **Password** tab.

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

5.6.8 Copying a Keyfile to a Smartcard (Backup)

If you want to copy a keyfile you have previously created to a smartcard, for example for backup purposes, execute the following steps:

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

5.7 User Management

If you want to use the user management functions to create one or more new user, you must log in to the CryptoServer as a user administrator with at least permission 2 in the user group 7 (min. required authentication status 20000000).

User profiles with predefined roles have been set up in the CAT to make it easier for you to create 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 you

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

You can select the following role-based user profiles:

User profiles	*Description*
ADMIN Manager one-person rule	Permissions: 22000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile 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	Permissions: 11000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile 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	Permissions: 20000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile is granted permission2 in user group 7 (User Management), and can authenticate all user management commands to the CryptoServer on its own.
User Management two-person rule	Permissions: 10000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile embodies the two-person rule. It is granted permission 1 in the user group 7 (User Management) and requires a second person to authenticate commands to the CryptoServer.

User profiles	*Description*
System Manager one-person rule	Permissions: 02000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile is granted permission 2 in the user group 6 (System Administration), and can authenticate all system management commands to the CryptoServer on its own.
System Manager two-person rule	Permissions: 01000000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile embodies the two-person rule. It is granted permission 1 in the user group 6 (System Administration), and requires a second person to authenticate system management commands to the CryptoServer.
NTP Manager one-person rule	Permissions: 00200000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile is granted permission 2 in the user group 5 (NTP Administration), and can authenticate all NTP administration commands to the CryptoServer on its own.
NTP Manager two-person rule	Permissions: 00100000 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile embodies the two-person rule. It is granted permission 1 in the user group 5 (NTP Administration), and requires a second person to authenticate NTP administration commands to the CryptoServer.
Cryptographic User	Permissions: 00000002 Default authentication mechanism: Smartcard (RSA Signature); can only be changed on user creation. This profile is granted permission 2 in the 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.

User profiles	*Description*
Customized User	Permissions: To be defined individually Default authentication mechanism: Password (HMAC); can only be changed on user creation. This is a user for customer-specific applications, e.g., PKCS#11.

Table 17: User profiles available in CAT

5.7.1 Creating a User

Prerequisites:

- The USB PIN pad provided by Utimaco is connected to the host-computer where CAT is installed on.
- If you are using a Windows host-computer, you have set the PIN pad settings in CAT as described in chapter 4.4, "Setting up a PIN Pad under Windows".
- If you are using a Linux host-computer, you have set the PIN pad settings in CAT as described in chapter 4.5, "Setting up a PIN Pad under Linux".
- If digital signature authentication mechanism (RSA or ECDSA signature) should be used with a key stored on a smartcard, the appropriate smartcard and smartcard holder should be available.

To create a new CryptoServer user, proceed as follows:

1. Start CAT.
2. Click the **Login/Logoff** button 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.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage User** button in the toolbar.
   The **User Management** dialog box opens.
6. Click the **Add User** button.
   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.*

8. Click ADMIN Manager one-person rule and select the role-based User Profile you require. All available user profiles are listed and explained in Table 17 above. To create a user with specific permissions, which do not match the permissions of any predefined user profile, e.g., PKCS#11 Key Manager, select the Customized User profile.
9. Specify the authentication mechanism for the new user under Authentication Mechanism.
10. If you have selected the Customized User profile above, define the user permissions in the different user groups under Group/Role and Permission Level.
11. 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.

    When you enter an Attribute, note the following:

    - Set an attribute in the following format:

      ```
      CXI_GROUP=<Name of the group>
      ```

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.

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 CXI key group.*

- If you do not set an attribute, the cryptographic user/key manager will not be able to access any key on the CryptoServer.

12. Click the **OK** button.

- If you have selected the **Password (HMAC)** authentication mechanism, the **Set Password of new User** dialog box opens.

a) Enter a unique, secure password in the **Password** text box.
b) Confirm your password entry in the **Confirm Password** text box.
c) Close the **Set Password of new User** dialog box by clicking **OK**.
The dialog box **Add User** closes automatically.

- If you have selected the authentication mechanism **Smartcard (RSA Signature)**, **Smartcard (ECDSA Signature)** or **Smartcard (PIN Pad on CryptoServer)**, the **Choose User Token to Add a New User** dialog box opens with pre-selected option **Smartcard Token**.

a) Click the **OK** button and follow the instructions on the display of the PIN pad.
b) Insert the smartcard, where the key is stored on, and press **OK** on the PIN pad.
The dialog box **Add User** closes automatically.

- If you have selected the authentication mechanism **Keyfile (RSA Signature)** or **Keyfile (ECDSA Signature)**, the **Choose User Token to Add a New User** dialog box opens with pre-selected option **Keyfile Token**.

a) Click the **OK** button.
b) Click the search button next to the **Key Path** field.
c) Select the keyfile path and click **Open**.
d) Click **OK** in the **Choose User Token to Add a New User** dialog box.
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.

5.7.2 Deleting a User

To delete a CryptoServer user, proceed as follows:

1. Start CAT.
2. Click the **Login/Logoff** button in the toolbar.
The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with at least authentication status 20000000 or as the default user ADMIN.
4. Click **Close** to close the **Login/Logoff User** dialog box.
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 the **Delete User…** button.
8. Confirm the deletion with **Yes**.

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.

The selected user has been removed from the user list.

5.7.3 Creating a User Data Backup

Before you can create a backup of the CryptoServer user database, you must first have imported the Master Backup Key (MBK) into the CryptoServer.

To create a backup of the CryptoServer user database, proceed as follows:

1. Start CAT.
2. Click the **Login/Logoff** button in the toolbar.
   The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer with at least authentication status 20000000 or as the default user ADMIN.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage User** button in the toolbar.
   The **User Management** dialog box opens.
6. Click the **Backup Users…** button.
   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 following folder:

   `C:\Program Files\Utimaco\CryptoServer\Administration`

   The type of the created backup file is by default `UserBackup (*.ubu)`.

5.7.4 Restoring User Data

You can only perform a restore of the CryptoServer user database, if the same MBK used for creating the user data backup has been previously imported into the CryptoServer.

1. Start CAT.
2. Click the **Login/Logoff** button 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 as the default user ADMIN.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage User** button in the toolbar.
   The **User Management** dialog box opens.
6. Click the **Restore Users...** button.
   The **Open User Backup File** dialog box opens.
7. Select the appropriate user backup file (`*.ubu`).
8. Click the **Open** button.

A separate window appears to tell you that the user list was restored successfully.

5.7.5 Changing a User Password/Token

Only the user themselves can change their password or token. No one else, not even the default administrator ADMIN we created, can change the password or the authentication token for another user.

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

1. Click the **Manage User** button.
   The **User Management** dialog box opens.
2. Select your user name in the list of users.
3. Click the **Change Token/Password** button.
   The **User Password of <user name>** dialog box opens.
4. Enter your current password in the **Password** text box.

5. Click the **OK** button.
   The **User Password of <user name>** dialog box closes. The **Change User Password** dialog box opens.
6. Enter here in the **New Password** text box your new password.
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** to close the **User Management** dialog box.

5.8 Master Backup Key Management

You can use the CAT to perform MBK management functions remotely.

In this context remote means you connect the PIN pad to the host computer from which you want to administer the CryptoServer.

You do not need to be logged onto the CryptoServer to perform the following actions:

- Backup an MBK
- Change the PIN of the smartcard on which the MBK is stored
- Retrieve information about an MBK

If you want to generate and import the MBK into the CryptoServer, you must log in to the CryptoServer with at least permission 2 in the user group 6 (min. authentication status 02000000).

5.8.1 Generating an MBK

Before you start generating an MBK, answer the following questions by considering the security policy of your company:

- Do you want to store the MBK outside the CryptoServer into keyfiles or on smartcards?
- How many people shall the MBK be distributed to?
- What is the minimum number of parts (people) required to use the MBK?

Utimaco highly recommends to generate and distribute the MBK in an m-out-of-n scheme, where <n> (n ≥ 2) defines the number of the key parts (shares) to be generated and <m> (m ≥ 2) specifies how many key parts are required for the key to be reconstructed and used.

In case you have decided to use smartcards for the MBK generation, make sure that the PIN pad is correctly connected to the computer where CAT is installed on and keep the required number of smartcards at hand.

Follow these steps to generate an MBK:

1. Start CAT.
2. Click the **Login/Logoff** button 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 administrator ADMIN.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage MBK** button in the toolbar.
   The **Remote Master Backup Key (MBK) Management** dialog box opens.
6. Enter a name for the MBK under **MBK Name**.
7. Select how many parts you want to split the key into.
   - If you enable **XOR**, the key is split into two parts and therefore two people will be needed to use the MBK (two-person rule).
   - If you select **m out of n**, you can select into how many parts you want to split the MBK **m (Shares)**, and how many key parts/persons are required **n (Shares)** to be able to use the MBK.
8. If you want to import the MBK automatically into the CryptoServer, select **Automatic MBK Import**.
9. Click the **Generate...** button.

   The dialog box **Master Backup Key (MBK): Share Storage 1/<n>** opens.
10. Select whether you want to save the MBK as a **Smartcard Token** or as a **Keyfile Token**.

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

- If you have chosen to store the MBK as a **Smartcard Token**, proceed as follows:

a) Click **OK** to trigger the generation of an MBK
b) Insert a smartcard into the PIN pad and press **OK** on the PIN pad.
c) Enter the PIN for the smartcard and press **OK** on the PIN pad.
d) 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.
e) Keep the **Smartcard Token** option selected and click **OK**.

f) Repeat steps b) to e) for the remaining MBK share(s).

After you have successfully created all m MBK shares, this is confirmed to you in a separate CAT window. Click **OK** to close this window.

▣ If you have chosen to store the MBK as a **Keyfile Token**, proceed as follows.

a) 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.

b) Select the location and enter the **File name** you require for the keyfile.

c) Click **Save**.

d) Optionally, enter a password in the corresponding text box to additionally protect the keyfile and click **OK**.

In a separate window you now see that you have successfully generated and stored the MBK share as a keyfile. Click **OK** to continue for the next MBK share (2/<n>).

The dialog box **Master Backup Key (MBK): Share Storage 2/<n>** opens.

e) Repeat steps a) to d) for the remaining MBK share(s).

After you have successfully created all m MBK shares, this is confirmed to you in a separate CAT window. Click **OK** to close this window.

11. Click **Close** to close the **Remote Master Backup Key (MBK) Management** dialog box.

5.8.2 Importing an MBK

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

In case you have stored the MBK on smartcards, make sure that the PIN pad is correctly connected to the computer where CAT is installed on and keep at least m (m ≥ 2, see chapter "Generating an MBK") MBK smartcards at hand before you start.

1. Start CAT.
2. Click the **Login/Logoff** button 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.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click in the toolbar on **Manage MBK**. The **Remote Master Backup Key (MBK) Management** dialog box opens.
6. Click the **Import** tab.
7. 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. Click the Import button.
   The Master Backup Key (MBK): Share Import 1/<m> dialog box opens.

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 MBK.

10. 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.

    - To import the MBK from a smartcard, proceed as follows:

    a) Select the option Smartcard Token and click OK.
    b) Insert the smartcard and press OK on the PIN pad.
    c) Enter the PIN for the smartcard and press OK on the PIN pad.
    d) In a separate CAT window you now see that you have successfully imported the first MBK share. Click OK to continue.
    e) Keep the Smartcard Token option selected and click OK.
    f) Repeat steps b) to d) for all remaining MBK shares.
    g) In a next CAT window you now see that you have successfully imported all required MBK shares. Click OK to close this window.

    - To import the MBK from a keyfile, proceed as follows:

    a) Select the Keyfile Token option.
    b) Click the search button next to the text filed Key Path and double-click of the previously generated MBK shares to select it. By default the MBK shares are keyfiles with the file extension `*.mks`.
    c) In case the MBK share keyfile is password protected, enter the appropriate password into the Password text box.
    d) Click OK.
    e) In a separate CAT window you now see that you have successfully imported the first MBK share. Click OK to continue.
    f) Repeat steps a) to e) for all remaining MBK shares
    g) In a next CAT window you now see that you have successfully imported all required MBK shares. Click OK to close this window.

11. After you have imported the MBK, close the Remote Master Backup Key (MBK) Management dialog box by clicking the Close button.

5.8.3 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.
- 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.

Follow these steps to create a backup copy of your MBK.

1. Start CAT.
2. Click the **Manage MBK** button in the toolbar.
   The **Remote Master Backup Key (MBK) Management** dialog box opens.
3. Under **Source Token**, select whether the MBK backup is to be prepared from **Smartcard**s 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.
4. Under **Destination Token** select whether the backup is to be created on **Smartcard**s 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 if the MBK backup keyfile shall be additionally protected with a password.
5. Then click the **Backup…** button to confirm your selection for both source and destination tokens.

   Create a backup from an MBK smartcard to another smartcard:

   a) Insert the source smartcard containing the first share of the MBK into the PIN pad and press **OK** on the PIN pad.
   b) Enter the PIN for the MBK smartcard and press **OK** on the PIN pad.
   c) Insert the first destination smartcard into the PIN pad and press **OK** on the PIN pad.
   d) 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 as described in the next section "Changing the PIN for an MBK Smartcard".

e) Repeat steps a) to d) for all source MBK smartcards containing MBK shares.

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

a) Insert the source smartcard containing the first share of the MBK into the PIN pad and press OK on the PIN pad.
b) 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. Confirm the warning by clicking YES to continue.

   A separate window appears to confirm the successful creation of the MBK share copy.
c) Repeat steps a) and b) for all source MBK smartcards containing MBK shares.

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

a) Insert the destination smartcard into the PIN pad and press OK on the PIN pad.
b) 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.
c) Repeat steps a) and b) for all MBK shares.

If the smartcard containing the copy of the MBK share is protected with the default PIN, change the PIN as described in the next section "Changing the PIN for an MBK Smartcard".

5.8.4 Changing the PIN for an MBK Smartcard

You do not have to be logged in to the CryptoServer to change the PIN of the smartcard, where the MBK is stored.

To change the PIN of the smartcard, where the MBK is stored, proceed as follows:

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

A separate window appears to tell you that the smartcard's PIN has been successfully changed.

5.8.5 Retrieving MBK Information

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

1. Start CAT.
2. Click the **Manage MBK** button 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 that is stored in the CryptoServer.
5. To view information about an MBK that is stored on a smartcard, click the **Card Info** button and follow the instructions on the PIN pad.
   All the important information about an MBK that is stored on a smartcard is displayed under **MBKs stored on Smartcard**.
6. Close the **Remote Master Backup Key (MBK) Management** dialog box by clicking the **Close** button.

5.9 Preparing Diagnostic Information

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

To view all the most important status information:

1. Start CAT.
2. Click the Show menu and select Diagnostics.

The following diagnostic information appears in the separate window Save Diagnostics:

- 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 in the CryptoServer
- All active firmware modules in the CryptoServer
- All the users set up in the CryptoServer
- Date and time on the CryptoServer
- The alarm log (only displayed if bootloader version ≤ 2.5 is loaded in the CryptoServer).
- Information about the Master Backup Key that is saved in the CryptoServer

3. To send the diagnostic information to the manufacturer Utimaco IS GmbH for problem analysis, click Save and save the `.txt` file on your computer.

In the sections that follow we explain the meaning of the individual bits of information, which you can also retrieve separately.

5.9.1 Showing the CryptoServer Status

If you click the Show Status button in the CAT toolbar, the system displays the CryptoServer's status in the CAT main window:

```
mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 39.9 [C]
alarm     = OFF
bl_ver    = 3.00.2.1          (Model: Se-Series)
uid       = db000017 189d4401                    |       D
adm1      = 53653130 20202020 43533434 32353938 | Se10    CS442598
adm2      = 53656375 72697479 53657276 65720000 | SecurityServer
adm3      = 494e5354 414c4c45 44000000 00000000 | INSTALLED
```

The following table shows the different status information fields and their meanings, and how they are displayed.

Description	*Meaning and coding*
`mode`	Shows the current mode (Operational/Maintenance)
`state`	Shows the current status (INITIALIZED / DEFECT)
`temp`	Shows the current temperature (in Celsius)
`alarm`	Shows the current alarm state (OFF/ON)
`bl_ver`	Shows the 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. Not available for CryptoServer CS- and Se-Series
`uid`	UID is an 8-byte binary data field. The UID is a "Universal Identification" which uniquely identifies every CryptoServer plug-in card. It is stored in a hardware component and loaded to the plug-in card during programming. The UID is displayed when the status information is extracted.
`adm1`	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`, `CSe100`, `CS10`, `Se10`, `CS50`, `Se50`, `Se400` or `Se1000`. The second 8 characters represent the serial number of the CryptoServer's plug-in card which is assigned by Utimaco IS GmbH during manufacture and then loaded into the CryptoServer. The serial number starts with the letters `CS`, followed by a 6-digit number. The character string adm1 is displayed when you select the status information. The 8-character serial number `CSxxxxxx` is also stored on the CryptoServer plug-in card.
`adm2`	adm2 is a readable 16-character string. The contents of the adm2 character string are also assigned by Utimaco IS GmbH and loaded onto the CryptoServer during

Description	*Meaning and coding*
	production. Whilst the CryptoServer is being manufactured, "SecurityServer" is entered here. The character string adm2 is displayed when you select the status information. It is not stored on the CryptoServer.
`adm3`	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 Se-Series CryptoServer, the value `Installed` is recorded here.

Table 18: CryptoServer status information fields and their meaning

5.9.2 Listing All Files

Open the CAT main window and click the Show Files button in the toolbar to display all the files resident in the CryptoServer's flash memory (RAM). You can display all the loaded firmware modules (`*.msc`), databases (`*.db`), logfiles (`*.log`) and license files (`*.slf`).

If you are using the signed configuration file `cmds.scf`, 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 chapters "Configurable Role-based Access Control (C-RBAC)" and "Interface Hardening by Disabling Selected Functions".

5.9.3 Listing the Firmware

1. Start CAT.
2. Click the Show Firmware button in the toolbar to display all the firmware modules that have been loaded into the CryptoServer.

   The next table is an example, and illustrates the meaning of the entries displayed here.

ID number (hexadecimal)	*Module name*	*Version number*	*Initialization Status*
0	SMOS	5.3.3.0	INIT_OK
68	CXI	2.1.9.2	INIT_OK
81	VDES	1.0.9.1	INIT_OK
82	PP	1.2.5.0	INIT_OK
83	CMDS	3.4.0.0	INIT_OK

ID number (hexadecimal)	*Module name*	*Version number*	*Initialization Status*
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	3.0.16.0	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 19: Example for how firmware information is displayed in CAT and its meaning

When you display the firmware module's initialization status, the following information may appear:

- 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 Crypto accelerator chip. This is the situation for Se10 and Se50 devices.

  For CryptoServer in the Se400 or Se1000 Series, which have a Crypto accelerator chip, the status `INIT_OK` is output for the firmware module HCE.

- INIT_INTERNAL

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

- INIT_DEP_OK

This status is usually only displayed during the boot phase (temporary) 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 the entries shown in the above table. Then contact Utimaco's customer support, and pass on these details to enable us to identify this module.

5.9.4 Viewing the Boot Log

Follow these steps to view the CryptoServer boot log:

1. Click the Show menu and 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).

   - If you have a Se10-, Se12-, Se50- or Se52-Series CryptoServer, the message `No Hardware Crypto Engine installed` is displayed. This means your CryptoServer does not have a Crypto accelerator chip.
   - The Crypto accelerator chip is present in the Se400-, Se500-, Se1000- or Se-1500-Series CryptoServer. In this case, you see the message `Hardware Crypto Engine detected`.
   - If you have a CSe10-, CS10- or the Se-10 or Se12-Series CryptoServer, the line `CMDS: 1000 TPS` appears in the boot log. In every other model, the line `CMDS: no TPS limit` appears here.
   - If your CryptoServer is a CSe100-, CS50-, Se50-, Se52-, Se400-, Se500-, Se1000- or Se1500-Series, and the line `CMDS: 1000 TPS` still appears, this may mean that no license file has been loaded. In this case the boot log contains the line `No license file found`. Alternatively, it means that a license file which does not match your CryptoServer model 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.

2. Perform a setup and then import the appropriate license file and the corresponding firmware package for your CryptoServer series.
3. After a Reboot, check once again the corresponding messages in the boot log.

5.9.5 Deleting Displayed Log Entries

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

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

1. Click the File menu and select Clear Console Output.
2. In a separate window, confirm by clicking OK that you want to delete the entries currently displayed in the main window.

5.9.6 Saving Displayed Log Entries

To save all the information currently displayed in the CAT main window:

1. Click the File menu and select Save Console Output.
   The CryptoServer Console Output dialog box opens.
2. In the File name text box, assign a unique name for the logfile.
3. Click the Save button.
   The logfile is stored by default in the following folder:
   `C:\Program Files\Utimaco\CryptoServer\Administration`
   The type of the created logfile is by default `Console Output File` (`*.log`).

This is a good idea if you want to store the information displayed in this window so you can analyze it at a later date or send it to the manufacturer's customer support in case of an issue.

5.9.7 Viewing CryptoServer's Battery State

The status of the carrier battery on a CryptoServer plug-in card is always displayed in the lower right-hand corner of the CAT main window. If you see the status LOW here, 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 which then deletes all sensitive data from the CryptoServer. You will find instructions on how the replace the carrier battery in the Operating Manual delivered in a printed form to you or on the product CD in the `Documentation\Operating Manuals` folder.

To check the status of the *External Battery* of your CryptoServer LAN by using CAT, click the Show menu and select Battery State. When the external battery reaches a critically low power level, it must be replaced as described in the corresponding *CryptoServer LAN Operating Manual*.

5.9.8 Viewing Driver Information

If your CryptoServer suddenly stops reacting to any commands, you can display the driver information. Have this information at hand if you then need to contact our support team.

This information includes, among other things, details about the CryptoServer driver, the slot number etc., which can only be interpreted by the manufacturer Utimaco IS GmbH.

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

5.9.9 Retrieving and Saving the Audit Log

To view the audit log:

1. Start CAT.
2. Click the **Show** menu and select **Audit Log**.
   This opens the **CryptoServer Audit Log** dialog box.

   Under **Logged Events** you see a list of all events that are written in the audit log, e. g.:

   - Firmware Management
   - User Management
   - Date/Time Management
   - Startup Messages
   - Audit Log Management
   - MBK Management
   - Failed Login Attempts
   - Backup/Restore

   Under **Audit Log Filters** you can filter the displayed audit log either by **User** or by **Command/Return Value**.

To save the audit log:

3. Click on the **Save Log...** button.
   The **CryptoServer Audit Log File** dialog box opens.
4. Assign a unique name for the audit log file in the **File name** text box.
5. Click the **Save** button.
   The audit log file is stored by default in the following folder:
   `C:\Program Files\Utimaco\CryptoServer\Administration`
   The type of the created audit log file is, by default, .log.
6. Close the **CryptoServer Audit Log** dialog box by clicking the **Close** button.

5.9.10 Configuring the Audit Log Files

You can adjust the audit log configuration to your individual requirements. By doing that you determine which information to be written into the audit log. Follow these steps:

1. Start CAT.

2. Click the **Login/Logoff** button in the toolbar.
   The **Login/Logoff User** dialog box opens.
3. Log in to the CryptoServer as a user with at least authentication status 22000000.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage** menu and select **Audit Log Settings**.
   This opens the **Audit Log Configuration** dialog box.

   In this dialog box you can setup the following settings:

   - **Number of audit log files**
     This is where you specify the number of audit log files. The number 3 (default setting) means that three audit log files are recorded in the CryptoServer. You can store a minimum of 2 and a maximum of 10 audit log files.
   - **File size (max. 240)**
     This is where you specify the size of each audit log file in kilobytes. The default setting is 200 kilobytes for each audit log file. You must specify at least 4 Kilobyte.
   - **When all log files are full**
     This defines how the audit log files are to be handled when they are full.
     - If you select **Rotate file** it means that the next audit log file is used when the previous audit log file is full. Once all the audit log files are full, the first audit log file will be overwritten.
     - If you select **Stop logging**, this means no audit log files will be overwritten when all the audit log files are full.

*If all audit log files are full, and you have selected **Stop logging** all CryptoServer commands generating a logfile entry will be blocked.*
In this case, you must delete all audit log files, in order to be able to administer the CryptoServer again.
For that purpose, you have to log in to the CryptoServer with authentication status 20000000 or 02000000.

   - **Events**
     Here you can specify which events are to be recorded in the audit log files.
     The table below describes the meanings of the individual selection options.

Event name	*Meaning*
Firmware management	Load, delete and replace firmware modules.
User management	Create and delete users, and backup 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 the relevant CryptoServer messages from 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.

Table 20: Logging events and their meaning

In the default settings for audit log files, only the Key Management and Successful login attempts are not enabled.

6. Click the Apply button.
   This saves your changes and the Audit Log Configuration dialog box remains open.
7. Click the OK button to finish processing.
   This applies your changes and closes the Audit Log Configuration dialog box.

5.9.11 Deleting an Audit Log in the CryptoServer

You cannot restore the CryptoServer audit log once it has been deleted. For this reason you must save the audit log before you delete it.

To delete an audit log file in the CryptoServer:

1. Start CAT.
2. Click the **Login/Logoff** button 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.
4. Click **Close** to close the **Login/Logoff User** dialog box.
5. Click the **Manage** menu and select **Audit Log** .
   This opens the **CryptoServer Audit Log** dialog box.
6. Click the **Clear Log...** button.
   In a separate window the system prompts you to confirm the deletion of the audit log in the CryptoServer by clicking **Yes**.

We recommend you to view, save and delete the audit log files regularly.

5.10 Creating a Database Backup

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

Before you can do this, you must first import your individual Master Backup Key into the CryptoServer. This Master Backup Key is then used to encrypt all the data, and therefore also all the databases, before they are copied from the CryptoServer to a backup directory.

1. Click the **Backup/Restore** button in the CAT toolbar.
   This opens the **CryptoServer Database Backup/Restore Wizard** dialog box.
2. Select the option **Copy databases from Source CryptoServer to Backup directory**.
3. Enter the IP address of the source CryptoServer in the **Source CryptoServer** text box.
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, under **Source CryptoServer**, select the databases you want to copy.
   - You can select all the databases by clicking the **Add All >>** button.
   - You can add databases individually by first selecting them and then clicking the **Add >>** button.

Once you have made your selection, the databases appear in the **Backup Directory** list.

6. Click the **Execute** button.
   The **Login User for Source CryptoServer** dialog box opens.
7. Log in to the CryptoServer as ADMIN (or another user with the same permissions) with the authentication status 22000000.
   The result of exporting the databases to a backup directory then appears in an information window **Database Export**.
8. Close the **Database Export** window by clicking the **Close** button.

5.11 Restoring Databases

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

The CryptoServer to which you want to copy the databases must have the same MBK that was used to create the database backup in the first place.

1. Click the **Backup/Restore** button in the CAT toolbar.
   This opens the **CryptoServer Database Backup/Restore Wizard** dialog box.
2. Select the option **Copy databases from Backup directory to Target CryptoServer**.
3. Enter in the **Target CryptoServer** text box the IP address of the CryptoServer where the databases are to be restored to.
4. Enter in the **Backup directory** text box the directory where the databases have been previously stored to.
5. In the lower part of the dialog box, under **Source CryptoServer**, select the databases you want to copy.
   - You can select all available databases by clicking the **Add All >>** button.
   - You can add databases individually by first selecting them and then clicking the **Add >>** button.

   Once you have made your selection, the databases appear in the list **Target CryptoServer**.
6. Click the **Execute** button.
   This opens the **Login User for Target CryptoServer** dialog box.
7. Log in to the (target) CryptoServer as a user who has at least authentication status 22000000 and then close the dialog box by clicking **Close**.
   The result of importing the databases from a backup directory into a CryptoServer is then displayed in an information window **Database Import**.

You must restart the CryptoServer, so that the restore of the databases get applied.

5.12 Copying Databases from One CryptoServer to Another

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

Before this can happen, you shall ensure that both CryptoServer are running the same version of the SecurityServer package. Additionally, the MBK of the source CryptoServer shall be imported into the target CryptoServer. This MBK is used to encrypt all database entries before they are copied from the source CryptoServer to the target CryptoServer. In case you have stored the required MBK 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 ≥ 2, see chapter "Generating an MBK") of the n smartcards, where the required MBK is stored on, at hand before you start.

1. Click the **Backup/Restore** button in the CAT toolbar.
   This opens the **CryptoServer Database Backup/Restore Wizard** dialog box.
2. Select the option **Copy databases from Source CryptoServer to Target CryptoServer**.
3. Enter the IP address of the source CryptoServer in the **Source CryptoServer** text box.
4. Enter the IP address of the target CryptoServer in the **Target CryptoServer** text box.
5. In the lower part of the window, under **Source CryptoServer**, select the databases you want to copy.
   - You can select all available databases by clicking the **Add All >>** button.
   - You can add databases individually by first selecting them and then clicking the **Add >>** button.

   Once you have made your selection, the databases appear in the list **Target CryptoServer**.
6. Click the **Execute** button.

   CAT first compares the firmware modules of both CryptoServer (source and target) that are involved in this process. The results of this comparison are then displayed in an information window.
   - If the results show that both CryptoServer have the same firmware modules (**OK!**), click the **OK** button to close this information window.
   - If the results show that the firmware modules or the firmware module status in the s are not identical, you can either click **No** to cancel the operation, or continue by clicking **Yes**.

   Comparing the firmware modules, and the firmware module status, do not actually affect how the databases are copied.

The **Login User for Source CryptoServer** dialog box opens.

7. Log in to the source CryptoServer as a user with at least authentication status 22000000.
8. Once you have logged on, click the **Close** button to close the **Login User for Source CryptoServer** dialog box.
   This opens the **Login User for Target CryptoServer** dialog box.
9. Log in to the target CryptoServer as a user with at least authentication status 22000000.
10. Once you have logged on here, click the **Close** button to close the **Login User for Target CryptoServer** dialog box.
    This opens the **CryptoServer Date/Time for Target CryptoServer** dialog box. This dialog box is where you specify the date and time for the target CryptoServer. However, setting the date and time for the target CryptoServer is optional and has no effect on how the databases are transferred.
11. Select **Apply host time** to transfer the date and time from the host system.
12. When you have finished entering your data, click the **Apply** button.
    This saves your changes and the **CryptoServer Date/Time for Target CryptoServer** dialog box remains open.
13. Click the **OK** button to finish processing.
    This applies your changes and closes the **CryptoServer Date/Time for Target CryptoServer** dialog box.

    The **Master Backup Key for Target CryptoServer** dialog box opens. The MBK will encrypt all database entries before they leave the source CryptoServer. Both CryptoServer involved in this process must have the same Master Backup Key so the databases can be decrypted correctly in the target CryptoServer.
14. In the **Master Backup Key for Target CryptoServer** dialog box, click on the **Import** tab.
15. Select under **MBK Type**, 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.
16. Under **m (shares)** specify the number of parts into which you have split the MBK.
17. Click the **Import** button.
18. 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 **Keyfle Token**.
19. Click the **OK** button.
20. Follow the instructions on the PIN pad and the CAT to import all the parts of the Master Backup Key into the CryptoServer (target).
21. After all the parts of the Master Backup Key have been imported successfully into the CryptoServer (target), click **Close** to exit the **Master Backup Key (MBK): Share Import** dialog box.

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

6 Contact Address for Support Queries

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

Utimaco IS GmbH

Germanusstr. 4

52080 Aachen

Germany

You can reach us from Monday to Friday 09.00 a.m. to 05.00 p.m., apart from public holidays and other customs days, under the following phone/fax number and e-mail address:

Phone: +49 (0) 241 1696-153

Fax: +49 (0) 241 1696-58153

e-mail: support-cs@utimaco.com

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

rma-cs@utimaco.com

To save the diagnostic information in a TXT file on your computer, proceed as described in chapter 5.9 in this manual.