CryptoServer

User Guide

Utimaco Safeware AG

Transaction Security

www.utimaco.com

Imprint

Copyright 2008	**Utimaco Safeware AG** **Transaction Security** **Germanusstraße 4** **52080 Aachen**
Phone	++49 (0)241 / 1696-200
Telefax	++49 (0)241 / 1696-222
Internet	www.utimaco.de
E-Mail	info.sh@aachen.utimaco.de
Document Number	2006-0001
Version	0.7.1
Status	draft
Date	8th October 2008
Authors	

Table of Contents

1 Introduction

The **CryptoServer** is the **hardware security module** developed by Utimaco Safeware AG, i. e. a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data. In a CryptoServer security system security-relevant actions can be executed and security-relevant information can be stored. It can be used as a universal, independent security component for heterogeneous computer systems.

The hardware security module CryptoServer is based on a tamper proof and tamper-responding microprocessor system which evaluates and defeats physical attacks. Security-relevant information, such as cryptographic keys and secret data, are stored in the tamper-proof buffered on-board memory to ensure maximum integrity and confidentiality. All security relevant software is running inside the CryptoServer.

CryptoServer is certified in accordance with the highest standards and available for a wide range of applications: transaction security in ERP systems, secure PKI environments, document management and archiving solutions, database security and authentication, payment applications and electronic invoicing, and others more. Herefore, Utimaco offers tailor-made solutions as well as a broad range of standard interfaces, to simplify integration in your existing applications.

1.1 About this Document

This document should be read by persons responsible for setting up and installing a CryptoServer system, or for CryptoServer administration. It should be read before all other CryptoServer documentation contained on the CryptoServer product CD is read, starting from here it will be refered to all further documentation which will be be necessary during the installation process.

In the following section the various CryptoServer product variants will be explained.

In chapter 3 all basic hardware and software components of a complete working CryptoServer system are presented.

Chapter 4 gives background information for better understanding of a CryptoServer system.

A guide through the installation process of a CryptoServer system, including all host software installation and and initialization tasks, is given in chapter 5.

Chapter 6 is a user manual for the CryptoServer Administration Tool CAT.

In chapter 7 a short practical guide through the most important administration tasks and how to perform them with the administration tool CAT will be given.

Chapter 8 gives help and practical guidance in critical situations like alarm, or in case the CryptoServer is not showing the expected reaction, or no reaction at all. This chapter can also be used directly, without having studied the other more comprehensive chapters before.

Brief information for PIN-Pad usage can be found in chapter 9, and in the last chapter 10 a reference list for all further documentation is given.

2 CryptoServer Product Versions

Apart from tailor-made solutions CryptoServer also offers a broad range of standard interfaces, to simplify integration in your existing applications: amongst others for Microsoft's Crypto API (CryptoServer CSP), PKCS#11 (CryptoServer PKCS#11), a proprietary interface for the most used cryptographic services (CryptoServer CSI) and a standard interface for payment systems (CryptoServer EFTPOS). CryptoServer CSI is also available in a version which is certified against the security standard FIPS 140-2.

In all product versions, the CryptoServer hardware remains the same, the difference lays only in different software packages running on the CryptoServer.

All CryptoServer product versions are based on the CryptoServer hardware, with individual firmware loaded, and enhanced by a product-individual library running on the host PC. The library offers a specific C interface by which the CryptoServer can be accessed from a host application.

2.1 CryptoServer Standard Platform

The CryptoServer standard platform is designed for customers who want to develop their own application software. It is also the basis for specific CryptoServer applications and individual solutions developed by Utimaco.

CryptoServer offers a modular firmware concept. It is always delivered with certain standard firmware modules made by Utimaco, which provide the CryptoServer's operating system, an external interface for administration and firmware management, and an internal interface for all basic cryptographic functionality. This internal cryptographic interface can be used by customer-developed further firmware modules which may offer then their own customer-specific external cryptographic interface.

Utimaco may also provide you with a specific CryptoServer development environment (SDK). The modular firmware enables the functionality and algorithms to be upgraded at any time without hardware exchange.

The most important technical data about the CryptoServer standard platform can be found in the CryptoServer datasheet [CS_Data].

2.2 Security Server

The Security Server consists of the hardware security module CryptoServer added by the firmware packages CryptoServer PKCS#11, CryptoServer CSP and CryptoServer CSI.

2.2.1 Package CryptoServer PKCS#11

The package **CryptoServer PKCS#11** contains the firmware package files 'pkcs11XXX.mpkg' (where 'XXX' stands for further name extensions, e. g. package version numbers), together with a special PKCS#11 C-library running on the host by which the CryptoServer CSP can easily be accessed from a host application.

CryptoServer PKCS#11 provides a secure and accurate implementation of the PKCS#11 industry standard interface [PKCS11]. PKCS#11 has been designed from the ground as a cryptographic API intended to support external hardware security tokens, whereas other cryptographic APIs were initially developed to support software-based cryptographic processes.

Further information about CryptoServer PKCS#11 can be found in the CryptoServer PKCS#11 Interface Specification [CS-PKCS11_Spec] and the CryptoServer PKCS#11 datasheet (which gives a brief technical overview, see [CS-PKCS11_Data]).

2.2.2 Package CryptoServer CSP

The package **CryptoServer CSP** contains a firmware package file 'cspXXX.mpkg' (where 'XXX' stands for further name extensions, e. g. package version numbers). It provides hardware-based security and cryptography for simplified usage in Microsoft™ Windows environments.

With the **CryptoAPI (CAPI)**, Microsoft™ Windows systems offer a standard interface for cryptographic services, which is ready-to-use for any application running on a Windows system. Below this interface, a **Cryptographic Service Provider (CSP)** performs the cryptographic algorithms and mechanisms that can be addressed over the CryptoAPI. A CSP can be realized by a hardware security module, a smartcard or simply by a software library. The user can select his favorite CSP, but he can also easily switch to another CSP without changing his application software.

CryptoServer CSP is realized as a hardware security module CSP which offers the complete implementation of Microsoft CryptoAPI specification interface and which is interoperable with Microsoft's standard CSPs. It provides all cryptographic keys and secret data with the highest physical and logical protection.

Further information about CryptoServer CSP can be found in the CryptoServer CSP Technical Specification [CS-CSP_Spec] and the CryptoServer CSP datasheet (which gives a brief technical overview, [CS-CSP_Data]).

2.2.3 Package CryptoServer CSI

The package **CryptoServer CSI** (**C**ryptographic **S**ervice **I**nterface) consists of the firmware package files 'csiXXX.mpkg' (standard version), 'csiExtXXX.mpkg' (extended version with back-up functionality) and 'csiFIPSXXX.mpkg' (CryptoServer CSI in FIPS-mode, see below), added in all cases by a special CSI C-library running on the host PC by which the CryptoServer CSI can easily be accessed from a host application. (Herein again 'XXX' stands for further name extensions, e. g. package version numbers)

CryptoServer CSI provides a proprietary cryptographic interface which offers a broad range of standard algorithms for encryption and decryption, signature generation and verification, key generation, various hashing algorithms, true and pseudo random number generation, as well as integrated key management and an interface for administration.

CryptoServer CSI in FIPS-mode is certified according to FIPS 140-2 Level 3, with Level 4 in the area of "Physical Security". FIPS 140-2[1] specifies security requirements for cryptographic modules on different levels, where Level 4 is the highest possible level within FIPS 140-2. For the protection of sensitive information, US-American and Canadian Federal agencies are obliged to use FIPS 140-2-certified cryptographic modules exclusively.

Compared to the CryptoServer CSI standard version, there are slight restrictions in the provided cryptographic API if the CryptoServer CSI is used in FIPS-mode: for instance certain algorithms are not available in FIPS-mode (like hashing algorithm RIPEMD-160, or AES MAC calculation), and random number generation and, based on that, cryptographic key generation will exclusively be performed with a deterministic FIPS-Approved random number generator (and not with the CryptoServer's True Random Number Generator, which is based on a physical noise source). Furthermore, there are differences in the installation process and later administration.

Therefore, for all customers who are not obliged by law to use only FIPS-certified cryptographic modules, Utimaco recommends to use the CryptoServer CSI in its standard version or its extended version (with integrated back-up functionality and Master Box Key handling).

Further information about CryptoServer CSI (standard version, extended version and FIPS-certified version) can be found in the CryptoServer CSI Interface Specification [CS-CSI].

2.3 Payment Server

There exists a specialized CryptoServer solution for payment and banking systems, which can be used e. g. for card production (PIN block generation etc.) and in authorization systems, and which offers all kind of chip card and magnetic stripe card functionality for payment networks. This CryptoServer payment solution is offered in two variants: as **CryptoServer EFTPOS** (Electronic Fund Transfer Point of Sales) for german payment systems (ZKA functionality), and as **CryptoServer EFTPOS-VM** for Visa and/or MasterCard payment systems. CryptoServer EFTPOS is also certified against all ZKA security requirements.

The CryptoServer payment solution and the belonging firmware packages are not part of the Security Server. Information about the CryptoServer payment solutions is therefore not given in this document but is reserved to specific documentation.

[1] The FIPS 140-2 standard is issued by NIST (National Institute of Standards and Technology), acting also as the United States FIPS 140-2 Cryptographic Module Validation Authority.

3 General Overview

To set up a working CryptoServer system, apart from the hardware security module itself several other components are needed. Some of these components are optional, and depending on the customer's demands and application there is a big variety of options of how the CryptoServer system could be built.

In this section a short description will be given about all hardware and software components that are (optionally) involved, as well as an overview of how these components work together and fit into the complete system.

The visible components of a CryptoServer system and its general hardware architecture are the following:

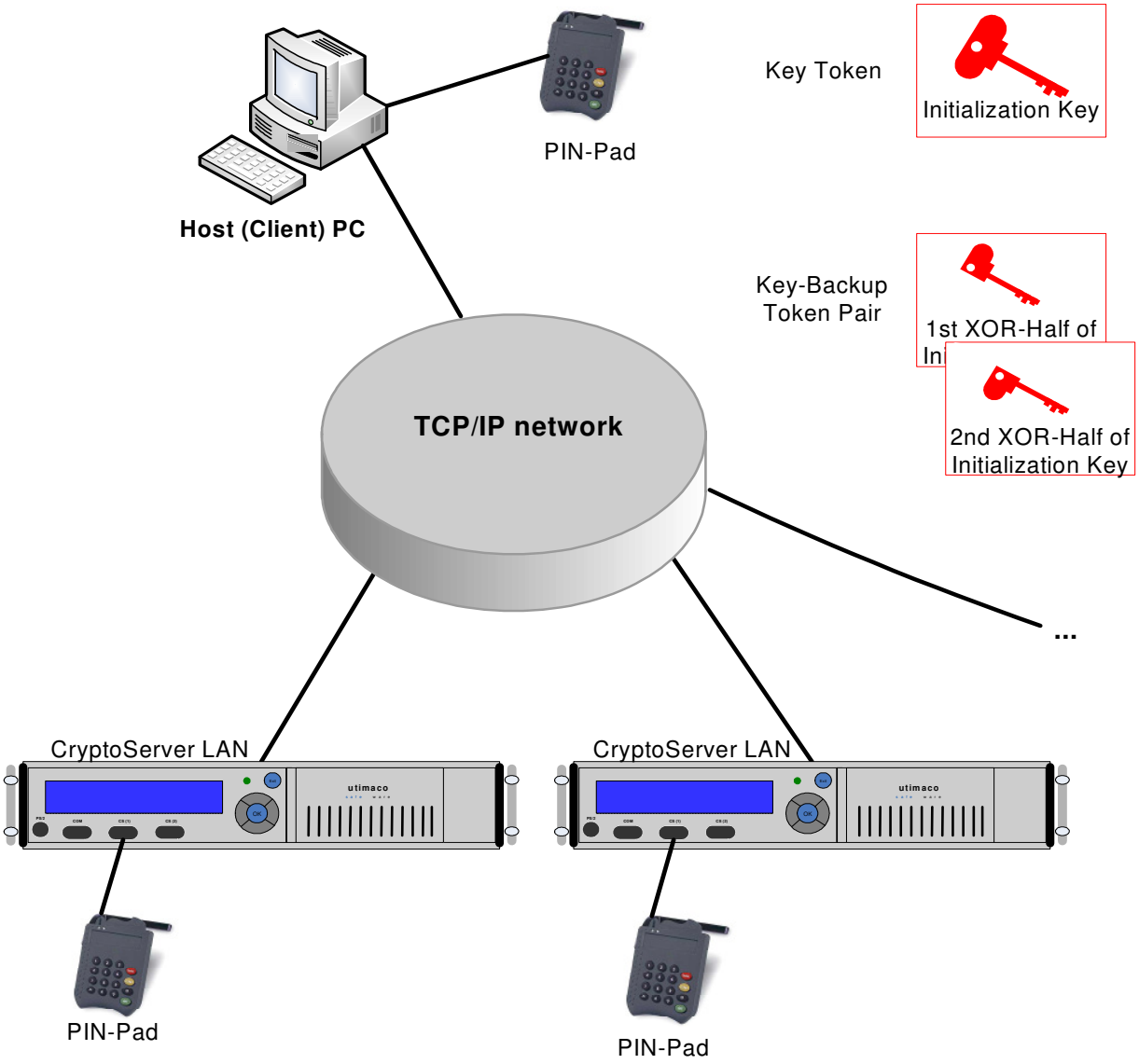

Illustration 1: CryptoServer system architecture

Inside the host PC, a CryptoServer PCI board may be included. The following illustration should give a rough overview about the various relevant and important software parts that are running on the host PC and about the communication paths between all software and hardware parts:

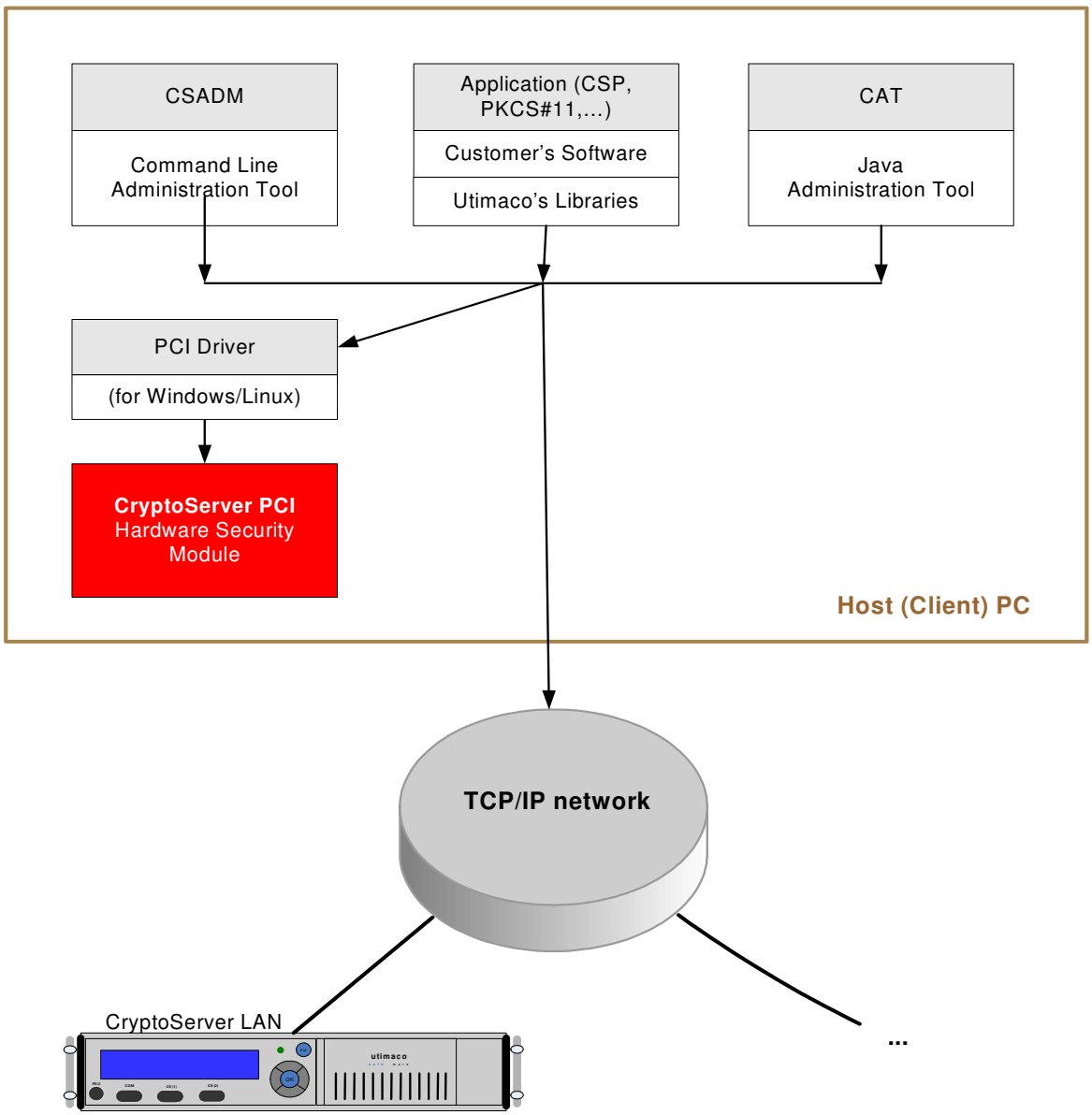

Illustration 2: CryptoServer host PC

Here, only one of the CryptoServer hardware security modules is mandatory, either as CryptoServer PCI board included directly in the host PC, or as CryptoServer LAN. Apart from that, all further CryptoServer/CryptoServer LAN are optional. In case that there is no CryptoServer PCI included on the host PC, the PCI driver software is of course also not needed.

Furthermore, the PIN-Pads are optional. In case a smartcard is used as key token to store the Initialization Key, at least one PIN-Pad is mandatory.

Generally, the key tokens to store the Initialization Key can be smartcards as well as other memory devices, or the key can even be stored in an (encrypted) key file on the PCs hard drive.

The application software running on the host obviously is application dependent and gives a C-interface either to one of the CryptoServers Security Server product packages (CSP, PKCS#11, CSI) or to further customer-individual applications.

The question if the CryptoServer is used locally as CryptoServer PCI plug-in card or remote via TCP/IP in its network-enabled variant CryptoServer LAN can only be answered individually and depends on the customer's IT (and personal) infrastructure and special needs. Also the question of how many CryptoServer/CryptoServer LANs are needed depends on the needs of performance and redundancy and the application environment.

In the following subsections short descriptions of the various components will be given.

3.1 CryptoServer PCI Board – the Hardware Security Module Itself

The **CryptoServer PCI board (CryptoServer)** is the hardware security module itself, a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys. It is the "heart" of the whole CryptoServer system.

The CryptoServer consist of an encapsulated, protected security module which is mounted on a PCI carrier card. Communication with a host PC and the "outer world" is realized over this PCI board, which supports a PCI interface as well as two serial interfaces (RS232), e. g. for connecting a PIN-Pad or printer to the CryptoServer.

The CryptoServer is encased in a hard opaque metal case which contains a tamper response envelope around the module: All hardware components of the cryptographic module (including the Central Processing Unit, all memory chips, Real Time Clock and hardware noise generator for random number generation) are located on a printed circuit board and encapsulated by metal shells, a special tamper detection envelope (which is a special foil bearing a flexible printed circuit with a serpentine geometric pattern of conductors) and potting material.

The following picture shows the CryptoServer PCI plug-in card:

Illustration 3: CryptoServer PCI-board

The CryptoServer offers cryptographic services via a well-defined command interface. Details of this command interface depend on the implemented firmware and thus in particular on the special CryptoServer product version that is used.

See also datasheet [CS_Data] and the installation manual [CS2Install-Manual] for more details and technical data of the CryptoServer hardware.

3.2 CryptoServer LAN – Hardware Security Module with Network Interface

CryptoServer LAN is the hardware security module in its network-enabled variant. With its TCP/IP Ethernet interface it is the ideal solution for a centralized storage, application and administration of cryptographic keys within any TCP/IP network. It is as well possible to call CryptoServer LAN's cryptographic services from several host PCs within the network, as well as to use several CryptoServer LAN devices parallel in a cluster.

Illustration 4: CryptoServer LAN

CryptoServer LAN consist of a 19”/ 2U housing communication unit which includes one CryptoServer PCI board and which offers a Gigabit network interface (10/100/1000 MBit; and optionally a second network interface), permitting up to 10,000 parallel connections.

A display and a keypad, 3½“ floppy drive and RS232 interface for PIN-Pad connection allow for comfortable local administration. Additionally CryptoServer LAN offers a PS/2 interface for keyboard connection on the front face, a parallel port for printer connection (e. g. for printage of logging output), a USB port, and a serial V.24 interface, if direct connection of a PIN letter printer or a PIN-Pad to the integrated CryptoServer hardware security module is required (e. g. for key management).

Thus secure administration and maintainance can be done either locally (over the integrated display) or remotely (TCP-based) from any PC within your network with installed administration software. CryptoServer LAN is cluster-enabled, for flexible scaling and redundancy.

Further details about the hardware and hardware installation of the CryptoServer LAN can be found in the Operating Manual [CSLANOpManual] and the datasheet [CSLAN_Data]. In CryptoServer LAN’s User Manual [CSLANUserManual] all necessary information for initialization, set-up and usage of the device is given.

3.3 Host PC

The host PC serves as communication interface for administrator and user of the CryptoServer system. It is equipped with the necessary software to address the command interface of any CryptoServer which is included in the system: the administrative command interface as well as the customer-dependant application command interface. Optionally a CryptoServer PCI board might be integrated (as PCI-plug-in card) in the host PC.

It is always assumed that a monitor and a keyboard are connected to the PC.

In your network also more than one host PCs may be included. In this case any of these host PCs may address any of the CryptoServer LANs in your system over the TCP/IP interface, plus the CryptoServer PCI board which is optionally integrated in the host PC itself.

The following software may run on the host PC:

- **CAT**, a Java tool for simplified and user-friendly administration of CryptoServer (PCI and LAN) and for key management and user tasks for CryptoServer's standard applications.
- The **application software**, consisting of basic C-libraries delivered by Utimaco plus customer-specific software.
- **PCI-driver** for communication with integrated CryptoServer PCI-board (only if CryptoServer PCI included).
- **CSADM**, a command line tool for extended administration of CryptoServer (LAN).

Only one of the CryptoServer administration tools, CSADM or CAT, is mandatory. Which tool should be prefered depends on the specific customer's needs.

The various software parts will be explained below.

3.4 CAT: CryptoServer's Java Tool for Administration

CAT (**C**ryptoServer **A**dministration **T**ool) is a Java tool for simplified and user-friendly administration of any CryptoServer or CryptoServer LAN. The Java GUI provides the user with an intuitive, self-explanatory administrative interface which does not need much further documentation.

CAT offers less administrative functionality than the command line tool CSADM (see 3.5 below), but still contains all basic administration functionality which will be needed for any CryptoServer application, like firmware management and status output. Additionally it offers all functionality for key management and user management tasks for CryptoServer's standard packages CryptoServer PKCS#11, CryptoServer CSP, CryptoServer CSI and CryptoServer EFTPOS.

For all customers who implement one of the CryptoServer's standard applications it is strongly recommended to use CAT for any CryptoServer's administration.

3.5 CSADM: CryptoServer's Command Line Tool for Administration

CSADM (**C**rypto**S**erver **Adm**inistration) is a command line tool for the extended administration of CryptoServer/CryptoServer LAN. In addition it contains utility functions which will be processed without a connection to any CryptoServer (e. g. preparing of firmware modules). It offers a broader set of administration functionalities than the Java Tool CAT (see 3.4) and is thus recommended for customers who are more experienced in CryptoServer usage and administration, and in particular for those who develop their own CryptoServer firmware.

The CryptoServer Administration Guide [CSAdmGuide] contains a detailed description of CSADM and a user manual for all CSADM functionality, and it gives guidelines of how to administrate the CryptoServer with CSADM.

3.6 Application Software

All CryptoServer product versions are delivered with product-individual C-libraries running on the host. These libraries offer a specific C-interface by which the CryptoServer can be accessed from a host application. It hides the CryptoServer's byte stream interface and PCI driver usage from the customer's application.

The following table shows the libraries of the specific CryptoServer product versions (for all possible host PC operating systems that are supported), and the C header files which have to be included:

Product / Package	Library		Header Files
	Windows	Linux or Solaris	
Standard Platform	csapi.lib (use with csapi.dll) csapi_s-x.y.z.lib (static library)	libcsapi-x.y.z.a	csapi.h csa_auth.h csa_chnl.h csa_cluster.h csa_cmds.h csa_sm.h
PKCS#11	cs2_pkcs11.lib (use with cs2_pkcs11.dll)	libcs2_pkcs11-x.y.z.so libcs2_pkcs11_m-x.y.z.a	cryptoki.h pkcs11.h pkcs11f.h pkcs11t.h
CSP / CNG	cs2csp.dll cs2cng.dll cs2cng.cpl	-	-
CSI	cs_csi.lib (use with cs_csi.dll) cs_csi_s.lib (static library)	libcs_csi.a	cs_csi.h

All C-libraries and header files are stored on the CryptoServer product CD in directory '\Software' and there in the various subfolders (where folder 'CSAPI' stands for the CryptoServer Standard Platform).

The host application has to be developed by the customer himself, according to his needs, and based on Utimaco's libraries as a lower layer. The customer's application software thus has to use Utimaco's libraries.

The application software now consists of these two software parts: customer's application software and included Utimaco's libraries, and it offers finally the user interface according to the customer's needs.

Since for CryptoServer CSP (which is of course only usable on Windows systems) the complete application software is given by Microsoft's CryptoAPI, in this case no host application has to be created by the customer and thus no C header file is necessary.

3.7 Initialization Key

The Initialization Key, a cryptographic RSA key which is stored on a key token, is mandatory for the authentication of security relevant administration functions to be performed on the CryptoServer:

Many tasks connected with the administration of a CryptoServer's system are security relevant, in particular the management of CryptoServer's firmware modules (e. g. download, replacement and deletion of firmware modules). These administrative functions shall only be performed by authorized personnel and have to be protected against non-authorized access.

Thus all security relevant administrative tasks can only be performed after a special form of authentication.

*Main tool for authentication of administrative tasks is the **Initialization Key**, a cryptographic RSA key which is stored on a key token (smart card or any other storage medium). If stored on smartcard, the Initialization Key is protected by PIN. If stored on any other medium, it should be stored in form of an encrypted and password-protected key file (see Link).*
The public part of the Initialization Key is stored inside the CryptoServer. This key is used to authenticate most security-relevant administrative commands.
The customer alone bears responsibility for the Initialization Key!

Usually, if the concerned CryptoServer system is not a test system, Utimaco does not know the *Initialization Key*; in particular, Utimaco does not have a back-up copy of the key!

For a productive CryptoServer system the customer bears full responsibility for the Initialization Key. A CryptoServer's administrator should be assigned who has, for the beginning, the task to generate the Initialization Key (see sections 5 and 7.1) and store it on a key token, for instance on a smartcard.

Because of the importance and the power of the *Initialization Key*, it is highly recommended to generate at least one **back-up copy of the key** and to store the key(s) very carefully, e. g. in a safe. Only few authorized persons, among these the CryptoServer's administrator(s), should be given access to it.

The key back-up will be stored in form of two XOR key halves on two separate smartcards, or as a copy of the original Initialization Key. All (back-up) key tokens should be kept secure and separate of each other.

See section 7.1 for a detailed description of how to generate and back-up your Initialization Key.

In case a CryptoServer test system is used, Utimaco will provide you with Utimaco's *standard Initialization Key*, stored on a smartcard. Since this standard key is well-known to Utimaco and every Utimaco customer using a CryptoServer test system, its use is strictly restricted to test purposes. Under no circumstances this key shall be be used in any productive environment.

*The **PIN of Utimaco's standard Initialization Key**, at the time of deliverance, is set to **"123456"**.*

For more background information of the meaning and tasks of the Initialization Key, see 4.2 and CryptoServer's Administration Guide [CSAdmGuide] section 3.6.2 *Customer's Initialization Key* K_{INIT}.

3.8 PIN-Pad

For many CryptoServer applications one or several PIN-Pads are needed, consisting of a key pad, a display and a smart card reader. The smartcard reader will in particular be used to get access to the Initialization Key (in case that the Initialization Key is stored on smartcard), but also to other cryptographic keys which are stored on a smart card.

In most cases, one PIN-Pad has to be connected to the host PC on which the administration tools are running (see *Illustration 1: CryptoServer system architecture*). This PIN-Pad will serve for supporting administrative tasks, in case the Initialization Key is stored on a smartcard, and in some cases also for key management tasks.

One or two PIN-Pads may be connected to any CryptoServer LAN which is part of the whole CryptoServer system:

- For the purpose of local administration and maintenance, a PIN-Pad might be connected at the front of each CryptoServer LAN.
- For specific key management tasks which afford a direct connection of smartcard reader to the integrated CryptoServer PCI-board (to avoid any possibility of data interception), a second PIN-Pad may be connected directly to the integrated CryptoServer PCI.

See section 9 for more information about which PIN-Pads can be used, and how to connect and operate them.

3.9 Key-Tool

Utimaco provides you with two possibilities to generate, store and back-up your own cryptographic keys (like Initialization Key):

1. There are key generation functionalities integrated in the CryptoServer's Administration Tool **CAT**.
   The resulting key and key back-ups can be stored on smartcard as well as in a key file (eventually encrypted) e.g. on floppy disk, USB-stick or directly on hard drive. But for key and key back-up the same storage medium (smartcard or key file) has to be chosen.

2. Additionally, Utimaco offers a specialized **Key-Tool** for a high secure way of key generation. Key-Tool is a software program located on bootdiskette, i. e. on a floppy disk with which a computer has to be booted.
   The resulting key can only be stored on smartcard. The key back-ups can be stored on smartcard as well as on diskette.

Both tools do not differ in the resulting smartcards (if smartcard is chosen as storage medium), but in the security level of the environment that they offer during the process of key generation and storage.

Which tool has to be used depends on the customer's security policy:

- *For most security needs, key generation with **CAT** offers a sufficient level of security.*
- *For highest security needs, the usage of Key-Tool is recommended:*
  Since Key-Tool is started from a boot diskette on a PC, the PC is operated without harddisk usage during Key-Tool's runtime. Therefore no possibility exists that underhand the generated key might be stored on the PC.
  Furthermore, Key-Tool takes the input for the "seed" (initial value) for its key generation algorithm from random keyboard entries, whereas CAT takes the seed input from internal PC data.

The Key Tool (as well as CAT) offers also the functionality to change the PIN.

For more information about Utimaco's CryptoServer Key-Tool and its usage, see the Key-Tool User Manual [CSKeyTool].

4 Security Concept

4.3 Alarm

The physical security of the hardware security module CryptoServer is mainly provided by its alarm mechanism:

Anytime a physical alarm happens to the CryptoServer, it will immediately be detected by the CryptoServer's integrated sensory which permanently watches temperature, voltage and chemical or mechanical attack, i. e. destruction of the foil. The sensory then directly triggers a well-defined alarm mechanism. Part of this mechanism is the erasure of all sensitive data and firmware, alarm logging and a restart of the CryptoServer.

If an alarm has occurred to the CryptoServer, this will be announced with the *Get CryptoServer State* command (**alarm = ON**), see Link. The detailed alarm reasons can be seen from the '**sens = (…)**' text which follows the 'alarm = ON' line. Generally, two different kinds of alarm are possible:

- Temporary alarms.
- Permanent alarms.

Only temporary alarms can be reset. Permanent alarms cannot be reset. Permanent alarms occur in case of a damage of the inner or outer tamper protecting foil, whereas usually all other possible alarms are temporary.

Possible reasons for alarm are

Abbreviation	Explanation
Temp_low	Temperature too low (see also 4.4)
Temp_high	Temperature too high (see also 4.4)
In_foil	Internal foil damaged
Out_foil	External foil damaged
Pow_high	Voltage/tension too high
Pow_low	Voltage/tension too low
ext_Erase	External deleting/clearing done
inval_MK	Invalid (corrupted) Master Key $\mathbf{K_{CS2}}$. Reason for this is usually an empty battery which then had to be exchanged (see 8.3.1).

Whenever a physical alarm occurs, all sensitive data, including CryptoServer's internal Master Key $\mathbf{K_{CS2}}$, will be erased immediately by hardware (within less than 4 msec after the occurrence of the alarm), and the CryptoServer will be restarted.

During the (following) boot process the boot loader erases all remaining data and firmware in order to set the CryptoServer back to the *initialized* state:

In case of an alarm, all firmware modules inside the CryptoServer will be deleted, as well as all customer's data except the public Initialization Key*.*
The CryptoServer is now in the initialized *state and in bootloader mode.*

Thus after an alarm, the CryptoServer contains only the boot loader code but no further firmware. Furthermore, the customer's public *Initialization Key* $\mathbf{K_{INIT\text{-}PUB}}$ as well as the alarm logfile will remain but no other customer-related keys and data.

During the boot process after an alarm the CryptoServer adds up an entry provided with timestamp into the ***alarm logfile****, in which also the alarm cause is stated. This alarm logfile can anytime and in any mode (boot loader mode or operational mode) be read out with the help of the* Show Alarm Logfile *command (see Link).*

If during the following restart process the physical alarm is not present any more (i. e. the cause of the alarm was corrected in the meanwhile, e. g. an old battery has been already replaced by a fresh one in case of a low-power-alarm) the boot loader continues with the boot process. But before any further command can be executed, the alarm has to be explicitely reset by the user.

Before the CryptoServer accepts any further commands, each alarm must explicitly be reset by the user: this has to be done by executing the Reset Alarm *command (see Link). By the fact that this* Reset Alarm *command must be authenticated by the* Initialization Key*, it is ensured that at least one responsible person has been informed about the occurrence of each alarm.*

If the *Reset Alarm* command has been performed successfully, the boot process will continue. If this is not possible, the CryptoServer cannot leave the alarm state.

If the physical alarm cause has not been remedied before the Reset Alarm *resetting, hardware will trigger a renewed CryptoServer's reset and the procedure will be repeated.*
Therefore a permanent alarm, e. g. foil damages, cannot be reset, in which case you are required to contact the manufacturer/Utimaco.

For the accurate procedure "What to do?" in case of an alarm see chapter 8.2.

4.4 Behavior of CryptoServer outside the Normal Temperature Range

If the internal temperature of the CryptoServer gets outside of the normal operating temperature range, the CryptoServer will behave in a special way, as shown in the table below:

Temperature	Behavior of the CryptoServer
below –13°C	An alarm is triggered and the CryptoServer enters *power down mode*.
–13°C to 5°C	The CryptoServer enters power down mode.
5°C to 58°C	Normal operation.
58°C to 66°C	The CryptoServer enters power down mode.
above 66°C	An alarm is triggered and the CryptoServer enters power down mode.

All temperature values in the table are approximate values. The exact temperature values may vary a little because of tolerances of the electronic components and the use of a hysteresis by the comparators.

Note that only the temperature inside the inner case of the CryptoServer device is relevant, not the environment temperature. The actual value of the inner temperature can be retrieved with the Get CryptoServer State *administration command.*

Once the CryptoServer has entered power down mode, it does not respond to any request. An attempt to access the CryptoServer will usually result in a kind of timeout error from the device driver.

Before entering power down mode the CryptoServer writes an entry into the temperature logfile which can be read out with the administration command *Get Temperature Logfile* (see Link).

The only way to get the CryptoServer out of the power down mode (and to get it into operational mode again) is to reset it using the *Reboot CryptoServer* command.

Resetting the CryptoServer has no effect if the temperature is still outside the normal range. In case of CryptoServer's power down caused by high temperature, it is recommended to switch the supply power off for some time in order to cool the CryptoServer down.

5 Installation

In this chapter the complete process of hardware and software installation and set-up is described.

General Preconditions:

Requirements for all host PCs on which the administration software is running (regardless if a CryptoServer is installed directly or a CryptoServer LAN is connected remotely) are the following:

PC-Hardware:

- no special requirements as far as memory and CPU performance is concerned.
- if CryptoServer LAN is used: network interface card to access CryptoServer LAN
- if a PIN-Pad is needed: one free serial port to connect the PIN-Pad.
- CD-drive

PC-Software (OS):

- Windows NT 4.0 Service Pack 4 (or higher), or
- Windows 2000/2003, or
- Windows XP, or
- Intel-based Linux (kernel version >= 2.4.0), or
- Solaris (only if CryptoServer LAN is used, and only for administration tool CSADM, not for CAT), version 5.8 or higher

In many applications additionally a PIN-Pad (smart card reader with keyboard and display) is needed. See section 9, *Appendix: PIN-Pads*, for details about connection and usage of PIN-Pads.

Guide for Installation:

Generally, the installation of a complete CryptoServer system is as follows:

Step 1. First the necessary hardware, i. e. the hardware security device/s, has/have to be installed, including driver installation. See section 5.1 for the installation of every CryptoServer, respectively section 5.2 for the installation of every CryptoServer LAN device in your system.

Step 2. Now all PIN-Pads should be connected, as far as wanted. Connecting a PIN-Pad is mandatory in all cases where the Initialization Key is stored on smartcard.
See 9.1 for how to connect a PIN-Pad to either the host PC or a CryptoServer LAN device.

Step 3. After hardware installation the necessary administration software, documentation and libraries have to be installed on every host PC which shall be used for CryptoServer administration and usage. Administration software can be either the command line tool CSADM, or the user-friendly Java administration tool CAT, or both (see 3.4 and 3.5 for more information about both administration

tools).
On Windows systems, all software and documentation can easily be installed in one step with the CryptoServer setup program, on Linux or Solaris systems the installation has to be done manually. See section 5.3.

Step 4. Generate your own Initialization Key (see 5.4).

Step 5. Now the hardware security modules CryptoServer/CryptoServer LAN have to be setup and initialized. This mainly comprises download of software for every device, creation of users and some key management tasks and is highly dependant from the wanted application.
See 5.5 for a description of the setup and initialization process for all CryptoServer product versions.

Step 6. After this your own application software, running on the host PC, has to be prepared and loaded on the PC. See section 3.6.

Step 7. Now your CryptoServer system is ready for usage within your wanted application.

See section 5.6 for how to de-install any software on your PC.

5.1 Installation CryptoServer

If you are using the CryptoServer PCI card, this PCI plug-in card has to be installed first in your host PC, as well as the necessary host software like the PCI driver.

Preconditions:

For this step the CryptoServer's Installation Manual must be on hand [CS2Install-Manual], as well as the CryptoServer product CD.

If later a PIN-Pad shall be used, you need one free serial port to connect the PIN-Pad at your PC.

CryptoServer PCI driver's installation is only possible for Windows or Linux systems but not for Solaris systems, see above.

What to do:

1. Install the CryptoServer PCI plug-in card. Instructions for the hardware installation can be found in [CS2Install-Manual]. Please read and follow also the included security advices.
2. Install the CryptoServer's PCI driver according to the instructions given in [CS2Install-Manual], section 5.[2] You will find the necessary PCI driver software and files on the CryptoServer product CD, folder 'Driver\[Windows|Solaris|Linux]'.

[2] Please ignore the there given instructions for CSADM installation and PCI driver testing. These steps will automatically be part of the host software installation described below in 5.3.

Installation under Windows 2000/W2K3/XP/Vista/W2K8

Driver installation under Windows 2000/2003/XP will be done in a windows-based installation process which will be started automatically when the PC is booted for the first time after the CryptoServer PCI board installation. See [CS2Install-Manual] sections 5.2.2 and 5.2.3.

When you will be asked for the CryptoServer's PCI driver, please insert the CryptoServer product CD in the PC's CD drive, and enter the respective path to the driver software (folder 'Driver\Windows').

Driver Installation under Linux OS

Please note the following warning:

The driver for the CryptoServer will be delivered as source code only and must be compiled on the target system. This requires some Linux know-how. The driver sources are located on the CryptoServer product CD in the directory '\Driver\Linux' for Kernel-2.4.x and 2.6.x. There are also example makefiles that can be used as compilation template.
Read the instructions in the Linux kernel documentation (available e. g. at http://www.kernel.org) under 'Documentation\kbuild\modules.txt', or ask your Linux guru.
For further information please read section 5 in the [CS2Install-Manual].

3. Continue with Step 2 above, or with the installation of further CryptoServer LAN devices.

5.2 Installation CryptoServer LAN

If you are using one or several CryptoServer LAN boxes, these devices have to be installed and connected to your network.

Preconditions:

The following equipment has been delivered together with CryptoServer LAN:

- the CryptoServer LAN Operating Manual (see also [CSLANOpManual])
- 1 power supply cable
- 1 PS/2 Y adapter, for the connection of mouse and keyboard, 1x6pin mini-DIN plug-on, 2x6pin mini-DIN socket, length: 0.2m

Please check if all components are available.

In most cases a PIN-Pad has been delivered as well.

Additionally you will need the CryptoServer LAN User Manual [CSLANUserManual].

The requirements for CryptoServer LAN installation are a 100-240 V power supply and a 10/100/1000 MBit Ethernet link. For service purposes and troubleshooting you need a standard VGA monitor and a PC keyboard with a PS/2 connector.

What to do:

1. Install the CryptoServer LAN device. Instructions for the hardware installation and connection to your network can be found in the CryptoServer LAN's Operating Manual, see [CSLANOpManual] section 3. Please read and follow also to the included security advices.
2. Connect the CryptoServer LAN to your network. Additionally it is possible to connect to the CryptoServer LAN from outside your current network. A description for both processes including how to check the network connection is given in the CryptoServer LAN User Manual [CSLANUserManual], section 3, in particular section *3.1 Installation*. Once the device is switched on, the system automatically powers up. After approx. 30 seconds the CryptoServer LAN is ready for operation.
3. Now the CryptoServer LAN communication unit (LAN box) itself can be configured, respectively the configuration can be changed if wanted. See [CSLANUserManual] section *3.4 Administration* for the various possibilities to do so. In the User Manual also all necessary administration tasks (e.g. for later maintainance) for CryptoServer LAN is explained.
4. Repeat this step for every CryptoServer LAN device.
5. Continue with Step 2 above.

5.3 Installation of CryptoServer Host Software

In this step the following software, together with further documentation etc., will be installed on your host PC which is communicating with the CryptoServer respectively CryptoServer LAN:

- **CryptoServer Administration Tool CAT:** CAT is the Java tool for a simpified administration of one or several CryptoServers and/or CryptoServer LAN devices in your network. It comprises the most important administrative functionality that is also offered by CSADM, plus certain standard management functionality depending on the implemented application (PKCS#11, CSP, CSI, EFTPOS).
- **CSADM:** CSADM is Utimaco's command line utility for extended administration of CryptoServer.
- **Application Software on host PC:** The CryptoServer product specific libraries and header files that have to be used to generate your customized host application software will be stored on the host PC, as well as all documentation about Utimaco's libraries and its C-interfaces. For a description of the application software see chapter 3.6.
- **Documentation:** Several documents for user guidance, manuals, technical information about the CryptoServer and interface specifications about the firmware packages and Utimaco's libraries will be stored on your host PC.

General Preconditions for Installation:

For the basic requirements of the host PC (OS etc.) see chapter 5 above.

To install CAT on a PC, the PC needs a Java environment version 1.4.2_01 or higher.

On Windows systems, in case that this Java environment is not available in the requested version yet, Java version 1.5.0_02 will be installed automatically from CD as part of the automatic installation procedure.

5.3.1 Setup Installation on Windows Systems

What to do:

1. To install the CryptoServer Software on a host PC, insert the CryptoServer Product CD in the CD drive of your PC.
2. If on your PC the autostart option for CDs is enabled, the CD Menu starts automatically. Otherwise you have to start the Setup Program **'CryptoServerSetupVx.y.z.exe'** (where x.y.z is the respective Setup version number).
3. Now the CD Menu will be shown in a browser. Please select 'Install' and go to the section 'CryptoServer Administration Tool CAT'. There click 'Install the CryptoServer Administration Tool'.
4. During the setup process you have to choose between different installation options:

Developer Installation: This includes the complete installation of the administration tools and storage of all firmware packages, software and documentation.

In case of doubt, this option should be choosen.

Runtime Installation: This comprises the installation of the tools CAT and CSADM and the storage of all firmware packages.

This option can be choosen if the host PC shall only be used to administrate one or several CryptoServer(s).

Custom Installation: With this installation option you can choose explicitly which tools, firmware packages, software and documentation shall be installed.

5. Furthermore, you have to choose a folder on your PC where all these files and data shall be installed. Throughout this User Guide documentation this folder will be denoted as **{CryptoServer} folder**.
6. Finish installation.

After installation there are three subdirectories below the {CryptoServer} folder on your PC:

Folder	Folder Contents
Administration	Contains the CryptoServer Administration Tool CAT (see chapter 3.4), the command line tool CSADM (see chapter 3.5) and the standard firmware packages.
Documentation	Contains all documentation (for administration, specifications and programming).
Programming	Contains libraries, header files and binaries needed to program the CryptoServer.

5.3.2 Installation on Linux or Solaris Systems

What to do:

1. If you want to install the administration commandline tool CSADM, copy the program file ‘Software\Administration\csadm\<platform>\csadm’ from the CryptoServer product CD to the desired destination folder on your PC.
2. The CryptoServer Administration Tool CAT is only available for Linux, not for Solaris. If you want to install CAT on a Linux system, copy all files that are contained in the folder 'Software/Administration/CAT/linux' to the desired destination folder. Furthermore you have to copy the wanted firmware packages, which can be found in the folder 'Firmware' of the product CD, to the desired destination folder.

To start CAT the shared library 'libadm_native.so' must be loaded by the java archive. Therefore the runtime linker has to know the location of this library. There are three possibilities to configure this option:

a. Set the environment variable `LD_LIBRARY_PATH` to the appropriate path of the shared object (where you have copied CAT):
   `# export LD_LIBRARY_PATH=/path/to/lib`

b. Copy the library 'libadm_native.so' to a directory that is already known by your runtime linker (e.g. `/usr/lib`).

c. Add the location of the folder that contains the shared library to the configuration file `/etc/ld.so.conf` and execute the command `ldconfig`.

CAT can now be started from the shell with the command:

```
# java –jar cs2admin.jar
```

3. For the development environment you have to copy the following header files and libraries to a destination folder which is reachable by your C compiler.

Package[3]	Header File(s)	Library
PKCS#11	'Software/PKCS#11/include/cryptoki.h' 'Software/PKCS#11/include/pkcs11.h' 'Software/PKCS#11/include/pkcs11f.h' 'Software/PKCS#11/include/pkcs11t.h'	'Software/PKCS#11/lib/linux/libcs2_pkcs11_m-n.n.n 'Software/PKCS#11/lib/linux/libcs2_pkcs11-n.n.n.so
CSI	'Software\CSI\include\cs_csi.h'	'Software\CSI\lib\windows\libcs_csi.a'

4. Since for the development of both packages the header files and the library of the CSAPI (CryptoServer API) library need to be present, please copy additionally the following files to a folder reachable by your C compiler:

Header File(s)	Library
'Software/CSAPI/include/csapi.h' 'Software/CSAPI/include/csa_auth.h' 'Software/CSAPI/include/csa_chnl.h' 'Software/CSAPI/include/csa_cluster.h' 'Software/CSAPI/include/csa_cmds.h' 'Software/CSAPI/include/csa_sm.h'	'Software/CSAPI/lib/windows/libcsapi-n.n.n.a

5. Too simplify the usage of the commandlinetool CSADM you should create an environment variable 'CRYPTOSERVER' for the address of the CryptoServer. The value of the variable is "/dev/cs2" if the CryptoServer is installed in a PC locally (CryptoServer PCI board), or "TCP:288@<IP-Address of the CryptoServer LAN>" if a CryptoServer LAN is used.

[3] For evident reasons, the package CryptoServer CSP does only run on Windows systems and thus is not mentioned here.

5.3.3 Manual Installation on Windows Systems

What to do:

1. If you want to install the administration commandline tool CSADM, copy the program file ‘Software\Administration\csadm\windows\csadm.exe’ from the CryptoServer product CD to the wanted destination folder on your PC.
2. If you want to install the CryptoServer Administration Tool CAT, copy all files that are contained in the folder 'Software\Administration\CAT' to the wanted destination folder on your PC.
   Furthermore you have to copy the wanted firmware packages, which can be found in the folder 'Firmware', to the wanted destination folder.
3. In order to install the runtime environment you have to copy some files to local directories. In dependence on the selected firmware package the following files have to be copied:

Package	Source File(s)	Target Directory
PKCS#11	Software\PKCS#11\lib\windows\cs2_pkcs11.dll	any
CSI	Software\CSI\lib\windows\cs_csi.dll	any
CSP / CNG	Software\CSP\windows\cs2csp.dll Software\CSP\windows\cs2cng.dll Software\CSP\windows\cs2cng.cpl	%SystemRoot%\system32
Standard Platform	Software\CSAPI\lib\windows\csapi.dll	any

   Please make sure that all target directories are reachable, edit the PATH-variable if needed.

   If you install the package CryptoServer CSP you additionally have to create some registry (sub-)keys below the following registry keys:

   a. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Utimaco CryptoServer CSP:

Key	Type	Value
Image Path	REG_SZ	cs2csp.dll
SigInFile	REG_DWORD	0x00000000
Type	REG_DWORD	0x00000001

4. For the development environment you have to copy the following header files and libraries to a destination folder which is reachable by your C compiler:

Package	Header File(s)	Library
PKCS#11	'Software\PKCS#11\include\cryptoki.h' 'Software\PKCS#11\include\pkcs11.h' 'Software\PKCS#11\include\pkcs11f.h' 'Software\PKCS#11\include\pkcs11t.h'	'Software\PKCS#11\lib\windows\cs2_pkcs11.lib'

CSI	'Software\CSI\include\cs_csi.h'	'Software\CSI\lib\windows\cs_csi.lib'

5. Since for the development of all packages the header files and the library of the CSAPI library need to be present, please copy additionally the following files to a folder reachable by your C compiler:

Header File(s)	Library
'Software\CSAPI\include\csapi.h' 'Software\CSAPI\include\csa_auth.h' 'Software\CSAPI\include\csa_chnl.h' 'Software\CSAPI\include\csa_cluster.h' 'Software\CSAPI\include\csa_cmds.h' 'Software\CSAPI\include\csa_sm.h'	'Software\CSAPI\lib\windows\csapi.lib'

6. Too simplify the usage of the commandline tool CSADM you should create an environment variable 'CRYPTOSERVER' for the address of the CryptoServer. The value of the variable is "PCI:0" if the CryptoServer is installed in a PC locally (CryptoServer PCI board), or "TCP:288@<IP-Address of the CryptoServer LAN>" if a CryptoServer LAN is used.

5.4 Generate Your Own Initialization Key

Precondition:

- You have to decide if CAT or Key-Tool shall be used for Initialization Key generation, see 3.9. If you have decided to generate the keys with the Key-Tool, the Key-Tool boot diskette and the user manual [CSKeyTool] must be on hand.
- You have to decide if your Initialization Key shall be stored on smartcard (INIT smartcard) or on any other storage medium (e.g. floppy disk, USB stick or just in a key file on the hard drive). The respective (empty) key tokens have to be on hand.
- You have to decide how many copies of the Initialization Key and how many key back-ups shall be produced. The respective (empty) key tokens have to be on hand.

As smartcard key tokens, Utimaco's "CryptoServer 2000" smartcards have to be used.

For the Security Server (CryptoServer PKCS#11, CryptoServer CSP, CryptoServer CSI) a simple minimal solution is to generate

1. *one Initialization Key, and to store at least*
2. *one copy of the Initialization Key.*

In case that smartcards shall be used, two empty "CryptoServer 2000" smartcards have been delivered by Utimaco together with every CryptoServer for this purpose. These two smartcards must be on hand.

What to do:

- Generate the wanted number of Initialization Key tokens, Initialization Key copies and key back-ups by following carefully the instructions in 7.1.

  Recommandation for a simple minimal solution:

  Generate one Initialization Key and at least one copy of the Initialization Key.

  For the most simple solution, store the keys and copies as (encrypted) key files (see Link) on any medium.

  For a more secure solution, store the key and the copy on one smartcard each, using the two empty “CryptoServer 2000” smartcards for this purpose.

- CryptoServer’s Administrator is responsible for the (customer’s) Initialization Key. All keys should be stored very carefully, e. g. in a safe. Only few authorized persons should be given access to it.
- **Keep all Utimaco’s standard Initialization Key key tokens for possibly later usage (e. g. after repair).**
- Continue with Step 5 above.

5.5 Initialisation/Set-Up of CryptoServer (LAN)

For this step it is assumed that the CryptoServer Java Administration Tool CAT has been installed and will be used. For how to set-up and initialize CryptoServer with CSADM see [CSAdmGuide] chapter 6.

Setting up the CryptoServer/CryptoServer LAN basically means loading the appropriate software (firmware modules), creating users and loading the needed cryptographic keys. The details of the process depend on the wanted application.

The following steps have to be repeated for every CryptoServer/CryptoServer LAN that shall be set-up and initialized. Some steps can be omitted in case a CryptoServer test system is used (i.e. a CryptoServer which shall only be used for test purposes: with firmware already loaded by Utimaco and using Utimaco's standard Initialization Key).

Precondition:

The respective firmware package file '*.mpkg' must be on hand. For the CryptoServer standard applications CryptoServer CSP, CryptoServer CSI and CryptoServer PKCS#11 you can find the respective firmware package file on your host PC in the folder '{CryptoServer}\Administration\Firmware', or on the CryptoServer product CD, folder 'Firmware'.

The customer's Initialization Key must be on hand, as well as Utimaco's standard Initialization Key.

Furthermore you need your customer-individual CryptoServer licence file.

What to do:

1. Set the CryptoServer's device address (see Link).
2. Set the data for accessing the Initialization Key (see Link). If the Initialization Key is stored on floppy disk (or hard disk), the name and path of the key file has to be given. If the Initialization Key is stored on smartcard, the used PIN-Pad type and the port where the PIN-Pad is connected have to be given.
3. Change the Initialization Key: Utimaco's standard Initialization Key that is loaded on the CryptoServer at the time of delivery has to be replaced by the newly generated customer's Initialization Key. See 7.2.
   This step can be omitted if a CryptoServer test system is used.
4. Set the CryptoServer's internal clock with the menu point **Firmware Management → Set Time** (see Link).
5. Initialize the CryptoServer with the wanted firmware package file '*.mpkg', see 7.3.

   For any other application the respective firmware package file has to be used.
   This step can be omitted if a CryptoServer test system is used.
6. Create users on the CryptoServer either using the command line tool CSADM, or the user-friendly Java administration tool CAT, or both (see 3.4 and 3.5 for more information about both administration tools). The attributes to be set for the new user depends on the firmware package loaded:

CryptoServer CSP:
A user with SHA-1 password authentication has to be created (user permission '00000001', flags "sma + no_login").

CryptoServer PKCS#11:
The PKCS#11 user and security officer are created for every slot via the PKCS#11 library functions (C_InitToken, C_InitPin, …), so no users need to be created at this time. Optionally a user with SHA-1 password or RSA signature authentication may be created (user permission '00000000', flags "sm + no_login ") for securing the communication channel between the CryptoServer and the application (for details see [CS-PKCS11_Spec]).

CryptoServer CSI:
A user with SHA-1 password or RSA signature authentication has to be created (user permission 00000020, flags "sm + allow_login ").

7. If you want to set-up the CryptoServer CSI in FIPS-mode:
   Verify whether the CryptoServer is now in FIPS mode and is not in any error state (using the *Get CryptoServer State* command, see Link). See [CSAdmGuide-FIPS] for more information about error indicators in FIPS-mode and details about administration resp. tasks for the CryptoServer administrator. In [CSUserGuide-FIPS] guidance for a person assuming the Cryptographic User role in FIPS-mode can be found.
8. Continue with Step 6 above.

5.6 De-Installation

De-Installation on Windows Systems:

To remove all installed software from the PC, please do the following:

1. In the Start-Menu select 'Settings → Control Panel' (german: 'Einstellungen → Systemsteuerung')
2. In the Control Panel window select 'Software'
3. In the 'Software' window select 'CryptoServer Administration' and click the button 'Remove'.

7 Typical Administration Tasks

In this chapter a short guide through the most important administration tasks and how to perform them with the administration tool CAT will be given.

For performing these administration tasks with CSADM, see [CSAdmGuide].

7.1 Generate a New Initialization Key

In this chapter Initialization Key generation with CAT will be described. In case that key generation shall be performed with CryptoServer's Key-Tool (see 3.9), see [CSKeyTool] for a respective description.

Generation of an Initialization Key, i. e. the key of CryptoServer's Administrator, has to be performed during the first installation and set-up of the CryptoServer system. But it might also be necessary to generate an Initialization Key at a later moment, for instance in order to implement the customer's policy of regular key exchange.

The Initialization Key, private and public part, can either be stored on a smartcard (which will by then be called *Init Key smartcard*) or in a key file '`*.key`' stored on any storage medium like USB-stick, or directly on hard drive. A key file may be encrypted and password-protected (private key part stored Triple-DES encrypted, public key part stored as plain text), or unprotected as plain text.

- *For highest security needs it is recommended to use a smartcard as key token, and not a key file.*
- *If no smartcard is used as key token, it is strongly recommended to generate an encrypted and password-protected key file. This is also the default option for Initialization Key key file generation.*
- *Floppy disks with unprotected key files shall never be used except for test purposes!*

Additionally, together with the Initialization Key one or more corresponding copies of the Initialization Key or one or more *key back-ups* should always be generated. See 3.7.

An Initialization Key *copy* is just an exact copy of the respective smartcard or key file. The respective PINs or passwords can later be individually changed, if wanted.

A *key back-up* can be produced if a smartcard is used as key token. The key back-up consists of two parts: the key is split in two XOR halves, each of them stored on one (PIN-protected) smartcard. Thus the key back-up can only be generated and used according to the 2-persons rule.

- *For the generation of a (new) Initialization Key it is highly recommended to generate at least one key back-up or key copy.*
- *All key and key back-up tokens have to be stored securely and seperately.*

Possible combinations of needed key tokens are therefore:

- 1 smartcard for each Initialization Key copy, 2 smartcards for each key-back-up
- If no smartcards are used: 1 key token for each Initialization Key copy (here, copy and key back-up are identical, and the storage medium can freely be chosen).

If smartcards are used as key tokens, for both purposes (Initialization Key smartcard, key back-up smartcards), Utimaco's "CryptoServer 2000" cards have to be used. These (empty) smartcards are part of the delivery of the CryptoServer system by Utimaco. Further smartcards can be ordered from Utimaco at any time.

Both types of smart cards (administration smartcard, back-up smartcards) are protected by a PIN.

*The default PIN of any "CryptoServer 2000" card, at the time of deliverance, is set to **"123456"**. It is highly recommended to change this standard PIN as soon as possible (see 7.5).*

Preconditions:

- At least two key tokens are needed (one for each Initialization Key copy, two for each key back-up, see above), i. e. the wanted number of smartcards or other storage mediums must be on hand.
- If smartcards are used, you need the appropriate number of empty "CryptoServer 2000" smartcards, see above. Each smartcard that shall be used should be provided with an individual PIN. If however the PIN is still set to the default PIN "123456" (see above), the PIN has to be changed by the person who is responsible for the respective smartcard. See 7.5 for how to do this.
- Furthermore, if smartcards are used, a PIN-Pad with included smartcard reader must be connected to the PC.

What to do:

If the **Initialization Key shall be stored on smartcard**, the following steps have to be perfomed:

1. Choose the menu points **Key-Tools → SmartCard → Generate INIT SmartCard**.
2. It is strongly recommended to enter the optional key info data which identify the key (e. g. 'Init-Key 1', maximum 64 characters) and to choose at least one extra key copy or key back-up smartcard pair generation (see Link for more details about that command).

3. Press the **Generate** button and watch the PIN-Pad display for the further user guidance. The INIT smartcard copies will be generated first, then the wanted number of back-up smartcard pairs will be generated. See Link.

If the **Initialization Key shall be stored in a key file**, the following steps have to be perfomed:

1. Choose the menu points **Key-Tools** → **Keyfile** → **Generate INIT Keyfile**.
2. Enter the path and name of the key file to be generated (see Link for more details about that command). It is strongly recommended to choose the “Work with encrypted Keyfile” option (see above). In that case the password to protect the encrypted key file has to be entered and to be confirmed.
3. Press the **Generate** button. The key will be generated and stored in the given (encrypted) key file.
4. It is strongly recommended to add some key info data on the key token (storage medium), like for instance a ‘*.txt’-file with key name and maybe the date of key generation.
5. Furthermore it is strongly recommended to produce at least one key back-up by simply copying the key file and optional key info data onto another key token and to store it safely and separately from the original key token.

7.2 Changing the Initialization Key

The *Initialization Key*, i. e. the key of CryptoServer's Administrator, shall be changed. Therefore its public part which is loaded onto the CryptoServer has to be exchanged, too.

Preconditions:

- An (old) *Initialization Key* is already loaded onto the CryptoServer (e. g. by Utimaco Safeware AG). This *Initialization Key* shall be replaced.
- The CryptoServer's Administrator has generated the new *Initialization Key*: either in form of an INIT smartcard with back-up copy for his representative (strongly recommended) or in form of an INIT keyfile. See 7.1.
- To perform the key exchange, the old *Initialization Key* is needed.
- For later re-initialization of the CryptoServer, a firmware module package with the wanted CryptoServer firmware is needed.

What to do:

1. To change the Initialization Key choose the menu point **Firmware Management → Change Init Key** of CAT. See Link for the details of this command.
2. Perform a complete re-initialization of the CryptoServer, by use of the new *Initialization Key*. See 7.3.

7.3 Complete Re-Initalization of CryptoServer

You want to clear all data inside of a CryptoServer and reload the complete firmware. This may be useful (for example) in the following situations:

- You want to securely clear all secret data inside a CryptoServer.
- You have changed the *Initialization Key*.
- You have received a new CryptoServer without any firmware loaded.
- An alarm has occured and has cleared all customer data and firmware modules inside the CryptoServer.

Precondition:

To perform a complete re-initialization, you need a firmware package file "*.mpkg" containing the wanted set of firmware modules. For the CryptoServer standard applications, the following firmware package files have to be used ('xxx' stands for further name extensions, e.g. by package version numbers):

- CryptoServer PKCS#11: **pkcs11**xxx**.mpkg**
- CryptoServer CSP: **csp**xxx**.mpkg**
- CryptoServer CSI, standard version (not in FIPS-mode): **csi**xxx**.mpkg**
- CryptoServer CSI, extended version with back-up functionality (not in FIPS-mode): **csiExt**xxx**.mpkg**
- CryptoServer CSI, in FIPS-mode: **csiFIPS**xxx**.mpkg**
- CryptoServer Payment Solution: **eftpos**xxx**.mpkg**

The current versions of the standard firmware package files can be found on the product CD (folder 'Firmware') or on your host PC in the folder {CryptoServer}\Firmware.

For further or more customized applications, various other firmware package files are available from Utimaco.

Furthermore the *Initialization Key* is needed, and your customer-individual CryptoServer licence file must be on hand.

What to do:

1. Choose the menu point **Firmware Management → Setup CryptoServer**.
2. In the upcoming window, enter the name and path of the firmware package file, as well as name and path of your licence file. Choose the "New Installation" option to enforce a complete deletion of the old loaded firmware modules. The command has to be authenticated with the (new) *Initialization Key*. Now all firmware modules of the new package file will be re-signed with the (new) Initialization Key (if necessary) and loaded into the CryptoServer. See *Link* for more details.
3. You can check if all firmware modules have been started properly using the menu point **Status → List Firmware**, see *Link*. If some firmware modules have not been initialized yet (i. e. not INIT_OK), please look at the boot loader log file to analyze the problem (menu point **Status → Show Logfile → Boot**, see *Link*).

7.4 Update of Firmware

New firmware modules (e. g. containing new functionality or a bug fix) shall be downloaded onto the CryptoServer, adding to or replacing existing firmware.

Precondition:

The new firmware has to be on hand in form of a firmware package file '*.mpkg'.

See 7.3 for a list of which package file is used for which (standard) application. For further or more customized applications, various other firmware package files are available from Utimaco.

The current versions of the standard firmware package files can be found on the product CD (folder 'Firmware') or on your host PC in the folder {CryptoServer}\Firmware.

Furthermore the *Initialization Key* is needed, and your customer-individual CryptoServer licence file must be on hand.

What to do:

1. Choose the menu point **Firmware Management → Setup CryptoServer**.
2. In the upcoming window, enter the name and path of the new firmware package file, as well as name and path of your licence file. Choose the "Update" option. The command has to be authenticated with the *Initialization Key*. Now all firmware modules of the new package file will be loaded into the CryptoServer. See *Link* for more details about this command.
3. You can check if all firmware modules have been started properly using the menu point **Status → List Firmware**, see *Link*. If some firmware modules have not been initialized yet (i. e. not INIT_OK), please look at the boot loader log file to analyze the problem (menu point **Status → Show Logfile → Boot**, see *Link*).

7.5 Change PIN of Smartcard

Both types of smart cards (Initialization Key smart card, key back-up smart card) are protected by a PIN. CAT (as well as the Key-Tool) offers also the functionality to change the PIN of any “CryptoServer 2000” smartcard. PIN changing should be done for each smartcard at least once at the beginning, to exchange the Utimaco standard PIN “123456” against an individual PIN.

Preconditions:

- Obviously the concerned “CryptoServer 2000” smartcard(s) must be on hand.
- A PIN-Pad with included smartcard reader must be connected to the PC.

What to do:

1. Choose menu point **Key-Tools** → **SmartCard** → **Change PIN of SmartCard**. Then follow the PIN-Pad dialogue. See Link for more details about that command.

7.6 Recover Initialization Key from Key Back-Up

In case the INIT smartcard, which stores the Initialization Key, is lost, or cannot be accessed anymore because of forgotten smartcard PIN, it is crucial to recover the Initialization Key from a back-up smartcard pair.

Preconditions:

- A back-up key token pair is needed, consisting of two back-up smartcards with each smartcard containing one XOR half of the Initialization Key: Thus Initialization Key recovery can only be performed according to the 2-persons rule.
- Furthermore an empty “CryptoServer 2000” smartcard is needed.[4] This smartcard should be provided with an individual PIN. If however the PIN is still set to the default PIN “123456”, the PIN has to be changed by the person who is responsible for the respective smartcard. See 7.5 for how to do this.
- A PIN-Pad with included smartcard reader must be connected to the PC.

What to do:

1. Choose the menu points **Key-Tools → SmartCard → Recover Initialization Key from Back-Up**. See Link for more details about that command.

[4] Empty smartcards can be ordered from Utimaco at any time.

8 Trouble Shooting

In this chapter it will be described how to escape from typical error situations.

8.1 Check Operativeness and State of CryptoServer

This section deals with the situation where it is not known whether the CryptoServer works at all, and in which mode/state it is. The following steps should systematically be performed to check CryptoServer's operativeness and, if possible, to get the CryptoServer working again.

Please be aware that a more detailed (error) treatment is possible if the command line Administration Tool CSADM is used, instead of CAT. See [CSAdmGuide] section 7.

Precondition:

If the CryptoServer is installed on your local PC, make sure that the PCI Driver is running and that the Administration Tool CAT is installed.

If the CryptoServer is a part of a CryptoServer LAN, make sure that CryptoServer LAN and Client-PC are properly connected to the network (try to 'ping' the LAN box from the Client-PC) and that the Administration Tool CAT is installed on the Client-PC.

What to do?

All described commands have to be performed with CAT.

1. Perform *Get CryptoServer State* command (see Link).

Result	Explanation/Reason/Adjustment
state = OPERATIONAL	Everything okay, continue with (2).
state = INITIALIZED, alarm = OFF	CryptoServer is in boot loader mode. ⇒ Reboot CryptoServer to get it in operational mode (3).
state = INITIALIZED, alarm = ON	An alarm has occurred (and is possibly physically still present) ⇒ See chapter 8.2 for alarm treatment (and 4.3 for more information about CryptoServer alarms).
state neither INITIALIZED nor OPERATIONAL	CryptoServer is not correctly initialized or even defect. ⇒ Please get in contact with Utimaco (see 8.3.2).

Result	Explanation/Reason/Adjustment
Error B9011xxx, B9015xxx, B9016xxx, B9017xxx or B9021xxx until B9024xxx	CryptoServer's PCI carrier card does not react. ⇒ Disconnect the power plug of the CryptoServer LAN or the PC with the CryptoServer PCI card. ⇒ Turn the power on. ⇒ Try to reboot CryptoServer (3). ⇒ Check the state of the CryptoServer.
other errors: B901xxxx or B902xxxx	No connection to CryptoServer / CryptoServer LAN, communication problem, wrong host or device name, problem with network. ⇒ Check CryptoServer address (with CAT, Link). ⇒ Perform 'ping' at CryptoServer LAN. ⇒ Check state/configuration of the TCP daemon on the CryptoServer LAN (locally, by performing the CryptoServer LAN **Selftest**, see section 4.2.5 in [CSLANUserManual]). See [CSErrorRef] for a list of possible errors codes.

2. Perform *List Firmware* command (see Link).

Result	Explanation/Reason/Adjustment
All necessary firmware modules are listed and initialized (INIT_OK).	OK. CryptoServer is in *operational mode* and ready to work. End.
Some necessary modules are missing in the given list.	Modules are not loaded onto CryptoServer. ⇒ Check presence of modules with *List All Files* command (see Link). ⇒ Update missing modules by loading an updated firmware package (see 7.4). The CryptoServer will be restarted after this update automatically. Repeat the *List Firmware* command. If then modules still cannot be started (e. g. wrong signature): ⇒ see next point

Result	Explanation/Reason/Adjustment
At least one module is not initialized (i. e. not INIT_OK).	Firmware module(s) cannot be started (e. g. module dependencies cannot be resolved). ⇒ Search boot log file for errors (see Link). ⇒ (If this has not been done yet:) Update missing modules by loading an updated firmware package (see 7.4). The CryptoServer will be restarted after this update automatically. Repeat the *List Firmware* command. If then modules still cannot be started: ⇒ Re-initialize the CryptoServer (see chapter 7.3).

3. Perform *Reboot CryptoServer* command (see Link).

Result	Explanation/Reason/Adjustment
no error and the *GetState* command works again	OK ⇒ back to (1)
error 0xB901773x	Switch CryptoServer off (disconnect power plug) and on again, then back to (1).
other error, or the *GetState* command does not work	Connect a PC's serial port with a crossed serial cable to the CryptoServer's serial port 1 (at the bracket of the PCI-card). Start a terminal program on the PC (115200 baud, 8 bit, no parity), perform the *Reboot CryptoServer* command and watch the terminal output. If there are error messages about firmware modules that are not started: ⇒ Go to (2). Otherwise ⇒ Re-initialize the CryptoServer (see chapter 7.3).

8.2 Alarm Treatment

An alarm can be triggered on the CryptoServer as a result of the following reasons:

- Power is too low
- Power is too high
- Temperature too high (> 66°C)
- Temperature too low (< -13°C)
- Outer foil is broken
- Inner foil is broken
- Invalid (corrupted) Master Key $\mathbf{K_{CS2}}$ (this usually occurs in case of an empty battery)
- External Erase is executed (manually, by a short-circuit of the 'External Erase' pins on the PCI-card)

See chapter Link for a detailed description of the CryptoServer's alarm mechanism.

Some alarm reasons can be removed (e. g. exchange low battery or cool down high tempera¬ture), these are called temporary alarms. Other alarm reasons cannot be removed, these are called permanent alarms. Permanent alarms occur e. g. in case of a damage of the inner or outer tamper protecting foil, whereas usually all other possible alarms are temporary.

The *Get CryptoServer State* command shows the reason of an alarm and if the alarm is still present. If the reason for an alarm cannot be removed then please get in contact with Utimaco (see 8.3.2), else you can reset the pending alarm state (see below).

Precondition:

An alarm has occurred to the CryptoServer. This will be announced with the *Get CryptoServer State* command (**alarm = ON**), see Link. The detailed alarm reasons can be seen from the '**sens = (…)**' text which follows the 'alarm = ON' line.

If *Get CryptoServer State* additionally answers with '**Alarm is present**' then the physical alarm reason is still present. But it is also possible that in the meantime the alarm cause has been removed, which is announced by '**Alarm has occurred**'.

What to do?

1. If the alarm is physically still present: Remove the alarm cause if possible. Execute *Get CryptoServer State* again (see Link) to check the success. Even if the reason for the alarm has been removed, the alarm state will still be 'ON', but the alarm should no longer be shown as 'present' (only as 'has occurred').
2. If the alarm is still shown as 'present': please contact Utimaco (see 8.3.2).
3. Else: Perform the command **Firmware Management → Reset Alarm** (see Link).
4. Execute *Get CryptoServer State* again. The alarm state should now be 'OFF'.
5. Since the alarm has cleared all data and firmware modules, a complete re-initialization of the CryptoServer must be performed now (see chapter 7.3).

8.3 Maintenance and Support

8.3.1 Batteries

Two batteries are relevant to back-up the CryptoServer's power consumption and to prevent data loss:

Any **CryptoServer PCI board** contains a battery to ensure that no security relevant data will be lost respectively deleted even when the CryptoServer is turned off or when the power supply is interrupted. If the device is not used over a prolonged period, i. e. during storage or if the computer is turned off, the battery will have a durability of half a year at a minimum. If the CryptoServer is permanently powered on, the battery is not discharged and the lifetime of the battery increases. This battery is called "**carrier battery**" because it is mounted on the PCI carrier card.

In case of a **CryptoServer LAN**, an additional **external battery** is included in the communication unit. This battery is directly connected to the included hardware security module(s) CryptoServer and serves as the main power supply of the CryptoServer in order to increase the lifetime of the carrier battery. In this case the carrier battery is used only after the external battery is exhausted. The lifetime of both batteries together amounts to at least 2 to 2.5 years.

The state of the batteries has to be checked regularly.
In case that one of the batteries is not replaced early enough, all data inside the CryptoServer will be deleted!

See the following subsections for how to check the battery state and how to exchange the batteries.

8.3.1.1 Check State of the Batteries

To check the state of the batteries the command **Status → CryptoServer Info** should be used (see Link). The output of this command contains a line starting with the string "`batt`" which shows the state of the batteries:

Output	Meaning
`batt ok`	All connected batteries contain sufficient charge.

`batt carrier battery failed.`
or
`batt carrier battery low.`
	The carrier battery of the CryptoServer has low power and must be exchanged.

`batt external battery failed.`
or
`batt external battery low.`
	The external battery has low power and must be exchanged.

Output	Meaning

`batt carrier battery failed.`
`external battery failed.`
or
`batt carrier battery low.`
`external battery low.`
	The carrier and external batteries both have low power and must be exchanged.

`batt ?`	The state of the batteries could not be determined because of concurrent data transfer to the CryptoServer. In this case (which should happen rarely) repeat the command “GetInfo“ until the battery state is shown.

8.3.1.2 Exchange of Batteries

If any of the CryptoServer batteries has reached a critical state of charge, it has to be exchanged.

Any **CryptoServer PCI board** only uses the carrier battery, there is no external battery connected. See [CS2Install-Manual] chapter 6 for how to exchange the carrier battery.

For a **CryptoServer LAN**, always both batteries are used. But since exchanging the carrier battery would demand opening the CryptoServer LAN communication unit, the customer is only allowed to exchange the external battery.

For a CryptoServer LAN, only specialized staff of Utimaco is allowed to replace the carrier battery!
Please do not open CryptoServer LAN for any kind of maintenance work! Otherwise all warranty claims against Utimaco Safeware AG will become void!!

In case that the carrier battery has to be exchanged, please contact Utimaco Safeware AG (see 8.3.2).

See [CSLANOpManual] for how to exchange the external battery of a CryptoServer LAN.

9 Appendix: PIN-Pads

For most CryptoServer applications a PIN-Pad is needed.

The PIN-Pad unit exists of a key pad, a display and a smart card reader.

Standard PIN-Pad is the ACR80 of ACS, but other PIN-Pads can be used, too[5]. Possible differences in using other PIN-Pads are marked in brackets and italic in the following description.

9.1 Connecting the PIN-Pad

First please connect the enclosed connection cable with the small plug to the connector on the right side of the PIN-Pad.

Connection to host PC:

Connect the PIN-Pad via the connection cable to a free serial port of the PC.

Connection to CryptoServer LAN:

Connect the PS/2 plug of the cable with the PS/2 connector on the left front of the CryptoServer LAN enclosure. Connect the 9-PIN serial plug into the front connector marked “CS2”.

If the CryptoServer LAN is switched on, the display of the PIN-Pad shows “*ACR80-0621*”.

[5] Further supported PIN-Pad types are e.g. Ingenico/Bull SafePad and Omnikey CardMan 8630.

9.2 Operation

Key(s)	Description/Meaning
0-9	■ enters numerical characters ■ the imprinted characters (American keyboard) are not supported
<CLEAR>	■ deletes the last character in the display *(On other PIN-Pads than the ACR 80 this key might be arranged or named differently, e. g. "**CORR**" or "←")*
<ENTER>	■ confirmation *(On other PIN-Pads than the ACR 80 this key might be named differently, e. g. "**VAL**" or "✓")*
function key: DOT	■ enters a dot *(On other PIN-Pads than the ACR 80 this key might be arranged differently or is marked with a "**.**")*
function key: SHIFT	■ Used to enter hexadecimal characters: Push the SHIFT key and then a key from 1 to 6 ■ Shift 1: A ■ Shift 2: B ■ Shift 3: C ■ Shift 4: D ■ Shift 5: E ■ Shift 6: F *(On other PIN-Pads than the ACR 80 the SHIFT key might be arranged differently or marked with a "*****")*
function key: CANCEL	■ aborts operations at the PIN-Pad *(On other PIN-Pads than the ACR 80 this key might be arranged differently or marked with an „X" or „ANN")*

10 References

Ref.	Title/Company	Doc.-No.
[CSAdmGuide]	CryptoServer – Administration Guide / Utimaco Safeware AG	2002-0021
[CSAdmGuide-FIPS]	CryptoServer – Administrator's Guide for CryptoServer in FIPS-Mode / Utimaco Safeware AG	2004-0002
[CS2API]	CryptoServer – Application Interface (CSAPI) / Utimaco Safeware AG	2002-0005
[CS2Install-Manual]	CryptoServer – Installation Manual / Utimaco Safeware AG (title of German-language version: CryptoServer – Installationsanleitung)	2003-0007
[CSUserGuide-FIPS]	CryptoServer – User's Guide for CryptoServer in FIPS-Mode / Utimaco Safeware AG	2004-0005
[CSLAN-OpManual]	CryptoServer LAN – Operating Manual / Utimaco Safeware AG (title of German-language version: CryptoServer LAN – Betriebsanleitung)	2005-0001
[CSLAN-UserManual]	CryptoServer LAN – User Manual / Utimaco Safeware AG	2003-0002
[CSLAN_Data]	CryptoServer LAN Datasheet / Utimaco Safeware AG	
[CS_Data]	CryptoServer Datasheet / Utimaco Safeware AG	
[CS-CSI]	CryptoServer – Cryptographic Services Interface – Firmware Module CSI Interface Specification / Utimaco Safeware AG	2004-0003
[CS-CSP_Spec]	CryptoServer Cryptographic Service Provider – Technical Specification / Utimaco Safeware AG	
[CS-CSP_Data]	CryptoServer CSP – Datasheet / Utimaco Safeware AG	
[CS-PKCS11_Spec]	CryptoServer – PKCS#11 Interface / Utimaco Safeware AG	
[CS-PKCS11_Data]	CryptoServer PKCS#11 – Datasheet / Utimaco Safeware AG	
[CSErrorRef]	CryptoServer Error Reference / Utimaco Safeware AG	2003-0001
[CSKeyTool]	CryptoServer Key-Tool – User Manual / Utimaco Safeware AG	2006-0002
[PKCS11]	PKCS#11: Cryptographic Token Interface Standard v2.20, 28th June 2004 / RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs	