



Key Handling Centre KHC-2000

The Key Handling Centre KHC-2000 is a security and management centre. With it, you can conveniently and securely perform all security, management and distribution tasks (including key management) involved in the operation of your phone cipher units. This centre simplifies the operation of your system and increases its availability. The KHC-2000 is available as an online and an offline version.

The Key Handling Centre KHC-2000 is a convenient centralised tool for finely scaled security and key management. It allows you to adapt your security policy directly on screen to any changes in organisational or security conditions. The KHC-2000 is simple to operate and intuitive to learn thanks to the familiar Windows user interface.

With the online version, you can directly transfer the security data and keys to the target units (HC-2203) using down line loading (DLL over a modem) or by local direct connection. You can also reach the HC-2203 or HC-24x3 indirectly by E-Mail on a PC with the auxiliary KPT-2000 programme. The HC-2203 units can be used as local distribution centres and extensions of the KHC-2000, because decentralised further distribution to other units (including Secure GSM) can be carried out from them. Cables or CSC smart cards are used for this purpose and for cloning units.

In the offline version, (encrypted) security data is distributed via CSC smart cards to the cipher unit (HC-2203). Alternatively, this data can also be sent on data media such as USB sticks, CD floppy disks or E-Mail to a PC equipped with KPT-2000 software and from there on to other cipher units (HC-2203 and HC-24x3). The only

difference to the online version is the DLL function.

The KHC-2000 consists of a specially equipped desktop computer and an HC-2203 cipher unit which doubles as a security co-processor. The HC-2203 serves here to separate network and security functions and as a smart card programming unit and reading station. It also ciphers all data for storage on the data media and on the hard disk using the same algorithm structure as in communication encryption. As a result your handling of keys is just as secure as your communication.

Key features

- KHC-2000 is a computer-based security and management centre that assists you with the secure management and distribution of security data and keys
- You can conveniently distribute keys offline via cable (locally) or enciphered via various data media or for example by regular mail or courier
- With the online version you can also distribute keys enciphered over phone lines to HC-2203 units without any additional travel or security expenses
- All cryptographic data and keys are stored in the security module or in the computer database in a cryptographically secure manner. That means they are never visible or accessible to outsiders
- The tamper-proof security module in the separate HC-2203 can be removed, and access to the KHC-2000 is also password-protected
- You work with a Windows-based application which is easy to learn to operate
- All units in the HC-2000 family are supported

General data

The Key Handling Centre KHC-2000 supports the management tasks for all security related data of the secure telephony family HC-2000: profiling the algorithm, planning network, administration of the cipher units, cryptographically protected distribution of secret data and maintaining the network.

The KHC-2000 consists of a specially programmed workstation and a PSTN Encryption HC-2203 used as a tamper-proof security co-processor, access control and smart card programming station. The system is delivered as a complete package and ready to use.

Built-in online help and a comprehensive user manual for simple and trouble-free use of the KHC-2000 are part of the package.

Management task

Algorithm

- Definition of data sets with customer's own secret data via familiar Windows user interface
- Administration of all units in the network
- Cryptographically protected storage of data sets in files on the hard disk
- Cryptographically protected distribution of data sets:
 - Online via downline loading (DLL) to any HC-2203 worldwide
 - Locally from KHC-2000 to HC-2203 and HC-24x3

- Via PIN-protected Smart Cards to HC-2203
- Via any communication means (e.g. floppy disk, E-Mail, etc.) to a PC and from there via KPT-2000 to the HC-2203 or HC-2423
- Via built-in data transfer function of the HC-2203 to HC-24x3

Cryptographic data

Algorithm

- HCA-480, customer-specific cipher algorithm Cipher Block Chaining mode CBC
- Customer managed profiling of algorithm by CMP with variety $> 10^{506}$
- Built-in high-quality true random generator for generation of all master keys
- Sophisticated generation of management key (MK) based on HCA-480 for each single data set

Keys

- Master management key (MMK): variety $> 10^{38}$ used for MK generation, stored in tamper-proof security module
- Management keys (MK): variety $> 10^{38}$
- Master communication key (MCK): $> 10^{38}$

Access control

- Password-based
- Verification in tamper-proof security module

All data are cryptographically protected during storage on the hard disk and distribution to the cipher equipment.

Delivery content

Workstation

- PC standalone with Windows XP operating system
- Flat screen monitor 19"
- Keyboard/mouse/floppy
- V.24 IF extension card
- Removable hard disk
- PC card slot including PC card security module
- KHC-2000 applications
- CD-RW drive for backup
- Installation CD-ROM including all delivered SW
- Boot disk and recovery CD-ROM including HD image
- ADM-1500 data modem

Security co-processor

- Standard HC-2203
- Interface data cable

User manual

- Hard copy and CD-ROM included

Accessories

- Distribution cable for HC-2203 (locally connected)
- Distribution cable for HC-24x3 (locally connected)
- 10 CSC-1000 Smart Cards
- 10 CD-R

KPT-2000

- Software on a CD-ROM for loading of security data from a PC to a HC-2203 or HC-2423

Telephony Management System

