KD03 PCCard

Encryption board for PC notebook

KD03 PCCard is a sophisticated platform specialy designed to meet the requirements of sensitive data protection and access control to PC notebook. The encryption board is manufactured according to the standard *CardBus Type II* interface and it integrates a smartcard reader. All encryption and access control activities are managed by a dedicated processor providing high throughput performance and lowering requirements on CPU power. Keys are stored in a dedicated and encrypted hardware environment. The main features of KD03 PCCard include bootstrap protection, hard disk encryption, and a high security access control system. The policy governing access rights is stored in the user's smartcard. The KDC03 is responsible of the configuration and management of KD03 PCCard. Simple to install, KD03 PCCard does not require the supervision of trained personnel. Crypto functions are user-friendly and in most cases transparent to the user. Additional specific software drivers make KD03 PCCard ready for off-line file encryption.

TELSY

KD03 PCCard Specifications

GENERAL

- protection of bootstrap and local resources, access control, off-line encryption
- Card Bus Type II standard board equipped with HW crypto environment featuring a protected area for key storage
- system requirements: Microsoft Windows for PC; 256 MB RAM and 10 GB of free space on hard disk (minimum), Pentium III 500 MHz processor
- system designed and manufactured according to ISO 9001; CE approval

APPLICATIONS

STANDARD APPLICATIONS FOR WIN.2000 SP4/XP/SERVER 2003

Hard disk encryption

The hard disk encryption is hardware based, implemented on FPGA, it is physical and affects the whole disk regardless of disk size and system performance. Data protection (even in the event of the board removal) is therefore granted against any attempts at copying data, against theft or even during repairing. The temporary files automatically generated from the applications are encrypted too. Encryption is completely transparent to the user.The operating system (if installed on the protected hard disk) is encrypted thus providing intrinsic protection against unauthorized modifications. KD03 PCCard encryption can be applied to external hard disks (USB), removable media: CD, DVD and floppy. Internal supported interfaces interne: PATA and SATA. External supported interfaces: USB. KD03 PC is available for WIN.2000 SP4/XP/SERVER 2003 operating systems.

Access control

Access control is based on a "two-party authentication" with smartcard and password. Communication between KD03 PCCard and token is not managed by the oprating system of the PC and it is encrypted, making any attempt at monitoring vain. Access control is ruled by a policy issued by KDC03 and stored on the smartcard. The policy sets user rights (eg: bootstrap from floppy disk, use of serial ports, USB). A PC station can be shared by different users, each of them provided with its own smartcard. The PC station can be temporarily locked by removing the smartcard from the reader.

Bootstrap protection

The computer can only be started by authorized users in possession of a smartcard and password. The hardware bootstrap is far more secure than any other software bootstrap.

Management

Through the KDC03 system, the network administrator can manage the security parameters of KD03 units guaranteeing the confidentiality and the integrity of encryption keys. The HD key is stored on the board and the deciphering process is physically executed on the smartcard. In case the password is forgotten or the smartcard is damaged, the administrator of the network can retrieve encrypted data. The management of keys, users and smartcards are the main tasks of the KDC03, which assigns and revokes access rights generating update files.

ALGORITHMS

Encryption algorithms, based on AES standards and are hardware implemented on FPGA, can be standard or specially designed for "community of interest". BCT01 Tigershark, approved by ANS-UCSi, is the available family of algorithms, which includes the AES. Key length is 256 bits. KD03 PC can be configured to host custom algorithms. Further standard or custom algorithms can be implemented on demand as long as they respond to the requirements of the system.

ADDITIONAL APPLICATIONS

Off-line encryption - *KD03 Datacrypt* -

Single files or entire directories can be encrypted on demand. Typical applications: encryption of floppy disk content

VARIE

Electrical:	• power: from CardBus slot
Ambientali	• operating temperature: from 0° to +55°C • operation relative humidity: from 5% to 95% • storage temperature: from -20° to + 65°C • storage relative humidity: from 5% to 95%
Dimensions:	• CardBus Type II standard board: 54 x 85 x 4 mm

File: KD 03 PCCard_NATO; 08.01.28