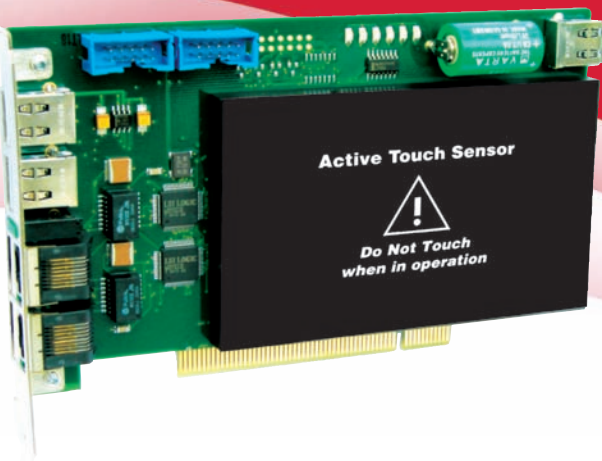




CompuSec[®] HSM

Hardware Security for Desktop PCs



CompuSec[®] HSM is the hardware based security product for Desktop PCs. This product provides all the features from the CompuSec[®] Security Suite in combination with a highly secure, hardware based encryption solution.

CompuSec[®] HSM provides unique features. The product is based on a 32-Bit PCI board running at 33 and 66 MHz PCI Bus speed. The product is intended for high-end security applications.

Pre-Boot-PKI²

CE-Infosys invented the Pre-Boot-PKI technology in 2002. With CompuSec[®] HSM, this Pre-Boot-PKI2 technology is introduced to desktop computing. A user's smart card contains certificates identifying the user while CompuSec[®] HSM provides its own certificates stored in its integrated security chip. With this combination of 2 certificates, a secure authentication and a secure remote control process are achieved. The use of a smart card as authentication tool allows easy combination with RF-ID transponder chips for physical access control. The smart card reader is directly connected to the CompuSec[®] HSM board.

The Computer-User Relation

CompuSec[®] HSM is fully supported by the GlobalAdmin management system. This means a user can use any number of machines with the e-Identity[®] smart card. At the same time, each computer can accept any number of users. This provides a flexible relation between users and computers. All relations are centrally managed using the GlobalAdmin product. CompuSec[®] HSM can also be locally managed in a single user installation.



Biometric Functions

CompuSec® HSM is also available with a Biometric Reader for fingertip scanning and smart card reading. This USB device provides both the function of a smart card reader and the functionality of a capacitive finger scan device. This provides the user additional security for authentication processes during logon and whenever the user identity has to be proven in the software running on the PC. The biometric logon is performed before the system boots.



Identity Management

CompuSec® HSM manages the identity of the user for applications. For existing applications requiring passwords, CompuSec® HSM learns the users' passwords, stores them in an encrypted format and automatically inserts the correct password into the application when required. This is available for local and WEB based applications. For newly designed applications, CompuSec® manages the complete application policies for each user. CompuSec® HSM collaborates with a policy database where tickets are generated for the applications. A powerful and easy-to-use API is provided for applications to query the user policies. This allows central management of user rights within applications. For critical business processes, a BioClick is used to initiate trustful transactions. BioClick is a touch of the finger scanner for half a second by the authorized person. The Identity management database will be available in Q3 2006.

Full Hard Disk Encryption

The hard disk encryption of CompuSec® HSM uses a fast implementation of the AES algorithm in the hardware. This encryption includes the operating system. Multiple Operating systems are supported on a single computer. The initial encryption can be performed before the computer is used by the user or transparent while the user is using the PC. The latter which is Background-Encryption allows the user to interrupt the encryption process and shut down the computer at any time. The support of the Hibernation mode is very important to mobile users. In Hibernation, the contents of the computer RAM are written to the disk and the computer shut down. When restarted, the contents in the RAM are reloaded from the hibernation file and the user can continue to work. This is faster and allows the user to shut down in the middle of an application. So far, most hard disk encryption products could not support this mode and disabled hibernation. CE-Infosys is the first company providing support for hibernation mode with its product line.



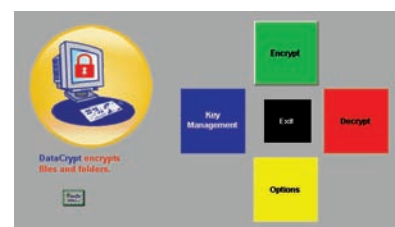
Encryption of Diskettes, CD-ROM & Removable Media - CDCrypt

Diskettes, CD / DVD and removable media devices such as Memory Sticks and USB thumb drives can be encrypted by CompuSec® HSM. The encryption for CD / DVD uses the CDCrypt feature to support internal and external CD burners that are connected using USB or IDE. With central administration, an encryption policy may define whether a user may or may not switch the mode from encrypted to non-encrypted when using such devices. As such, an organization can easily enforce a policy to use only encrypted Diskettes, Removable Media Devices and CD-RW / CD-R / DVD to minimize the threat of data theft. Such encryption is unobtrusive and does not change the way the user works with these devices.



Encryption of Individual Files - DataCrypt

CompuSec® HSM includes a module that enables users to encrypt individual files called DataCrypt. DataCrypt will enable users to encrypt their messages and send them via email, ftp etc. The data will travel safely over whatever medium chosen to allow CompuSec® users to safely exchange files. DataCrypt can also be used as a software module and can be forwarded to other users without a license free of charge. DataCrypt employs Public-Key-Cryptography based on elliptic curves to generate keys for encryption and decryption. DataCrypt also uses a new technology called 'Sealing' that will hide all structures in the header of the encrypted file, giving additional protection against 'traffic analysis' on the network.



Encryption of Server Files & Subdirectories - SafeLan

File and Directory Encryption with CompuSec® HSM can be performed for local or network files and/or directories. This function called SafeLan will ensure that all files written or copied into the encrypted directory will automatically be encrypted and remaining completely transparent to the end user. This also means that a user without an authorized directory key will not have access to the directory and will also be unable to see the files. This function is used to separate users of the same file server in a strong cryptographic way and also ensure that server administrators cannot see the contents of the encrypted files. SafeLan supports NTFS, Novell, FAT and network based file systems.



Encryption of Voice Communication - [ClosedTalk]™

[ClosedTalk]™ is a component of CompuSec® HSM used for encrypted voice communication between 2 CompuSec users. The built-in sound system of the computer is used for [ClosedTalk]™. No IP telephone is needed. [ClosedTalk]™ uses Internet to transport the voice data from one user to the other. E-mail addresses are used to contact communication partners. An e-mail address is self-explanatory and easier to remember than traditional phone numbers. [ClosedTalk]™ uses a gatekeeper service to find the communication partner on the network. The Diffie-Hellman key generation protocol is used to provide secure session keys for each talk.



Encrypted Network Ports

CompuSec® HSM provides 2 Ethernet network ports on the board. These ports can be used for encrypted network traffic. The IP frames are encrypted inside the HSM board. This function is completely transparent to the software of the protected PC. CompuSec® HSM also performs the complete key management for the network traffic. In situations where access to an encrypted and a plain network is required from the same station, one port can be used for plaintext traffic while the other port can be used for the encrypted traffic. An enhanced IPSec client is inbuilt into the HSM to manage and tunnel the encrypted IP traffic. The IP encryption supports pool address modes, multiple dial-in points and other features, which are explained in detail in our IPCryptor product literature. The IP encryption of CompuSec® HSM cooperates with an IPCryptor as counterpart in the network.

E-mail Encryption and Signing for Microsoft Outlook & Lotus Notes

CompuSec® HSM uses the Digital Certificates of the user to encrypt and sign e-mails using Microsoft Outlook, Outlook Express or Lotus Notes. The cryptographic software comes with a signed CSP Cryptographic Service Provider. The mail security uses the S-MIME standard to guarantee the compatibility with other users not using CompuSec® yet.



Smart Card Reader

CompuSec® HSM comes with a CE-Infosys USB smart card reader. The USB reader is directly connected to the CompuSec® HSM board. Furthermore, this smart card reader can be used by applications using the Microsoft PC/SC interface.



OS Support

CompuSec® HSM supports Microsoft operating systems such as Windows XP, Server 2003 and Windows 2000. In addition, a support for several Linux distributions based on Kernel 2.6 and 2.4 is provided. Most boot managers are also supported, allowing multiple operating systems to reside on a single system.



Installation & Management

CompuSec® HSM can be deployed as a locally or as centrally managed product. In single-user installations, CompuSec® HSM creates a security file with all the secret keys locally. The user is responsible for keeping these keys a secret. In larger organizations, central management of CompuSec® HSM is recommended. The GlobalAdmin program manages all CompuSec® HSM policies and provides additional functions like unattended installations, automatic software roll out, remote password reset and a complete management of the VPN functions. CompuSec® HSM can also be an integrated part of a corporate-wide PKI structure. Details are described in the GlobalAdmin product literature. For large customers with multiple locations, remote e-identity loading stations are available. A product for the user help desk is also available to assist support staff with the remote password reset functions. Automatic synchronization with Microsoft user management and Active Directory is provided for CompuSec® HSM.

About e-Identity® Smart Cards

Each CompuSec® HSM comes with one e-Identity® smart card. A secure password change mechanism is provided to allow help desk operators to change passwords remotely. The security chip used for e-Identity® and the implemented operating system has a Common Criteria EAL E4 high certificate. e-Identity® can be provided with inbuilt ECC functions or the standard RSA cryptography. e-Identity® supports all standards like Microsoft PC/SC, PKSC#11, Microsoft CSP including an integrated driver-to-driver interface.



Inbuilt ATD Device

CompuSec® HSM comes with a high-end protection mechanism. A new technology called 'Active Touch Sensor' protects its stored secrets while the board is in operation. Additional mechanisms protect all stored secrets while the PC is powered off. CompuSec® HSM can erase the main storage of the PC and send hidden alarm signals when an attack is detected. All security related components including all encryption and all key management functions are protected by the Touch Sensor. Additional information can be provided to our customers upon request.

Active Touch Sensor



Do Not Touch
when in operation

Flexibility of Cryptographic Algorithms

CompuSec® HSM provides the flexibility to modify the encryption algorithms. A fast hardware based AES algorithm is built in. The S-Boxes of the AES algorithm can be customized to provide additional cryptographic security

System Requirements

- PC Workstation with Intel Architecture
- Windows Server 2003, Windows XP, Windows 2000 or Linux 2.4 / 2.6
- PCI or PCI-X Bus slot
- 60 MB Free Hard Disk Space
- Build-in Sound Card for [ClosedTalk]™



CE-Infosys GmbH
Am Kuemmerling 45
D-55294 Bodenheim
Germany
Tel.: +49 (0) 6135 / 77 0
Fax: +49 (0) 6135 / 77 77
de.sales@ce-infosys.com

CE-Infosys Pte Ltd
390 Havelock Road
08-02 King's Centre
Singapore 169662
Tel.: +65 6235 8722
Fax: +65 6235 3164
sg.sales@ce-infosys.com

CE-Infosys FZ-LLC
Dubai Internet City
P.O.Box 500434
Dubai, UAE
ae.sales@ce-infosys.com

For more information, please visit our website
<http://www.ce-infosys.com>

CompuSec® & e-Identity® are registered trademarks of CE-Infosys Pte Ltd in Singapore.

Reseller: