



CompuSec™

with e-Identity™

www.ce-infosys.com

CompuSec™ is a Security Suite for protection of Notebook and Desktop PCs, providing Access Control, Hard Disk Encryption, Email Security, VPN and Single-Sign-On. CompuSec™ uses PKI technologies and comes with an e-Identity™ security device. This is either a smart card with an USB reader or an USB token.

CompuSec™ was made for customers who want more than just a password protection. The high security level achieved is combined with a flexible user transparent mode of operation. Individual, small groups of users as well as large enterprises use the product. CompuSec™ combines a set of often-needed security functions, while still giving the user the option to configure the product for its own needs. Large organizations find all the required functions for the efficient use of the product. This includes unattended installation, centralized rollout, support for disk images, central software distribution, service functions and central user management.

CompuSec™ uses new technologies developed by CE-Infosys, which provide previously unknown functionalities to PC security products. These are the Pre-Boot USB access, the use of PKI technology before a system boots and the Hibernation support. The USB bus is managed by CompuSec™ prior to the boot phase in order to access USB-Tokens and smart cards. This allows smart card based PKI functions before the computer boots. The unique Hibernation support allows the CompuSec™ users to shut down and restart the computers using the fast Hibernation mode of the Microsoft OS.



■ Smart-Access

Whenever a system is started the Pre-Boot-Authentication process manages the user logon with a strong 2-factor authentication. This requires the smart card or the USB token. Smart-Access provides protection against spy technologies that tap to the signals of a smart card reader to get the PIN information. The new developed Smart-Access technology does not use the traditional PIN codes. Instead a challenge response technology is used to perform a Single-Sign-On at a smart card level. This technology provides security advantages and ease-of-use compared to the normal smart card logon at the operating system level.



e-Identity™ token

■ Pre-Boot-PKI

CompuSec™ uses a new developed Pre-Boot-PKI technology to manage the access to the hard disk of a computer. This allows multiple users on a single machine as well as multiple machines access for a single user. The user management is easily performed by the GlobalAdmin station for large organizations, or by the installation program for small user groups or individuals.



e-Identity™ smart card & USB reader

■ Password Management

The password strategies can be defined to the organizations need. This includes password lifetime, password usage count, password change options, minimum and maximum length and more. In cases where a password was forgotten, a challenge-response procedure with the GlobalAdmin station provides an easy help for the user to get a new password.

■ Single Sign On

Two alternatives for single sign on are provided. First, the e-Identity™ of the user stores the system logon password together with the user ID and the domain name. This replaces the traditional logon procedure at an operating system. The second and more advanced method provided by CompuSec™ uses a digital certificate of the user together with its private key inside the e-Identity™. This certificate-based logon at the domain server is the preferred way for domain users and is fully integrated into the Microsoft operating systems. The certificate based Single-Sign-On requires the GlobalAdmin station, which may be used as a full Certification Authority (CA). Lotus Notes users will store their ID file on the e-Identity™ and also use the certificates of the e-Identity™.



■ Full Hard Disk Encryption

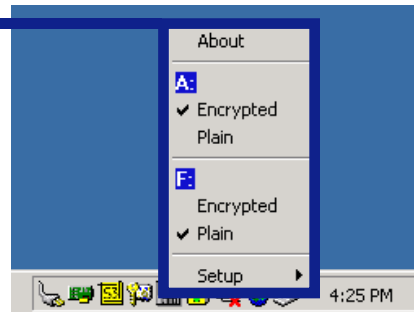
The hard disk encryption of CompuSec™ uses a fast implementation of the AES algorithm. The encryption includes the operating system. Multiple Operating systems are supported on a single computer. The initial encryption can be performed before the computer is used by the user or transparent while the user is using the PC. The second, Background-Encryption allows the user to interrupt the encryption process and shut down the computer at any time.

Very important for mobile users is the support of the Hibernation mode of the Windows operating systems. In this mode the contents of the computers RAM is written to the disk and the computer is shut down. When restarted the RAM contents is 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 hard disk encryption products could not support this mode and disabled hibernation. CE-Infosys is the first company providing support for the hibernation mode with its product line, including CompuSec™.



Encryption of Diskettes and Removable Media

Diskettes, removable media and removable drives such as Memory Sticks are supported by the CompuSec™ encryption. An encryption policy defines the mode in which these devices will be used. A user may or may not have the right to switch the encryption mode. As such, an organization can easily enforce a policy to use only encrypted Memory sticks.

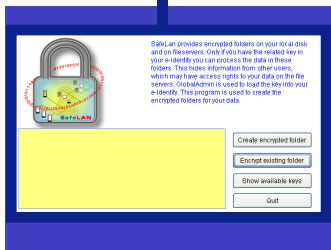


Email Signing and Encryption



CompuSec™ provides the necessary encryption modules to encrypt and sign e-mail using Microsoft Outlook, Outlook Express or Lotus Notes. The required digital certificates for the mail security are stored in the e-Identity™. The cryptographic software comes with a Microsoft signed CSP (Cryptographic Service Provider). The mail security uses the S-MIME standard to guarantee the exchangeability with other users not yet using CompuSec™.

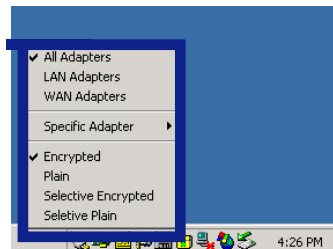
Encrypted files and directories on network drives



File and Directory Encryption with CompuSec™ can be performed for local or network files and/or directories. This function will ensure that all files written or copied into the encrypted directory will automatically be encrypted, 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 also not see the files. This function is used to separate users of the same file server in a strong cryptographic way and to ensure that server administrators cannot see the contents of the encrypted files. This function is called SafeLan and requires the NTFS file system.

Advanced VPN Client for secure connections to corporate networks

CompuSec™ provides IP encryption for WAN and LAN users. An enhanced IPSec client is a selectable function of CompuSec™. The IP encryption client supports pool address modes, data compression, multiple dial in points and other features, which are explained in detail in our IPCryptor product literature. The IP encryption of CompuSec™ needs an IPCryptor as counterpart in the network.



Installation and Management

CompuSec™ can be installed as a product without a central management station. In this case CompuSec™ creates a security file with all the secret keys of this installation. It is the user's responsibility to keep these keys secret. In larger organizations a central management is recommended. This GlobalAdmin station manages all the CompuSec™ installations and provides functions for unattended installations, automatic software rollout and software update, remote password reset and a complete management of the VPN functions. CompuSec™ can be used as an integrated part of a company wide PKI structure. Details are described in the GlobalAdmin product literature. For large customers with multiple locations a remote e-Identity™ loading station is available. A supplementary product for the user help desk is available to assist support staff with the remote password reset functions. Automatic synchronization with Microsoft user management and Active Directory is provided for the CompuSec™ management.

System Requirements

- PC Notebook or Workstation with Intel architecture
- Windows 2000, XP or NT (limited functions)
- Linux Red Hat and SuSe distributions
- USB bus with either Universal or Open host controller
- 20 MB free hard disk space

CE-Infosys Pte Ltd
390 Havelock Road,
03-02 King's Centre
Singapore 169662.
Tel.: +65 6235 8722
Fax: +65 6235 3164
sg.sales@ce-infosys.com

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 GmbH
Friedrichstrasse 153A,
D-10117 Berlin
Germany.
Tel.: +49 (0) 30 / 20 61 23 18
Fax: +49 (0) 30 / 20 61 23 11
berlin@ce-infosys.com

CE-Infosys GmbH
Bifangstrasse 7,
CH-8730 Uznach
Switzerland.
Tel.: +41 55 280 6060
Fax: +41 55 280 6082
ch.sales@ce-infosys.com