



# Managed CompuSec®

Software Security for Desktop PCs and Notebooks

Managed CompuSec® is a Software Security Suite that protects Desktop PCs and Notebooks. It provides Access Control, Single Sign On, Harddisk Encryption, CD/DVD Encryption, File Encryption, Network Encryption, Container Encryption and VoIP Encryption.

Managed CompuSec® provides high level of security with a flexible and transparent mode of operation. Individuals, small groups of users as well as large enterprises uses Managed CompuSec®. It combines a complete set of security functions, while providing users the option to configure the product to their own needs. Large organisations will also find a lot of special functions to efficiently manage a large implementation of CompuSec, such as unattended installation, centralised rollout, support for disk images, central software distribution, service functions and central user management.

## Pre-Boot-Authentication

Whenever a computer starts, a user authentication is required. This is a prerequisite in order to boot up the operating system. This process provides additional protection since the authentication process is independent of the operating system. The Pre-Boot Authentication needs a User-ID and password within the startup process of the PC. Managed CompuSec® provides several help functions in the pre-boot phase to assist users with forgotten passwords.

## Password Management

Password strategies can be defined according to the organisational needs. This includes password lifetime, password usage count, password change options, minimum and maximum length and more. In situations where passwords are forgotten, a challenge-response procedure with the GlobalAdmin station provides an easy and secure method for users to obtain their new password.

## Single Sign On

Managed CompuSec® will encrypt and store the system logon password together with the username and the domain name to automatically log the users into their operating system. This function provides a greater level of convenience for users who now only need to remember one set of username and password. Managed CompuSec® also provides a keyboard or screensaver lock that users can quickly activate when they leave their systems momentarily.



## Full Harddisk Encryption

The harddisk encryption of Managed CompuSec® uses a fast implementation of the AES algorithm. 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 in the background allowing the user to work on the PC, interrupting the encryption process and shut down the computer at any time. The support of the hibernation mode is very important to mobile users. Hibernation of the PC requires the contents of the RAM to be stored in the hibernation file onto the hard disk before the PC is powered down. When the PC is restarted, the user is required to authenticate himself, then the contents of the hibernation file will be decrypted and reloaded back into the RAM. With this technology it is safe to use the hibernation mode for convenience.

## Encryption of CD's / DVD's & Removable Medias - CDCrypt

CD's /DVD's and removable media devices such as Memory Sticks and USB thumb drives can be encrypted by Managed CompuSec®. The encryption for CD/DVD uses the CD Crypt feature to support internal and external CD burners that are connected using USB or SATA. 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 organisation can easily enforce a policy to use only encrypted Removable Media Devices and CD's / DVD's to minimise the threat of data theft. Such encryption is unobtrusive and does not change the way the user works with these devices.



## Network Encryption for Secure Communication in Corporate Networks

Managed CompuSec® provides IP encryption for WAN and LAN users. An enhanced IPSec client is a selectable function of Managed 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 Cryptor family product literature. The IP encryption of Managed CompuSec® needs at least a Cryptor as counterpart in the network.



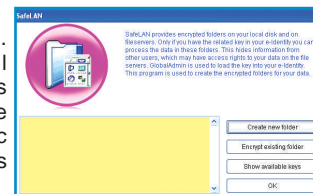
## Encryption of Individual Files - DataCrypt

Managed CompuSec® includes a module that enables users to encrypt individual files, called DataCrypt. DataCrypt will enable users to encrypt files exchanged with third parties and send them via e-mail, ftp etc. DataCrypt can also be used as an independent software module and can be provided to business partners free of charge. DataCrypt employs Public-Key-Cryptography based on elliptic curves to protect session keys for the actual file 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 Managed CompuSec® protects local and 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. This function is completely transparent to the authorised end user. This also means that a user without an authorised directory key will have no access to the directory and is unable to see the files in that directory. This function is used to separate users of the same file server in a strong cryptographic way and ensure that server administrators cannot see the contents of the encrypted files. SafeLan supports NTFS and network based file systems.



## Encryption of Voice Communication - [ClosedTalk]®

[ClosedTalk]® is a component of CompuSec® used for encrypted voice communication between CompuSec® users. The built-in sound system of the computer is used for [ClosedTalk]®. No IP telephone is needed. [ClosedTalk]® uses the 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. The encryption of the voice data is end-to-end and does not pass through any server.



## Container Encryption - [DriveCrypt]

The [DriveCrypt] module provides a simple way to store sensitive data securely on the harddisk without the need to encrypt the entire harddisk. [DriveCrypt] creates a large file on the harddisk and encrypts it using a strong AES algorithm with 256-bit key. The file is then mounted as a separate drive in the file system for normal use. Data written into the "drive" will automatically be encrypted, while data read out will automatically be decrypted.



## Identity Management

Managed CompuSec® manages the identity of the user for applications. For existing applications requiring passwords, Managed CompuSec® learns the users' passwords and user-id's, stores them in an encrypted format and automatically inserts the correct password and user-id into the application when required. This is available for local and WEB based applications.

## Installation & Management

Managed CompuSec® can only be used with a central management station, called GlobalAdmin. The GlobalAdmin station manages all installations and provides additional functions for unattended installations, audit log, remote challenge/respond for password reset and complete management of the VPN functions. GlobalAdmin also manages the access of multiple users to a single machine as well as the access for a single user to multiple machines. Managed CompuSec® can also be used as an integrated part of a company wide PKI structure. Details are described in the GlobalAdmin product literature. Automatic synchronisation with Microsoft user management and Active Directory is provided for the management of CompuSec®.

## Our Support

Service and maintenance contracts are available. Please feel free to contact us to find out more about user support for your organisation.

### System Requirements

- PC, Notebook / Workstation or Tablet PC with Intel Architecture
- Windows 7, Windows Vista or Windows XP (64 & 32 bit mode)
- Windows Server 2003, Windows Server 2008 (64 & 32 bit mode) and Windows Server 2008R2
- 40 MB Free Harddisk Space
- Built-in Sound Card for [ClosedTalk]®



**CE-Infosys GmbH**  
 Am Kümmerling 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**  
 12 Tannery Road  
 #09-01/02 HB Centre 1  
 Singapore 347722  
 Tel.: +65 6899 9392  
 Fax: +65 6899 9373  
 sg.sales@ce-infosys.com

CompuSec and [ClosedTalk] are registered trademarks of CE-Infosys Pte Ltd in Singapore.  
 UPEK and TouchStrip are registered trademarks of UPEK, Inc

Reseller: