



CompuSec[®] BIO

Biometric Security for Desktop PCs

CompuSec[®] BIO integrates a fingerprint scanner with a built-in smart card reader to the comprehensive set of security functions found in CompuSec[®] e-Identity[®]. CompuSec[®] BIO brings a higher level of security with greater convenience that users can now enjoy.

CompuSec[®] BIO provides 3-factor Access Control, Single Sign On, Hard Disk Encryption, CD encryption, file encryption, network encryption and VoIP encryption. CompuSec[®] BIO is ideal for customers who want a high level of security, while maintaining a flexible and transparent mode of operation. Large organizations will also find all the additional functions required to efficiently manage a large implementation of CompuSec[®] BIO with unattended installation, centralized rollout, support for disk images, central software distribution, service functions and central user management.

CompuSec[®] BIO uses the latest technologies developed by CE-Infosys to provide functionalities previously unknown to PC security products, such as Pre-Boot access to the Fingerprint scanner, the use of PKI technology before a system boots and support for Hibernation mode.

Easy and Safe

CompuSec[®] BIO introduces the use of fingerprints as a factor in the Pre-Boot Authentication process. Users will be able to use fingerprints from one or multiple fingers to identify themselves. The template of each fingerprint will be captured and stored inside the e-identity[®] smart card for added security. With the use of fingerprints, CompuSec[®] BIO users will now be able to protect their PCs or notebook with up to three-factor pre-boot authentication. Users can now choose from a range of authentication methods:

Authentication	Combination 1	Combination 2	Combination 3
Fingerprint	No	Yes	Yes
Password	Yes	No	Yes
e-Identity [®]	Yes	Yes	Yes

Pre-Boot-PKI

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



Password Management

The password strategies can be defined according to the organizational need. 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 help for users to obtain a new password. CompuSec® BIO users have the option not to use passwords when they opt only to authenticate with their Fingerprint and smart card.

Single Sign On

CompuSec® BIO includes a Single Sign On component that will automatically log users into their local machine or their Windows Domain. The username and password or digital certificate will be automatically supplied by CompuSec® to provide greater convenience to users. CompuSec® BIO will deactivate the screen saver and keyboard lock with a quick scan of the user's finger.



Identity Management

CompuSec® BIO manages the identity of the user for applications. For existing applications requiring passwords, CompuSec® BIO 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® BIO manages the complete application policies for each user. CompuSec® BIO 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.

Hard Disk Encryption

The hard disk encryption of CompuSec® BIO 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 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.



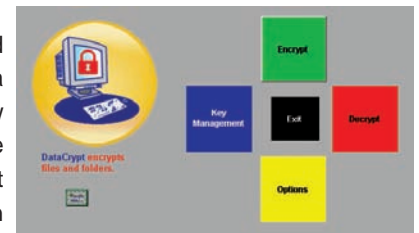
Encryption of Diskettes, CD-ROM & Removable Media - CDCrypt

Diskettes, CD / DVD and removable media devices such as Memory Sticks and USB thumb drives can be encrypted by CompuSec® BIO. 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.



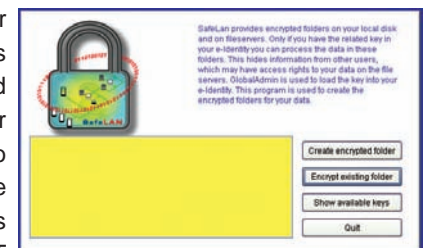
Encryption of Individual Files - DataCrypt

CompuSec® BIO 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® BIO 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.



Advanced VPN Client for Secure Connections to Corporate Networks

CompuSec® BIO provides IP encryption for WAN and LAN users. With a scan of the user's finger, an enhanced IPsec client will be enabled for secure remote connections. 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® BIO needs an IPCryptor as counterpart in the network.



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

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



Encryption of Voice Communication - [ClosedTalk]™

[ClosedTalk]™ is a component of CompuSec® BIO 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 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.



Installation & Management

CompuSec® BIO can be installed as a product without a central management station. In this case, CompuSec® BIO 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® BIO 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 BIO loading station is available. A supplementary 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 the management of CompuSec® BIO.

About e-Identity® Smart Cards

Each CompuSec® BIO 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, PKCS#11, Microsoft CSP including an integrated driver-to-driver interface.



System Requirements

- PC Notebook or Workstation with Intel Architecture
- Windows 2000, XP
- Linux Red Hat & SuSe Distributions
- 40 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: