



■ CompuSec™ with e-Identity USB Token or Smart Card Reader

The heavy reliance on PCs today has led to the tremendous increase in computer related crimes. The computer today is the access point of an endless amount of information. So much critical information resides in your computer that PC security can no longer wait to be implemented.

CompuSec™ is the leading personal computer security product designed to provide a strong security system for PCs modelled after our hardware-based security systems, Elkey and CryptCard. CompuSec™ will protect your system from unauthorised access, encrypt your entire hardisk to ensure confidentiality of your data, additional level of encryption for files and folders in your local and/or network drive, floppy drive encryption and a secure storage for your access keys.

■ **Strong Access Control** built into your system with CompuSec™ will protect your PC from unauthorized access. CompuSec™ requires you to enter a password together with a secured hardware token to authenticate yourself prior to your system booting up. This hardware token - your e-Identity™ - can either be CE-Infosys' USB token or a smart card inserted into CE-Infosys' USB smart card reader. Additional access control features found in CompuSec™ allow the setting of sophisticated password policies, defining the types of password that a user is allowed to enter. Password requirements such as the password lifetime, change strategies, complexity parameters and more can also be set to your requirements.

■ **Single Sign On** in CompuSec™ allows you to automatically login to a windows environment by keying your password only once, when you authenticate yourself prior to boot-up. CompuSec™ learns from your login information during the logon and stores it in your e-Identity™ token. When you logon the next time, all required login information would be automatically provided from your e-Identity™ token.

■ **Hard Disk Encryption** is the primary mechanism used to keep your data confidential. Your entire hard disk will be encrypted using standard algorithms like Triple DES or AES, with the option for you to specify a customized algorithm that you would like to plug-in. Authentication prior to boot-up with full hard disk encryption, which includes the encryption of the operating system, will protect your system from attacks such as the "Trojan Horse". Moreover, full hard disk encryption is performed using an intelligent program that optimizes computer resources, ensuring fast encryption speeds that will not slow down your work.

■ **File and Directory Encryption** with CompuSec™ can be performed for local or network files and/or directories. This feature 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 and suitable hierarchical permissions will not have access to the directory. Where all files in the protected directory is invisible to users. This feature is available when CompuSec™ is installed on operating systems that support NTFS (Windows NT File System).





■ **Floppy Drive Encryption** in CompuSec™ allows users to secure their floppy diskettes when transferring files between their CompuSec™ protected PCs. This feature will ensure that all files written in the floppy is encrypted and only accessible by authorized users.

■ **IPCrypt Client** for IP encryption comes free with CompuSec™ for Secure Remote Access solutions. IPCrypt Client complements IPCryptors, providing VPN connections to company resources with automatic user authentication, completely transparent to the user. To find out more about IPCrypt Client, please refer to our IPCrypt Client USB brochure.

■ **Installation of CompuSec™** is easy and can be done in various ways. If you use CompuSec™ in a large organization, an automated installation process via the company network is available. Programming of e-Identity™ smart cards, tokens, the management of the keys and the installation data are then done by a central administration system - GlobalAdmin. For individual users, the CD based installation provides you with an easy-to-use program that will program your e-Identity™ smart card or USB token on your machine.

■ **Technical Specifications:**

- Made for Windows XP, W2K (ME and 98 will soon follow)
- Access control by token and knowledge
- Configurable password length 6-16 character
- False password threshold
- Password lifetime and expiration data manager
- Password complexity check
- Secure remote password reset with cryptographic challenge response
- Single Sign On (for Windows XP and W2K)
- Full or Partitioned hard disk encryption
- Additional file/directory encryption for local and/or network drives (on NTFS File Systems)
- Floppy disk encryption
- Multiple operating systems on one hard disk
- Boot virus recovery
- Support of multiple smart card versions
- Easy client deployment via network or CD-ROM or image distribution
- Central administration using GlobalAdmin
- IPCrypt Client for additional IP encryption
- Option: Customer replaceable cryptographic algorithm
- Option: Auto logon for automated software update

