# SecureDoc
## DISK ENCRYPTION

## The most secure and versatile disk encryption software

**Secure**

⇨ FIPS 140-1 Level 2 Certification
⇨ Common Criteria Validation
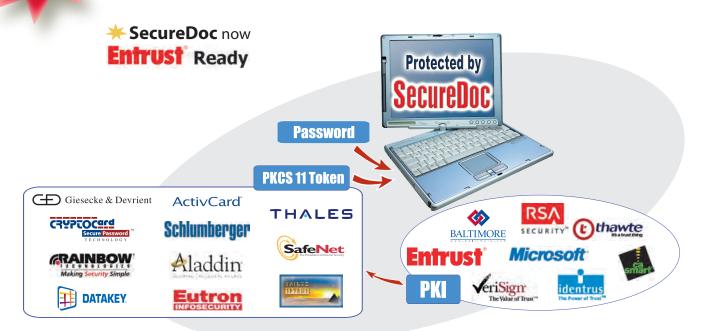⇨ 256-bit AES Cryptographic Module Validation from NIST/CSE (Certificate #1)
⇨ CAPS Certification (for the UK government) in progress.

**Versatile**

⇨ 1, 2 or even 3-factor Authentication at Pre-Boot using
SMART CARDS, USB TOKENS, BIOMETRICS and PKI (Public Key Infrastructure).
⇨ SecureDoc Keys can be placed on hardware tokens, thus the encryption keys – even encrypted – do not exist on the disk.

**New**

⇨ SecureDoc now supports HIBERNATION MODE in Windows 2000/XP/2003.
⇨ Supports popular TABLET PCs with on screen keyboard at Pre-Boot.
⇨ Supports US DoD Common Access Card.

**SecureDoc** now
**Entrust** Ready

**Protected by**
**SecureDoc**

Password

PKCS 11 Token

Giesecke & Devrient
CRYPTOCard Secure Password TECHNOLOGY
RAINBOW TECHNOLOGIES Making Security Simple
DATAKEY
ActivCard
Schlumberger
Aladdin
Eutron INFOSECURITY
THALES
SafeNet The Foundation of Internet Security
SPYRUS

BALTIMORE
RSA SECURITY
thawte its a trust thing
Entrust
Microsoft
casmart
VeriSign The Value of Trust
identrus The Power of Trust

PKI

# www.winmagic.com

**WINMAGIC**
**DATA SECURITY**

# SecureDoc DISK ENCRYPTION

## *Trusted by the most security-conscious organizations worldwide.*

## COMPREHENSIVE AND FLEXIBLE

- Entire Disk Encryption: Every byte of data is encrypted. SecureDoc secures residual data, temporary files, paging files and hidden partitions left unprotected by other encryption methods.

- Transparent operation. User works as usual after entering a password and/or smart card or USB token at boot logon.

- Fully customizable text and color screen at boot logon. Users can choose the language, text and color (foreground/background) of their preference.

- An unlimited number of users can be issued individual key files to access a single computer.

- Password Rules assist users in password preparation - thus readily conforming to in-house security policies and pratices.

- Single Sign-On with Windows. SecureDoc locks computer if the token is removed

- Disk-lock precludes unauthorized copying of data to floppy disk or other removable drives. Configurable to allow only encrypted removable media.

- Compatible with disk defragmentation software, even Windows built-in utility.

- Compatible with disk imaging software such as Ghost, Drive Image (image and compress encrypted disks) and Rapid Restore (disk and images are always encrypted on the PC).

- Works seamlessly with boot manager utilities such as BootMagic or System Commander. Multiboot to different OSes.

- Encryption support for floppy, Zip, Jaz, USB drives as well as the IBM MicroDrive PC-Card.

- Encrypt or Wipe Files and Folders. SecureDoc File Viewer is available free of charge for non-SecureDoc users.

## SECUREDOC PDA for encryption of Pocket PC devices.

## SECUREDOC ENTERPRISE SERVER

- Remotely manages users' computers over LAN and WAN network environments. SecureDoc employs its secure and efficient communication on SOAP (Simple Object Access Protocol) standard protocol to be compatible with different networks and corporate firewalls.

- Uses LDAP to work with directories such as Active Directory and PKI servers. Other methods to import users' profiles and credentials are available.

- Web-based password recovery provides a secure way to recover access to user's computer in case the smart card or USB token or password is lost – eliminating extra work for the help desk.

- By using MS SQL server or MS Access Database as back end, SecureDoc Enterprise Server can scale up to hundreds of thousands of users. Concepts of different levels of administrators, folders and groups help organize user information. Group operations allow modifying users' data with just a few mouse clicks.

## SECUREDOC'S UNIQUE DESIGN, NOT FOUND IN ANY OTHER DISK ENCRYPTION PRODUCTS

### 1. PKCS #11 (Public Key Cryptographic Standard #11)

SecureDoc utilizes the architecture of PKCS#11 from the ground up. This adherence to Industry Standards results in a higher degree of security due largely to world scrutiny and efficient interoperability.

### 2. ROLE & IDENTITY-BASED KEY LABELING

SecureDoc allows the option of labeling keys utilized for encryption. This feature results in the ability to share access of encrypted objects in a very flexible way. It offers customization such as specifying precisely which user or group of users can or cannot access an encrypted hard disk, floppy disk or other removable disks.

### 3. CENTRALIZED ADMINISTRATION WITHOUT "MASTER PASSWORD"

Outdated encryption designs still rely upon a single password, called "Master Password" allowing access to all of the computers in the enterprise. This flaw carries tremendous ramifications: If the Master Password is compromised, then all of the computers in the enterprise are compromised.
SecureDoc's unique approach to user keys and key files breaks away from the competition, offering peace of mind without any of the "Security Holes" associated with a "Master Password".

**WINMAGIC DATA SECURITY**