



WinMagic Data Security™ Enterprise Full Disk Encryption Solutions

23 Differentiating Features

January 2007



Knowing
You're Protected

(This page left intentionally blank.)

- Corporate Profile..... 5**
- SecureDoc™ 7**
 - SecureDoc™ 7
 - SecureDoc Enterprise Server™ 7
 - Compartmental SecureDoc™ 7
 - SecureDoc PDA™ 7
 - SecureDoc: All Inclusive Protection..... 7
- SecureDoc™ Features 9**
 - Design and Architecture..... 9
 - Pre-Boot Authentication 9
 - Flexible Key Labeling 9
 - No "Master Password" Vulnerability 9
 - Transparent Operation and Thorough Encryption 9
 - Supports PKI (Public Key Infrastructure) Starting at Pre-boot Time 9
 - Integrates with USB Tokens and Smart cards..... 9
 - Increased Compatibility 9
 - Encrypts Removable Drives 9
 - Protected Multi-Users for Shared Computers 9
 - Fully Customizable Text and Color Screen at Boot Login 9
 - Single Sign On 9
 - Password Rules 10
 - Secure Screen Saver 10
 - Disk Lock..... 10
 - Enterprise Version..... 10
 - Algorithms Used 10
- 23 Unique Features of SecureDoc 11**
- Common Questions in considering Full Disk Encryption 13**
 - Prerequisite Criteria 13



(This page left intentionally blank.)



Corporate Profile

WinMagic's mission is to become the world leader in full-disk encryption through high standards and strong ethics. Our worldwide award-winning products fulfill the requirements of even the most security conscious users by focusing on concrete policy-driven security features, while simultaneously offering unparalleled flexibility and ease of use. WinMagic's sole purpose is to meet the marketplace demand for solutions that eliminate "data at rest" problems.

WinMagic Inc. commenced its operations in 1997. It is now operating through direct and/or indirect channel support in over 43 countries. WinMagic has been supporting the AES algorithm since its adoption. It is able to provide seamless integration with single- or multi-factor authentication technology right at pre-boot. SecureDoc addresses data security needs of today's increasingly-mobile workforce, by making it simple to protect all information on desktops, laptops, removable media, and PDA's.

WinMagic Inc. provides the world's most secure full disk encryption software represented by the SecureDoc product suite including: SecureDoc, SecureDoc Enterprise Server, Compartmental SecureDoc, SecureDoc PDA, and SecureDoc Personal Edition. Its SecureDoc line of products ensures protection of sensitive information stored on desktops, laptops, and other mobile devices by employing authentication from password to hardware token, biometrics, and PKI commencing right at pre-boot time.

WinMagic's world wide award winning products fulfill the requirements of even the most security conscious users by focusing on concrete policy driven security features, while still offering unparalleled flexibility that also incorporates the Unicode Standard. Utilizing Public Key Cryptographic Standard PKCS #11 (Cryptographic Token Interface Standard) from the ground up for extreme adaptability, the SecureDoc line has earned an impressive list of validations including NIST Cryptographic Module Validation, FIPS 140-1 Level 2, FIPS 140-2 Level 1 & 2, and is scheduled to achieve the Common Criteria Evaluation Assurance Level 4 (EAL-4) certification in early 2007.

Consistently delivering originality and advancement over the last 10 years, WinMagic offers support for Trusted Platform Module - TPM v1.1 and v1.2, and biometric support for pre-boot authentication. WinMagic's competitive advantage resides not only in the robustness of our full-disk encryption solution, but equally in our ability to customize our products to fit into our customer base's IT infrastructure and comply with their respective corporate governance with regard to privacy and security. As an example, WinMagic took on the challenge of a two year old project at the National Security Agency (NSA) that was doomed to failure, and provided an appropriate solution within 6 months. After the FORTEZZA card project with the NSA, WinMagic has been offering smartcard and PKI integration at pre-boot since 2000.

WinMagic is proud of to be a global leader in hard disk and removable media encryption technology. SecureDoc is certified, authenticated, implemented, and used by the most sensitive Government offices including the NSA, IRS, SSA, US State Department, NIST, Homeland Security, DoD.

Our SecureDoc Disk Encryption software uses state-of-the-art AES 256-bit encryption to fully encrypt every aspect of the hard disk, and removable media, including the boot record, operating system, user data, software applications, paging/swap files, temporary files, offline folders of an email application, the recycle bin, deleted but not erased files, and disk sectors that are not fully written (slack space). It is designed to be an "install-and-forget" solution which, once installed, is fully transparent to the user.

As a thought leader and innovator, we are proud of our leading edge record of accomplishments and capabilities:

DISK ENCRYPTION

- 1) The only disk encryption certified by the National Security Agency (NSA) for SECRET data for US government agencies (for the FORTEZZA based SecureDoc), see <http://www.winmagic.com/images/nsacert.jpg>,
- 2) The only disk encryption software to have FIPS 140-2 level 1&2, see <http://csrc.nist.gov/cryptval/140-1/1401val2006.htm> with the crypto module validation AES (256-bit) encryption algorithm with certificate number 1 by NIST <http://csrc.nist.gov/cryptval/cmvp2002/photos.html>,
- 3) The only disk encryption to support DoD Common Access Card Smartcard, and even pass the PKI enable interoperability test at Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC), see http://jitc.fhu.disa.mil/pki/vendor/winmagic_securedoc3_8.html,
- 4) The first and only disk encryption to be used for HSPD 12, FIPS 201 (at State Department).
- 5) The first organization to provide support for:
 - ▶ Hibernation
 - ▶ Imaging software such as Ghost
 - ▶ Windows 2000, Windows VISTA
 - ▶ SQL database for centralized management through the introduction of WinMagic's SecureDoc Enterprise Server causing others to stop advertising "master password" as a feature due to its vulnerability.

SecureDoc simply represents the most robust full-disk encryption solution available today in that it is the fastest to encrypt the hard drive while taking into consideration intentional or unintentional power interruptions, bad sectors, and a potential need for the Windows OS to conduct pre-fetch (defrag).

SecureDoc™

SecureDoc: A commercially available full-disk encryption software application designed specifically to run transparently with Windows Vista/2000/XP/2003. While thoroughly encrypting all residual data, temporary files, paging files, and hidden partitions, SecureDoc utilizes the AES 256-bit encryption algorithm to encrypt the entire hard-drive where every byte is encrypted. It is superior to other encryption products and technologies in its robustness and reliability. It offers many exciting new features including the ability to run disk utility applications like "ghost" on drives that may or may not have bad sectors.

SecureDoc™

WinMagic's SecureDoc encryption software addresses the needs of organizations increasing mobile workforce by ensuring protection of sensitive information stored on desktops and laptops by employing authentication from password to hardware token, biometrics, and PKI commencing right at pre-boot time. SecureDoc presents a user-friendly solution, providing solid security for PCs and laptops alike by utilizing Public Key Cryptographic Standards PKCS-11. SecureDoc has achieved validations for Common Criteria, FIPS 140-1 Level 2, and FIPS 140-2 Level 1 & 2.

SecureDoc Enterprise Server™

The SecureDoc Enterprise Server lets administrators install, encrypt, and configure user machines centrally. It enables secure, yet flexible creation, distribution of key and key files as well as assignment of access privileges to users. The administrators can customize password rules for the entire network, as well as recover lost passwords through a secure one-time challenge and response online engine. Most importantly: the unique design of the SecureDoc Enterprise Server's Key file management eliminates all the vulnerabilities associated with the "Master Password" concept so commonly used by other encryption software.

Compartmental SecureDoc™

Compartmental SecureDoc offers an affordable software-based solution to create compartments on a computer, which are also enforced by encryption. Based on WinMagic's SecureDoc Disk encryption software, Compartmental SecureDoc offers all the features of SecureDoc and in addition, offers a viable solution for laptop computers. With Compartmental SecureDoc, a laptop computer can be a Compartmental Computer, functioning as a Multi-Level Security System. It offers AES 256-bit encryption for USB/FireWire External Drives, pocket drives, flash cards, PCMCIA Drives, Zip, Jazz, etc. - thus providing a full range of protection for virtually all forms of storage devices.

SecureDoc PDA™

SecureDoc PDA™ addresses the needs of an organization's increasingly mobile workforce, with more and more data to protect than ever. SecureDoc PDA utilizes the versatility and security of WinMagic's award-winning SecureDoc functionality, offering strong encryption through the 256-bit AES encryption algorithm. The encryption process takes place transparently in the background, invisible to PDA users.

SecureDoc: All Inclusive Protection

SecureDoc addresses the needs of organizations increasingly mobile workforce, with more and more data to protect than ever. Comprehensive and flexible, SecureDoc has earned validations such as Common Criteria, FIPS 140-2 level 2; its FORTEZZA-based version is the only disk encryption software certified by the NSA to protect SECRET data for US government agencies.



(This page left intentionally blank.)

SecureDoc™ Features

Design and Architecture

Utilizing Public Key Cryptographic Standards PKCS-11 from the ground up, WinMagic designs its Disk Encryption product with security and flexibility unparalleled in the industry.

Pre-Boot Authentication

SecureDoc integrates with popular third-party tokens and Public Key Infrastructure (PKI) commencing **at pre-boot time**. SecureDoc provides the upgrade path from a password-only solution to enterprise-wide token-based PKI integration.

Flexible Key Labeling

Versatile key labeling is provided so the users can share encrypted files, disks, and **removable media**.

No “Master Password” Vulnerability

Unique centralized key management without using the comprising “master Password” concept.

Transparent Operation and Thorough Encryption

After installing SecureDoc, the encryption process is transparent. This means the computer user does not need to worry about the encryption process because it takes place automatically in the background.

Supports PKI (Public Key Infrastructure) Starting at Pre-boot Time

SecureDoc works seamlessly with virtually all PKI suppliers e.g. **CyberTrust, CA, Digital Signature Trust, Entrust, Identrus, Microsoft, RSA Verisign**, and other PKI vendors. Users need only one token to work with all applications.

Integrates with USB Tokens and Smart cards

SecureDoc offers dual and triple factor authentication for ultimate security and protection (password, tokens, and biometrics). It works with ActivCard, Aladdin, Datakey, Eutron, Kobil, Rainbow, and other industry leading suppliers of tokens.

Increased Compatibility

SecureDoc is compatible with Windows 2000/XP and 2003 operating systems. Integrates and works seamlessly with most antivirus software, boot manager utilities such as BootMagic and System Commander. Disk imaging software such as PowerQuest DriveImage can image an encrypted disk.

Encrypts Removable Drives

Easily encrypts floppy, Zip, Jazz drives, USB, PCMCIA, memory sticks, Firewall drives as well as flash drives such as IBM MicroDrive PC-card.

Protected Multi-Users for Shared Computers

An unlimited number of users can be issued individual keys to access a single computer. Users can easily choose the method of securing their computer utilizing a password-only and/or token integration.

Fully Customizable Text and Color Screen at Boot Login

Users can choose the language, text, and color (foreground/background) of their preference.

Single Sign On

Users can be configured to sign into Windows operating system with only one password.

Password Rules

Users can set up personal passwords with appropriate expiry dates conform to in-house security policies and practices.

Secure Screen Saver

SecureDoc screen saver protects against CD-ROM attacks. In the event the user prefers to leave his/her computer running but unattended – the token is simply removed thereby locking it down. To activate the computer, the token is reinserted and access is restored.

Disk Lock

Disk Lock precludes unauthorized copying of data to floppy disks.

Enterprise Version

For enterprise wide deployment of SecureDoc,

- Central Administration allows “silent” installation, installs and set up user’s PC’s through the network without any administration on the client PCs.
- Central Database lets the administrator manage users and keys. The central administrator has access to all PCs, guaranteed to be able to recover data in case the employee leaves the company.
- Remote one-time password key recovery allows user to log on to use the PC if the user forgets the password. Help desk can issue an one-time key unlock password on a challenge-response way so an attacker would not be able to access the PC even if the attacker intercepts all transmitted data.

Algorithms Used

For encryption, the Advanced Encryption Standard ([AES](#)) 256-bit, encryption algorithm is used. The hashing algorithm used is [SHA-2](#).

23 Unique Features of SecureDoc

The following list describes 23 features that distinguish WinMagic's SecureDoc from its competition.

Centralized Management with Standard DBMS

- Enterprise class DBMS
- Communication with Client PCs
- Unlimited Profiles
- Centralized Administration

SecureDoc Enterprise Server (SES) uses Microsoft SQL Server as its data repository. This ensures our enterprise customers have a scalable DBMS that supports distributed computing, backup functionality, replication and clustering.

SES communicates with client-PC's via LAN, over the Internet, intermittent network or even if users do not have network access at all.

SecureDoc Enterprise Server (SES) provides centralized administration for client's machines

It provides several schemes of centralized deployment, import of user's data from an LDAP directory or Active Directory Service or PKI, remote control of client through encrypted communication, on-line password recovery via Web and more.

Strong Biometric Support

Support for biometrics devices – all at **pre-boot**. WinMagic's SecureDoc is the only product to support biometrics at **pre-boot**. It has been used by the U.S. Department of State in HSPD-12, FIPS 201 compliant projects.

Strong Access Control with Multifactor Authentication via passwords and Hardware Tokens

Pre-boot support for smartcards, USB crypto tokens and PKI.

As hardware tokens are gaining popularity, authentication and SSO become more important. WinMagic has delivered smartcard and PKI integration with SecureDoc since 2001 (e.g. to the New Zealand govt.).

Trusted Platform Module (TPM) Support

SecureDoc supports TPM security chip at boot time. The TPM chip is embedded in newer laptops.

Interoperability with imaging software

SecureDoc interoperates with Ghost, Drive Image, Rapid Deploy, BootWorks, Rapid Restore and Rescue & Recovery. This significantly enhances the deployment capabilities within large organizations.

Virus Recovery

User is able to recover data even if the disk is infected by viruses. The recovery software works as if the disk is not encrypted.

Compatible with various boot managers

SecureDoc is compatible with various boot managers. These include Boot Magic, Boot-US and Windows boot manager. SecureDoc supports systems that have multiple operating systems (multi-boot).

Compatible with Partitioning Software Managers.

Please note that SecureDoc supports unlimited number of partitions.

SecureDoc operates with partitioning software such as Partition Magic. Encrypted disk partitions can be resized; partitions can be added or deleted as if the disk is not encrypted.

Compatible with VMWARE Supports Hibernation Mode

SecureDoc works with VMWare "out of the box".

SecureDoc protects data in hibernation mode.

Supports removable media

SecureDoc supports removable media (USB memory sticks, SD cards, ZIP, JAZ, etc.): Administrators can configure SecureDoc in order to:

- Disable all removable media access
- Allow read-only access if the removable media is not encrypted
- Allow access only if the removable media is encrypted (with pre-defined keys etc.).

Power Out Protection

Robust capabilities that allow the initial encryption (conversion) to be interrupted by a power outage without data loss.

Large Disk Support

Support disks of larger than 2,000 Giga bytes and unlimited number of partitions. Furthermore, different partitions can be encrypted with different keys, e.g. for sharing.

Magneto Drive Support

Support for encryption of Magneto Optical drives. Even though the removable Magneto Optical drives are most popular in Asia, the technology to support drives with sector sizes different than 512 bytes show the thoroughness and the modularity of the SecureDoc software design.

Support for RAID controllers

SecureDoc can be used in a server environment with RAID controllers.

Full Disk Encryption

Encryption of the entire disk, not only partitions.

Compartmental Encryption Version

A test at Network Computing showed that users can add partitions and SecureDoc automatically encrypts them.

Robust encryption

Divides the disk into compartments, encrypted by different cryptographic keys. The separation is so strong that a virus in one compartment will not affect the other compartments. User can run any defragmentation tool during the initial encryption conversion.

Support of SHA-2

WinMagic has used the more advanced SHA-2 with SecureDoc V4 since early 2005

FIPS 140-2 Level 2 (Certificate # 698)

WinMagic is the only Software Encryption vendor on the planet to offer this level of protection regarding disk encryption.

Unicode Standard Support

The Unicode Standard is an industry wide standard designed to allow text and symbols from all of the writing systems of the world to be consistently represented by computers. WinMagic's comprehensive support for Unicode, a global language standard, will allow customers to centrally maintain and manage implementations of SecureDoc in virtually every modern language in a single database.

Supports Microsoft Windows Vista

Immediately available to early adopters, SecureDoc is uniquely positioned to compliment Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, and Windows Vista Ultimate. The same purity of design that prevents hackers from bypassing the encryption level while simplifying integration with single or multi-factor authentication through tokens, biometrics, and PKI technology has allowed WinMagic to deliver full Vista support to customers in just one week. It is this competitive advantage that will allow WinMagic to fully support Windows Vista today, and as Windows Vista evolves.

Supports Removable Media encrypting full CD / DVD

SecureDoc encrypts CD/DVD automatically when data is written to it. Downloadable versions of DiskViewer and ContainerViewer allows non-SecureDoc users and non-SecureDoc encrypted endpoint devices to read encrypted external hard drives, USB thumb drives, and CD's / DVD's.

Common Questions in considering Full Disk Encryption

Prerequisite Criteria

Robustness

- Q. Can your encryption software recover during the hard drive encryption process (converting) if it were to be interrupted by either intentional or unintentional power failures?
- A. At WinMagic, we believe that an full disk encryption product should be able to recover from any type of interruption. Our SecureDoc product was tested using a typical laptop (IBM T43 with 1.86ghz processor and 1.50gb of RAM) and passed our interruption test, including power interruption. During initial encryption, the laptop was put in Standby mode, Shutdown mode, Sleep mode, Turned off, and the battery and power supply where disconnected. The test resulted in no lost of data or system crashes. Once the computer system came back up, the SecureDoc encryption process continued right where it left off.
- Q. Given that hard drives will be encrypted during every day use, could you please describe the conditions under which you stress tested your full disk encryption software?
- A. SecureDoc has been stressed tested with a variety of computers including laptops/desktops containing common hard drives sold into the corporate and commercial market segment today. The conditions that were used are similar to the conditions that exist for the average user such as creating MS Word documents, accessing large graphic files, Internet access, accessing/writing emails, copying files, compressing/decompressing files using various compression tools available today. SecureDoc has passed our stressed testing with negligible derogation to the speed of the device.
- Q. If the hard drive contains bad sectors, how does your full disk encryption software handle them?
- A. If SecureDoc detects that there are bad sectors on the hard drive, we will skip over them and continue with the encryption. Some of our competitors require that you use a 3rd party tools in order to mark the bad sectors before their encryption solution can begin, or they simply fail the encryption process.
- Q. Does the hard drive need to be defragmented before I distribute and execute your full disk encryption software?
- A. SecureDoc encrypts the hard drive on a sector by sector level. Due to our encryption process, we do not require that the drive be defragmented before the encryption process begins. Some of our competitors require that in order to gain optimal performance during encryption with their product, you need to defragment the hard drive. This process can be quite cumbersome to mandate to a fleet of notebooks, desktops, and other mobile devices across a LAN or WAN when they may or may not be connected, adding time and complexity to the security solution that our customer are looking to implement in encrypting their machines.

Speed

Q. What are the average size hard drives that we are seeing today on desk-tops and notebooks? Could you indicate the average speed to reliably and fully encrypt these hard drives?

A. Given our deployment of over 1.5 million licenses over 9 years, we have seen that the average hard drive size for desk tops and notebooks are now approaching anywhere between 60GB - 320GB depending on laptop or desktop. This includes both internal and external hard drives. SecureDoc can encrypt a hard drive at a minimal rate of 20GB/hour depending on processor. With Dual Core processors becoming the standard in most laptops and desktops, our encryption time can be anticipated to be faster, for example 50 GB per hour. Some of our competitors have been benchmarked to take over twice the amount of time to encrypt a hard drive.

(This page left intentionally blank.)



200 Matheson Blvd. West, Suite 201
Mississauga, ON, Canada L5R 3L7

Tel: (905) 502-7000
Fax: (905) 502-7001
Web: www.winmagic.com
Email: inquiries@winmagic.com

WinMagic Inc. is headquartered in Mississauga, ON (Toronto) Canada and is now operating through direct and indirect channel support in over 43 countries. For more information concerning its products or services, please visit www.WinMagic.com or call 1-888-879-5879, or email info@WinMagic.com.

©Copyright 2007 WinMagic Inc. All rights reserved. This document is for informational purpose only. WinMagic Inc. makes NO WARRANTIES, expressed or implied, in this document. All specification stated herein are subject to change without notice. All other brand or product names are trademarks or registered trademarks of their respective owners.