



# **WINMAGIC**

## **DATA SECURITY**

Knowing You're Protected

# WinMagic Data Security™

## Enterprise Full Disk Encryption Solutions

WinMagic Inc.  
November 2006

©Copyright 2006 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.

---

201- 200 Matheson Blvd. West, Suite 201  
Mississauga, ON, Canada L5R 3L7  
Tel: (905) 502-7000 Fax: (905) 502-7001  
Web: [www.WinMagic.com](http://www.WinMagic.com) Email: [inquiries@WinMagic.com](mailto:inquiries@WinMagic.com)

*(This page left intentionally blank.)*



# WINMAGIC DATA SECURITY

Knowing You're Protected

- Executive Summary ..... 5**
  - Corporate Profile ..... 6
  - Mission Statement ..... 6
  - Company Background ..... 6
  - References ..... 6
- The Need for Full Disk Encryption..... 7**
- Common Desktop Security Software Problems ..... 9**
  - Temporary Files ..... 9
  - Paging Files ..... 9
  - File Slack ..... 9
  - The Recycle Bin..... 9
  - The Windows Registry ..... 9
  - The Windows NT File System (NTFS) ..... 9
  - Hibernation and Sleep Mode..... 10
  - Hidden Partitions ..... 10
  - Free Space and Space between Partitions ..... 10
  - Summary ..... 10
- Analysis of the Different Encryption Methods ..... 11**
  - Manual File Encryption ..... 11
  - Folder Encryption ..... 12
  - Virtual Drive/Disk Encryption..... 13
  - Disk Encryption ..... 14
  - Boot Protection ..... 14
  - Full Disk Encryption: The Logical Choice ..... 14
- SecureDoc™ ..... 16**
  - SecureDoc™ ..... 16
  - SecureDoc Enterprise Server™ ..... 16
  - Compartmental SecureDoc™ ..... 16
  - SecureDoc PDA™ ..... 16
  - SecureDoc: All Inclusive Protection ..... 16
- SecureDoc™ Features ..... 17**
  - Design and Architecture ..... 17
  - Pre-Boot Authentication..... 17

- Flexible Key Labeling..... 17
- No "Master Password" Vulnerability ..... 17
- Transparent Operation and Thorough Encryption..... 17
- Supports PKI (Public Key Infrastructure) Starting at Pre-boot Time..... 17
- Integrates with USB Tokens and Smart cards ..... 17
- Increased Compatibility ..... 17
- Encrypts Removable Drives..... 17
- Protected Multi-Users for Shared Computers..... 17
- Fully Customizable Text and Color Screen at Boot Login ..... 17
- Single Sign On ..... 17
- Password Rules ..... 18
- Secure Screen Saver..... 18
- Disk Lock ..... 18
- Enterprise Version ..... 18
- Algorithms Used ..... 18
- 22 Unique Features of SecureDoc ..... 19**
- Certifications ..... 21**
- Common Questions in considering Full Disk Encryption..... 24**
  - Prerequisite Criteria ..... 24
  - Authentication..... 26
  - Certificates ..... 28
  - Compatibility ..... 30
  - Deployment..... 31
  - Directory Management ..... 32
  - Encryption..... 33
  - Hardware Support ..... 34
  - Management..... 35
  - Recovery..... 36
- Appendix A: Glossary..... 37**
- Appendix B: References..... 40**

## Executive Summary

WinMagic commenced operations in 1997. Their product, SecureDoc, is the only disk encryption product based on PKCS#11 Standard (industry standards for API between applications and “token” or cryptographic engine module) from the ground up – even between internal components. This foundation has enabled WinMagic to deliver SecureDoc based on the FORTEZZA card to the United States National Security Agency (NSA) within 6 months which enabled WinMagic to secure the only world wide certification to protect SECRET data for the US government. In addition, WinMagic has been supporting AES algorithm since very early 2000.

Not only based on the fact that the NSA has assisted WinMagic greatly in their product development and testing since 1999, they are confident that SecureDoc is the most SECURE disk encryption product available anywhere.

While similar products might provide some similar functionalities (such as remote password recovery, or “secure” communication between server and clients), WinMagic does not think any of its competitors made as much effort as they did to design and balance between security and user-friendliness including the provisioning of details on how SecureDoc does things. In fact, it is not unusual for WinMagic to receive feedback from several of our corporate clients highlighting that they are the only one vendor which provides details on design, giving their customer base a warm feeling demonstrating that WinMagic security is sound, and not based on obscurity.

While some of the providers of data security software claim to support hardware tokens, WinMagic points out that:

- They have delivered integration with hardware token at pre-boot since 2000 and have been continually improving their software offering.
- In order to work with token at pre-boot, one has to have the technology to handle PC – hardware (e.g. USB controllers, PCMCIA controllers, PCI-bridge) and native low-level protocol to interface with smart card readers and smart card chip. This requires Non Disclosure and Confidentiality Agreements in addition to dedicated support from the vendors.
- Organizations now seeking to either enter into the marketplace or augment their current data security offerings would have to spend years developing these technologies, incur incredible resource expenditures on securing the required intellectual capital, and need to spend years nurturing the necessary partnerships with the token vendors.
- If competing organizations and vendors claim to provide integration with smart card “shortly”, then it is simply NOT TRUE.
- The only exception is Aladdin’s eToken. Aladdin develops its own 16-bit driver for its token to facilitate disk encryption vendors to interface with eToken at pre-boot. But Aladdin’s technology doesn’t match WinMagic’s capability (supports less PCs, cannot deal with certain USB controllers and hubs, and does not support PKI capability).

Flash cards, SD Cards, Multimedia Cards, Micro Drives, and other removable media are encrypted automatically. Removable media can be transferred to other PDA's and accessed through the SecureDoc PDA user's key, protecting a user's vital information from unauthorized access.

## Corporate Profile

WinMagic Inc. develops disk encryption software. Its SecureDoc line of products ensures 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. WinMagic's award winning products fulfill the requirements of even the most security conscious users by focusing on concrete security features, nevertheless still offering unparalleled flexibility. Utilizing Public Key Cryptographic Standards PKCS-11 from 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 by Q1 2007.

WinMagic Inc. is a Canadian company based out of Mississauga, Ontario. For more information concerning its products or services, please visit [www.WinMagic.com](http://www.WinMagic.com) or call 1-888-879-5879, or email [info@WinMagic.com](mailto:info@WinMagic.com).

## Mission Statement

As a thought leader and innovator, WinMagic's mission is to become the world leader in full disk encryption through high standards, strong ethics, and strict adherence to policies relating to privacy and security.

## Company Background

Our headquarters are located in Mississauga, ON (Toronto) Canada. WinMagic commenced operations in 1997, and is now operating through direct or indirect channel support in over 43 countries.

## References

Please refer to Appendix B.

## The Need for Full Disk Encryption

Protecting data has become increasingly important for companies, as laws enforcing consumer privacy have come into effect across the globe. These laws are placing companies accountable for their customers' information. Companies need to guard their customers' personal information to avoid lawsuits and public embarrassment.

Companies are scrambling to install firewalls, virtual private networks, and endless security patches to protect their sensitive data from being stolen and destroyed. Organizations now need to disclose why they are collecting data, where is it being stored, who has access to the data, what the data will be used for, and what measures are being taken to secure the data from a physical prospective as well as from a technology prospective. With over 70% of 300 Canadian businesses surveyed reporting computer security breaches, with 32 companies reporting losses exceeding \$1 million<sup>1</sup>.

In 2005, according to the Computer Security Institute (CSI) 56% of the companies surveyed reported at least one successful security breach in the past year, with 9% of the respondents reporting over 10 security penetrations. CSI also reported the same amount of internal security breaches as external ones.<sup>2</sup>

Information protection typically surrounds concerns relating to connectivity and IT architecture measures relating to the transferring of data from one node to another, leaving critical information residing in a static format on the hard drive vulnerable. Consequently if a PC falls into the wrong hands or if data rich workstations and servers are sold as old assets, the data initially protected by firewalls, virtual private networks, Windows NT access control, etc., is now left vulnerable to unauthorized users who can view this digital information. We only need to refer to recent incidences of security breaches with organizations in market segments like banking, finance, insurance, and government agencies – to name a few – to become aware of the legal and financial repercussions in inadvertently allowing confidential, sensitive, and personal information to become available to unintended or unauthorized individuals.

CardSystems has been named in a class action suit as well after failing to maintain adequate data security, that lead to a security breach leaving over 40 million credit card holders accessible to fraud. In these cases, securing the retail transactions is of equal and paramount concern to securing the medium carrying and storing card holder credit and financial information.

In 2005, there was a significant increase in stolen information. This string of exposed customer information has prompted companies to start encrypting their data.

In one recent example, CitiFinancial blamed UPS for losing data tapes with personal data for 3.9 million people, intends to start encrypting backup data in June 2005.

In another recent example, the Bank of America's admission in February 2005 that the company lost data tapes containing federal workers' customer and account information brought issues relating to data security to the foreground.

"Very few people encrypt backup tapes, which means that they rely on the security of the backup and off-site rotation process," said Jon Oltsik, senior analyst for information security at Enterprise Strategy Group. "Here's a clear example of the risks of doing this."<sup>3</sup>

---

<sup>1</sup> The Ernst & Young *Global Information Security Survey 2004* questioned 1,233 leading organizations in 51 countries. Its conclusions were made public in September 2004. For more information, please refer to [http://www.ey.com/global/content.nsf/Canada/Media\\_-\\_2004\\_-\\_Global\\_Information\\_Security\\_Survey](http://www.ey.com/global/content.nsf/Canada/Media_-_2004_-_Global_Information_Security_Survey).

<sup>2</sup> "10th CSI/FBI Survey Shows Cybercrime Losses Down For Fourth Straight Year", Computer Security Institute. July 14, 2005. <http://www.gocsi.com/press/20050714.jhtml>

<sup>3</sup> "Bank's Tape Loss Puts Spotlight on Backup Practices" by Paul Shread. Internetnews.com: February 28, 2005.

"Bank of America is eliminating backup tapes where possible, and transitioning to computer-to-computer data transfer", Representative Betty Riess says. "Since the third quarter of last year, all of BofA's data exchanges with credit bureaus have been encrypted. The bank, which lost data tapes for 1.2 million federal employees — including U.S. senators — in February, is testing encryption on backup tapes", Riess says.<sup>4</sup>

Incredibly in another example, shortly after it lost track of Social Security numbers and other data for 600,000 current and former U.S. employees in May 2005, Time Warner decided to begin encrypting backup tapes.<sup>5</sup>

If security on a laptop were limited only to windows password protection rather than encryption, achieving access to data on a disk would be as simple as removing a hard drive from a computer and connecting it to another computer to read all the files.

In addition, with the use of a low-level disk editor, an attacker can gain access to raw data on a hard disk bypassing all access control set up by the operating system, along with other access control management software. ATA-3 type or later hard drives can be protected by a hard disk password, but are also assessable directly by an attacker, reading the disk media directly using forensic data recovery techniques.

An attacker can use [forensic data recovery techniques](#) to read [deleted magnetically stored data](#) on a disk through its drive controller connector. Using PC-hosted software, through its drive heads bypassing the disk's controller circuits, or by directly reading the disk platter's recording surface in a clean room. To wipe away data from a disk therefore making it unrecoverable through forensic data recovery techniques, one must use [Clearing per DOD 5220.22-M](#).

Unless vendors take extensive measures to guard against theft, the most sensitive data on a security system such as the private key can be written onto the disk. This would typically happen when the memory containing the keys is paged out to disk by the operating system. Therefore, security measures would be rendered useless if the platforms, on which the program operates, were compromised. Public Key Infrastructure, Virtual Private Network, and Electronic Commerce are all vulnerable if the laptop is compromised.

The FBI reports more than 1 million laptops are stolen each year in the United States, with more than 98% of laptops never being recovered. The 2005 CSI Survey reported 56% of all respondents reported a financial loss from theft and security breaches. Out of 56% of 639 respondents stated \$131,104,542 in total losses.

While the above numbers are startling, there have only been diminutive attempts to date to quantify the dollar losses as a result of information theft from these missing computers. It becomes apparent the need for security beyond the boundaries of the network increases daily. As an ever-increasing proportion of the workforce (teleworkers, sales forces, etc.) becomes wired, the volume of information subject to the above mentioned risks increases as more and more companies become totally dependant on digital information.

Being protected against malicious attacks and computer / laptop theft requires solid encryption. Encryption allows for an effortless and cost effective solution to protect sensitive files, applications, residual information, and even the operating system.

---

<sup>4</sup> "Data losses push businesses to encrypt backup tapes" by Jon Swartz, USA TODAY: June 13, 2005.

<sup>5</sup> "Time Warner employee data missing: Information on 600,000 current, ex-workers lost by storage firm; Secret Service investigating." by Caleb Silver. CNN: May 3, 2005.

## Common Desktop Security Software Problems

The following are problems, which are not covered when using most desktop security software.

### Temporary Files

Commercial software packages create temporary files to store data while a file is open, often to store a copy of the original in the event of unanticipated shutdowns. It is difficult to find a word processor, spreadsheet, database, or other business application that does not make extensive use of temporary files. While these files are extremely useful, the files also pose a security risk if not encrypted when created.

### Paging Files

Paging files (also called “swap files” in Windows 95) are used extensively in modern operating systems. The operating system appears to have limitless memory resources available for software applications. The purpose of paging files is when memory resources run low, it automatically writes data onto the hard disk into the paging files. As soon as the application is needed again, the operating system copies the data back into memory, and places another applications’ data in storage. The operating system puts everything onto the hard disk, including plain text copies of sensitive data is supposedly secure.

### File Slack

Windows file systems arrange data in clusters, which are made up of one or more (up to 64) sectors. A file might only be a few bytes long; nevertheless, it will occupy a whole cluster. Alternatively, a file can be long but it might occupy only a few bytes in the last cluster of several thousand bytes. Thus, the last sector of a file contains random data collected from RAM at the time the file is saved, which can contain passwords, and private keys.

The last cluster of a file can contain very sensitive data, including random data from RAM in the last sector of the file, and data from files such as email messages and word processing documents that were previously stored in the remaining sectors left in the cluster. File slack can be a severe security risk, allowing sensitive information to be recovered by forensic data recovery techniques.

### The Recycle Bin

Another place where data can reside is in the “Recycle Bin”. When a file is deleted, Windows removes it and places it in the recycle bin. Until the recycle bin is emptied, the user can still retrieve the file. However, when the recycle bin is emptied and Windows shows the file no longer exists, the physical data still remains on the disk. The deleted information can easily be found with inexpensive utility software, and will remain on the hard disk until it happens to be overwritten by new data.

### The Windows Registry

Microsoft Windows and most application software, store various data in the Windows registry. A web browser might save the domain name of the sites you visited in the Windows registry. Even word processing software might save the name of the file you last edited to the registry. Windows itself needs the registry to know the configuration of how to start up; therefore if an encryption method starts after Windows, then these files will not be encrypted.

### The Windows NT File System (NTFS)

It is often assumed a file system with built-in access control (such as Windows NT) is secure. The fact users must enter a password to access their personal files leaves many people with the mistaken impression their files and data are protected. However, even a file system with built-in Access Control List (ACL) security, such as the NT file System (NTFS), provides no protection against an attacker with either physical access to the disk, or administrator privileges on the local machine (which is a very common configuration). Both of these avenues are available (a thief would have both), and an attacker can simply read the raw data from the disk and then freely use available and inexpensive disk editors to locate and read the plain text of any document desired.

**Hibernation and Sleep Mode**

Hibernation or Sleep Mode is often found on laptop computers. It is a feature designed to conserve battery power when a computer is powered on, but not in use. When a notebook computer goes into hibernation mode, it saves all its RAM memory data to the hard disk. By allowing the PC to re-create the exact state of the computer from before, it entered hibernation mode. Of course, all data in memory at one time, for instance program files and sensitive data is stored on the disk.

**Hidden Partitions**

A hidden partition is a portion of the hard disk an operating system, such as Windows, does not recognize or display a file system for. Software applications sometimes use these hidden partitions to save data. For example, some hibernation mode software continually saves data on a hidden partition instead of in a file on a visible partition. This quiet action can create blocks of information in plain text for which there is no security at all.

**Free Space and Space between Partitions**

Sectors at the end of the disk do not belong to any partitions may be displayed as free space. Other unused sectors are found between partitions and extended partition tables. Unfortunately, some applications and virus software use this free space to store programs and data. Even when a disk is formatted, this free space remains unaffected, and the information can be recovered.

**Summary**

There are many software security issues, which can be resolved by encryption software, but not all encryption methods are equal. Different encryption methods and encryption software have various strengths and weaknesses, [some encryption software may lack secure data protection](#). Each encryption method is explained below outlining the common concerns related to it.

## Analysis of the Different Encryption Methods

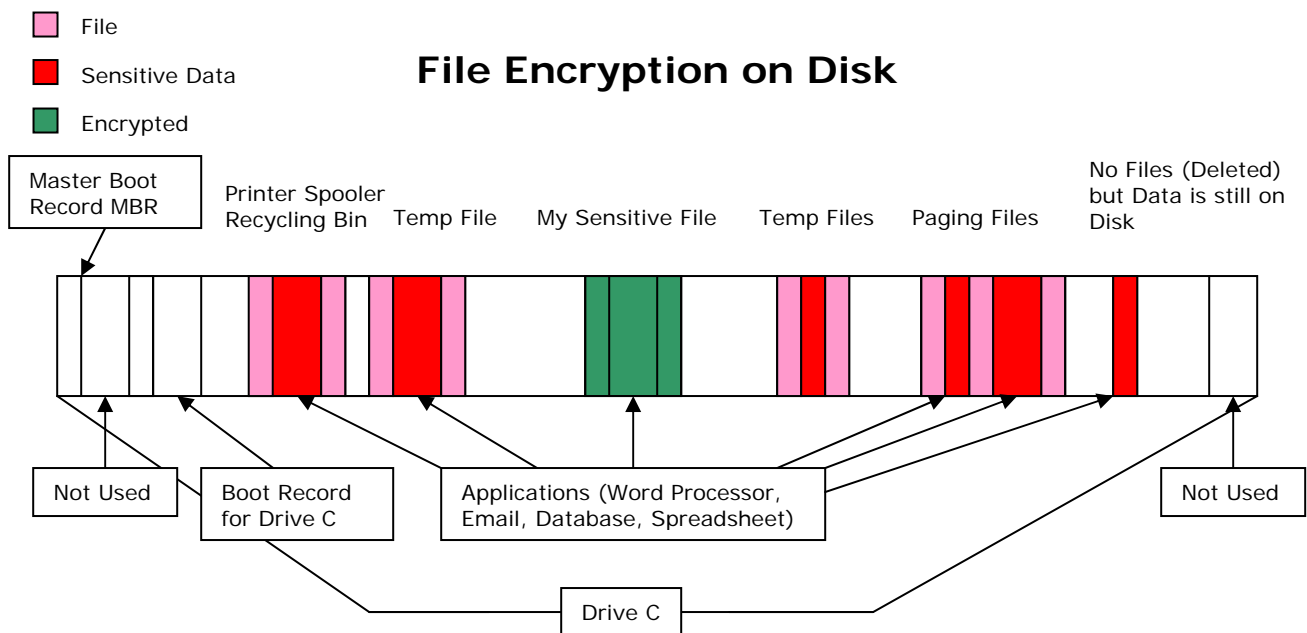
### Manual File Encryption

File Encryption is used primarily to send files over email and across the Internet. A user manually encrypts files he/she needs to encrypt to protect them from being examined by unauthorized users.

However, this method is slow, especially when it involves a large amount of data to process, as is the case with spreadsheets or databases. Manual File Encryption has serious limitations as a viable data security method for most organizations since it encrypts only the original file; temporary and paging files are not secured, and remain in plain text. Furthermore, of concern is the lack of transparency, meaning a user must manually encrypt or decrypt the file. This leaves plenty of room for human error, for example, if a user forgets to encrypt a file, thereby leaving it vulnerable.

*FILE ENCRYPTION DOES NOT PROTECT TEMPORARY FILES. IT'S LIKE LOCKING THE OFFICE DOORS BUT LEAVING THE WINDOWS OPEN.*

Therefore, Manual File Encryption software may be acceptable for sending a file from computer to computer as e-mail or attachments, but it cannot protect storage data efficiently or completely.

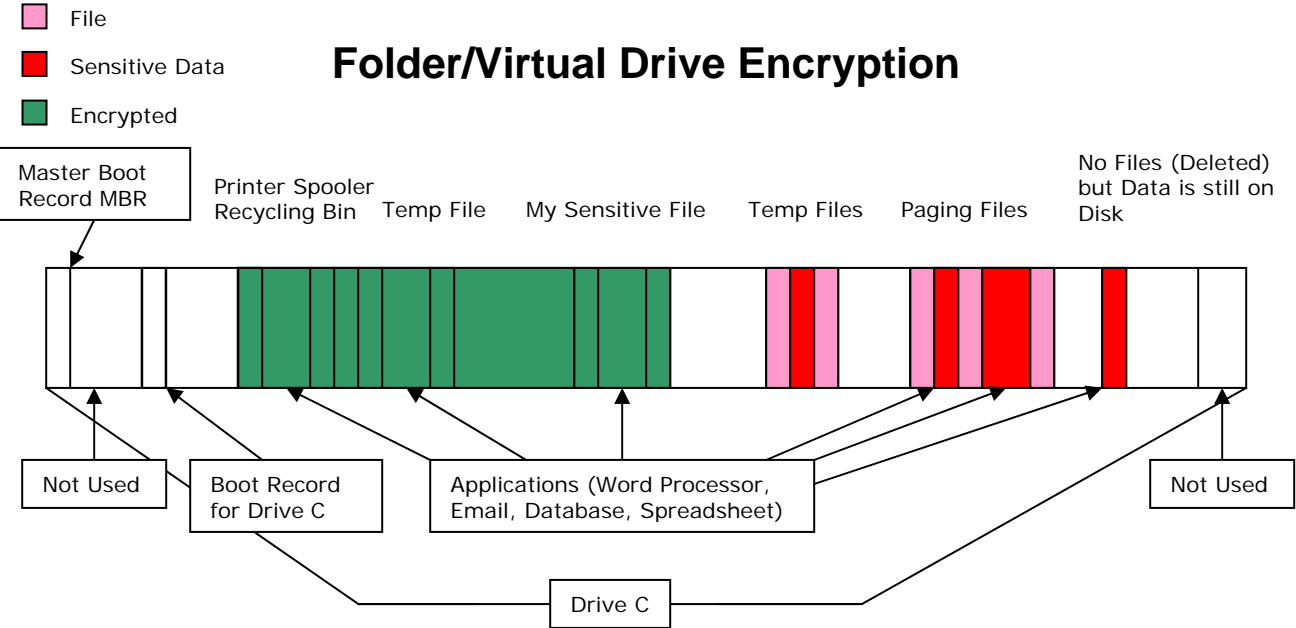


**As you can see, encrypting the file "My Sensitive File" will not encrypt the same sensitive data scattered all around the disk.**

**Folder Encryption**

Unlike File Encryption, Folder Encryption allows a user to move files into a specified folder to be encrypted automatically. This allows Folder encryption to be seamless compared to Manual File Encryption, but needs greater intervention with the operating system.

In addition, Folder Encryption products do not offer thorough protection for temporary files, paging files, deleted files, hidden partitions, or free hard drive space.



**As you can see, encrypting the file "My Sensitive File" will not encrypt the same sensitive data scattered all around the disk.**

*FOLDER ENCRYPTION IS NORMALLY NOT ECONOMICAL WITH CPU AND DISK RESOURCES*

The overhead power required by the CPU to check file access and the memory demands on the disk itself (more than 2KB per file for some products) make Folder Encryption very cumbersome and slow to use.

In short, although Folder Encryption can protect your files transparently, it is a time consuming, resource demanding method for protecting data, in the company of a lack of protection for paging files and temporary files.

**Virtual Drive/Disk Encryption**

The Virtual Drive/Disk Encryption method creates a large hidden file, which it then organizes and presents to the Windows operating system as a usable logical drive. Software can then be placed on the virtual drive, where it can be compressed to save disk space.

Several encryption software packages use virtual drives to secure information. Users specify a file is then opened as a useable drive eases the need to partition a hard disk. All information is placed on the virtual disk, where it is encrypted.

However, Virtual Drive encryption has several disadvantages. For instance:

- It provides the same features and functionality as disk encryption, but uses substantially more overhead. Whenever the disk accesses the virtual drives it must be redirected to another physical file, thus slowing down system performance.
- The operating system does not recognize a virtual drive as an actual physical disk. As a result, the operating system refuses to create temporary or paging files on a virtual drive.
- Compared to folder encryption, virtual drive has advantages and drawbacks. As opposed to folder encryption, virtual drive encryption protects file names stored in its virtual partitions. However, as a partition, virtual drive cannot be expanded as a folder, making it less elegant and attractive than a folder encryption.
- By far the largest drawback, Virtual Drive encryption suffers the weaknesses of folder encryption. It cannot thoroughly protect the security holes mentioned above such as the Temporary & Paging files

The fact that the virtual drive is in reality a file also makes it vulnerable to accidental or malicious deletion by applications.

**Disk Encryption**

The greatest difference between sector-based disk encryption software and the previous two methods of desktop security is disk encryption is volume-based (volume = drive), not file-based. In other words, every file saved on the hard disk will be encrypted. Disk encryption software transparently encrypts the data before writing it onto the disk.

The point where data is intercepted and encrypted or decrypted is an important consideration. Operating systems normally use one specific point to access the disk at the sector level. This means Disk Encryption products can easily capture and encrypt all information (including temporary, paging, and recycled files), a difficult task for the competition.

A common misconception is a system is much slower with encryption than without encryption. With the improved computing performance and intelligent disk caching features of newer operating systems, speed becomes a non-issue for disk encryption products. A WinStone benchmark of 3% reduction in system speed means the reduced performance is unnoticeable to the naked eye in all but the most unusual of circumstances.

The purpose of Disk Encryption is to make sure sensitive data is never written in clear text on a disk.

**Boot Protection**

Boot logon secures full disk encryption by authenticating a user before DOS or Windows even boots. This provides greater protection to disk data, by encrypting the operating system as well, so an attacker cannot bypass Windows Login Authentication because the attacker will wind up retrieving only encrypted information.

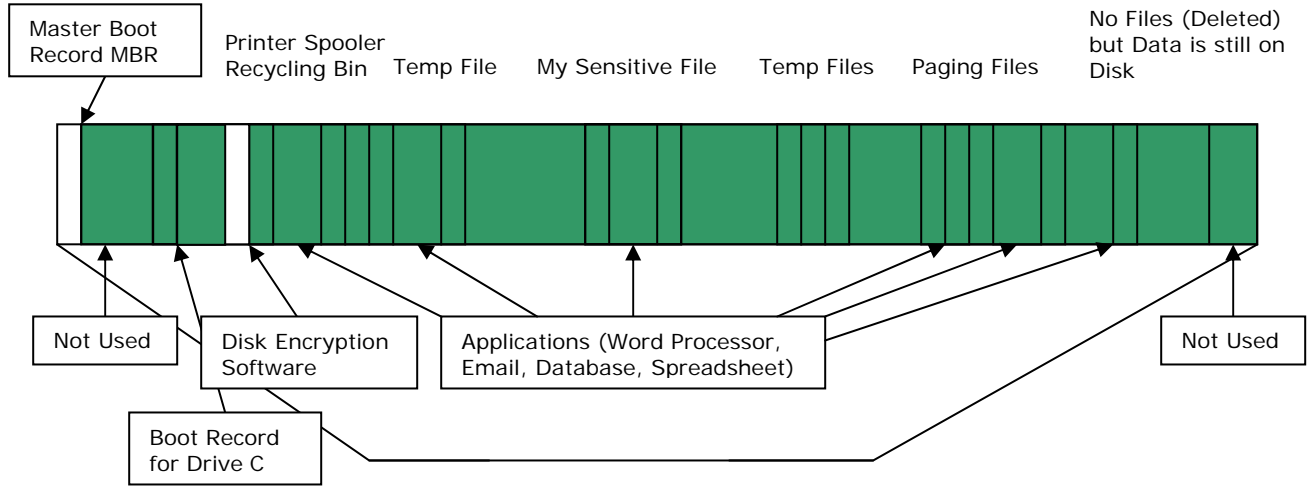
Please note if a disk encryption package does not use a boot logon before the computer starts, it does not fully encrypt the entire hard disk. In this case, the software does not encrypt Windows boot and system files. Therefore disk encryption software without boot logon is not recommended.

**Full Disk Encryption: The Logical Choice**

Since Disk Encryption software does not consider files individually, all data on the disk is encrypted. This includes temporary files, database files, executable files and documents. It requires the least memory overhead on a disk (less than file and folder methods), and CPU usage is extremely economical. The reason disk encryption is superior in this area is because the necessary information must be extracted to perform decryption only needs to be retrieved once for an entire encrypted hard drive. Although, File and Folder Encryption methods, however, must extract unique encryption key information and calculate the session key before decrypting the data for each file or folder.

- File
- Sensitive Data
- Encrypted

## Disk Encryption



**Note that Disk Encryption encrypts the entire disk including the un-used space before the partition C and after it. (Encrypting only drive C may leave attacker code in these spaces).**

## SecureDoc™

SecureDoc is a commercially available full disk encryption software application that been specifically designed to run transparently with Windows 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, FIPS 140-2 Level 1 & 2, and SecureDoc's FORTEZZA-based version is the ONLY disk encryption software certified by the US National Security Agency to safeguard US government SECRET information.

### 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.

## 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](#).

## 22 Unique Features of SecureDoc

The following list describes 21 features that distinguish WinMagic's SecureDoc from its competition.

### Centralized Management

- Enterprise class DBMS
- Unlimited Profiles

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.

### Communication with Client PC's

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

### 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.

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

SecureDoc works with VMWare "out of the box".

### Supports Hibernation Mode Supports removable media

SecureDoc protects data in hibernation mode. 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. 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.

**Magneto Drive Support****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.

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

**Compartmental Encryption Version**

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.

**Robust encryption**

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.

**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.

## Certifications

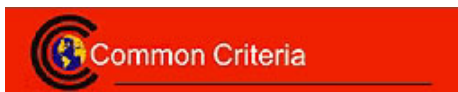
To determine whether a security product does as its vendor claims, a purchaser has three options: trust the vendor, test the product, and/or rely on an impartial third party with the experience and knowledge to evaluate the product. WinMagic believes in peer review as well as formal validation by third parties and has made SecureDoc source code available to several credible third party validation bodies.

- a) Source code validation is the only way to verify that a product does not have (vendor) back doors. Bruce Schneier, world-renowned crypto-analyst and creator of the BlowFish and TwoFish algorithms (a final AES candidate) has reviewed and crypto-analyzed SecureDoc source code. Bruce has verified the strength of SecureDoc's construction, and testified that there are no security holes.

*"SecureDoc's sector based encryption is smart. It sits at the lowest level and intercepts all requests to read and write to the disk, so the entire disk is encrypted and no sectors are missed. With strong, trusted encryption algorithms, SecureDoc has a clean design."*

Bruce Schneier, world renowned cryptographer, author of "Applied Cryptography", and president of Counterpane Systems.

- b) SecureDoc has undergone strict tests required by the Common Criteria Evaluation and Certification Scheme for security software. These standards are recognized and endorsed by 13 countries, including the United States, U.K., Germany, and Canada. All testing takes place in high-quality, controlled facilities accredited to ISO/IEC Guide 25 specifications (guidelines for the testing IT security products and systems). The results of the evaluation are that SecureDoc 2.0 is a secure product that in fact has all of the security features and strengths as laid out in its documentation. In addition, SecureDoc is one of the very few disk encryption products, if any, to receive Cryptographic module Validation Certificates for DES and triple DES from the National Institute of Standards and Technology (NIST).



- c) SecureDoc cryptographic engine has achieved FIPS 140-2 level 2 validation from NIST/CSE (March 2002). The United States Congress requires the entire Federal government,

including federal contractors, to use FIPS 140-1 certified cryptographic devices when they exist. SecureDoc, with an even higher level 2 validation, satisfies this requirement for a broad class of government security implementations.

While most software products can only achieve a level 1 validation, WinMagic's SecureDoc has achieved a level 2 validation.

This achievement underscores a trusted platform not only for the government but also for any enterprise that wishes to protect its sensitive data on laptop and desktop PCs.

SecureDoc is a pre-qualified IT security product for Canadian Government agencies, see the CSE pre-qualified product.

The FORTEZZA version is the only one disk encryption certified by the NSA for SECRET data for US Government agencies, see NSA certification.

In summary, SecureDoc's encryption offers more security and adaptability. SecureDoc disk encryption is based on PKCS#11 standards from the ground up, employs state-of-the-art encryption concepts

and possesses the unique centralized key management without the vulnerability of a “Master password”.



- d) SecureDoc has been CESG Assisted Product Scheme (CAPS) certified, WinMagic's hard disk encryption product. This follows an extensive evaluation by CESG, the United Kingdom National Technical Authority for Information Security.

CAPS was introduced to meet the increasing HMG demand for cryptographic products. It formalizes and enhances the services that CESG has provided over a number of years, and which have already provided a wide range of Commercial-Off-The-Shelf (COTS) products currently used by HMG.

Products developed under CAPS can address all HMG cryptographic requirements with the exception of the most highly sensitive security needs, which are outside the scope of this scheme.

CAPS enables products to be cryptographically verified by CESG to HMG cryptographic standards and formally approved for use by HMG and other appropriate organizations. For HMG customers, CAPS provides assured solutions: for CAPS subscribers it provides enhanced opportunities to market their products to government.

CAPS helps private sector companies to develop cryptographic products for use by HMG and other appropriate organizations.

CAPS is a subscription scheme for companies interested in commercial risk developments for the UK government market. An annual subscription gives companies access to CESG's knowledge, skills and experience in the field of Infosec, supplemented by a range of guidance documentation. As subscribers to the Scheme, members may incorporate appropriate CESG cryptographic or public domain algorithms in their products and submit them for evaluation by CESG. When approved, these products may be advertised as suitable for purchase by HM Government (HMG) as well as the UK public sector.



- e) WinMagic Inc. has completed the certification process with the department of defense for the CAC card interoperability with its SecureDoc hard disk encryption software. Products sent to be certified by the DoD must be enabled to take advantage of the services a PKI offers. Without enabled applications, the infrastructure holds little value. It is essential that applications become enabled and utilize the infrastructure. However, enabling is a complicated task. SecureDoc has been evaluated to ensure it is enabled correctly and securely, and is interoperable with the DOD PKI.

DoD Joint Interoperability Test Command (JITC) has completed testing this new product for interoperability with the DoD PKI, which provides certificates validation including CA signature check, revocation check through CRL or OCSP and other DoD requirements.

[View SecureDoc evaluation certificate issued by Department of Defense](#)

The DoD CAC Card integrated with SecureDoc disk encryption software permits only authorized users to boot up their PCs or notebook computers authenticating and authorizing users for secure access to their encryption hard drives. This provides an added measure of security, especially for mobile workers who have a higher risk of having their notebooks lost or stolen.



The Government of Canada's Communication Security Establishment (CSE) tested SecureDoc in its IT Security for Telework project. The report's conclusion was only Disk Encryption (as offered by SecureDoc) provides effective protection for data on a hard disk.

The National Security Agency (NSA) of the U.S. Government currently uses a slightly modified version of SecureDoc. This organization includes some of the best cryptographers in the world and is intent on providing the best security to its government and military. WinMagic believes it is a testimonial to our product excellence, that a high profile security agency like the NSA uses our software.

SecureDoc is the only software available on the market that not only protects the temporary files and paging files but also offers sophisticated key management and standards compliance.

## 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 3<sup>rd</sup> 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. Some of our competitors have been benchmarked to take over twice the amount of time to encrypt a hard drive.

## Authentication

### PreBoot Authentication

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.

### Support for 2-factor Authentication

This feature provides full disk encryption to protect sensitive information stored on laptops, desktops and PDAs. By offering integration with popular tokens and PKI at PreBoot time (after bios POST but before the OS loads) with dual and triple factor authentication (password/token/biometrics/TPM) SecureDoc provides the ultimate security and flexibility in data protection.

### Password Lockout

Yes, this can be achieved and managed by the administrator.

### Password Recovery Method

We have a four password recovery methods:

- 1) Hint
- 2) Self Help
- 3) Online Password Recovery
- 4) Admin/User Challenge Question

### Does it work for users not on a network?

Yes it does. The first two are available locally. For Online Password Recovery the user may communicate with the helpdesk by phone.

### Reset mediated by helpdesk?

Yes this can be achieved, through the Online Password Recovery mechanism that generate one-time password for the user and enforce him/her to change their password once logged in.

### What methods are available to allow users to access encrypted data (certificates, passwords, tokens, etc)?

SecureDoc is the only disk encryption product based on PKCS#11 Standard (industry standards for API between applications and "token" or cryptographic engine module) from the ground up – even between internal components. This foundation has enabled WinMagic to deliver SecureDoc based on the FORTEZZA card to the NSA within 6 months (which garnered the certification to protect SECRET data for the US government, the only one in the world) and support AES algorithm very early on (in 2000).

While some of our competitors claim to support hardware tokens, we should point out that:

- We have delivered integration with hardware tokens at pre-boot since 2000 and are continually expanding our software support capabilities;
- To work with token at pre-boot one has to have the technology to:
  - a) handle PC – hardware (e.g. USB controllers, PCMCIA controllers, PCI-bridge)
  - b) native low-level protocol to interface with smart card readers and smart card chip. This requires NDAs, support and working closely with our vendors.
- Our competitors would have to spend several years to develop these technologies and the partnership with the token vendors.
- If they claim they can provide integration with smart card "shortly", then it is simply NOT TRUE.
- The only exception is Aladdin's eToken. Aladdin develops its own 16-bit driver for its token to facilitate disk encryption vendors to interface with eToken at pre-boot. But Aladdin's technology

doesn't match WinMagic's capability (supports less PCs, cannot deal with certain USB controllers and hubs, and does not support PKI capability).

- SecureDoc utilizes X.509 certificates for user authentication. We can work both with certificates on token and in the form of PKCS#12 or PKCS#7 files. As an additional factor of authentication SecureDoc includes an option of certificate validation at the time user logs into Windows. The certificate can be verified on-line at Certification Authority (CA) via Certificate Revocation List or Online Certificate Status Protocol

#### **List supported authentication tokens?**

WinMagic is the leader in MFA – multifactor authentication at boot logon. We support virtually all of industry standard tokens both Smart Card and USB. For complete list, please see:

[http://www.winmagic.com/partners/tech\\_partners.asp](http://www.winmagic.com/partners/tech_partners.asp).

We also support biometrics (at boot logon), the Sony FIU-810 Puppy® Fingerprint Identity Token and the Precise Biometrics 250/200 MC Readers working with DataKey SmartCard 330M G3. Again, we are the only vendor to support RSA's SecurID 800 Combination Token.

#### **For the supported operating systems define the authentication mechanism implemented.**

SecureDoc V4.x supports Windows 2000/XP/2003. Future versions will also support Linux. SecureDoc supports FAT16, FAT32, NTFS and NTFS5 file systems for hard disk. This product works on servers, desktops and laptops. SecureDoc PDA works with Pocket PC 2003 under Windows CE. Authentication is handled using our Boot Login process, which is identical regardless of Operating System.

#### **Does the encryption system allow for "password hints" to allow for user recreation of encryption keys?**

SecureDoc offer numerous key recovery methods thereby allowing both safe and secure recoveries. As simple as offering a "hint" to One Time Recovery through a help desk, or .net environment as well as our preferred method being Self Help Recovery. From our prospective, the Master Key is not even an alternative - if a Master Key is ever compromised, the entire computer community is vulnerable, something that our company will not support. SecureDoc also offers Admin Keys upon demand to allow access to a computer should the requirement arise.

## Certificates

### Security Certifications FIPS (\*2), CC (\*3)

WinMagic's products are certified for FIPS 140-1 Level 2, FIPS 140-2 Level 1 & 2, Cert # 698 & 699, Common Criteria, NSIT Cryptographic Module Validation Program (CMVP) for: AES Cert #1, SHA-1 Cert # 76, 3DES Cert # 7 & 9, DES Cert # 85 & 87, CAPS (for use by HMG), and DoD Joint Interoperability Test Command (JITC) for DoD CAC integration.?

<http://csrc.nist.gov/cryptval/140-1/140crt/140crt698.pdf>

<http://csrc.nist.gov/cryptval/140-1/140crt/140crt699.pdf>

DoD PKI Interoperability

<http://www.WinMagic.com/downloads/dodvalidation.pdf>

Common Criteria EAL-1. Currently the product is undergoing evaluation for Common Criteria EAL-4:

<http://www.cse-cst.gc.ca/services/common-criteria/ongoing-evals-e.html>

### Strong standards-based encryption (\*4)

SecureDoc addresses the needs of an organization's increasingly mobile workforce, with more and more data to protect than ever. SecureDoc offers strong encryption through the 256-bit AES encryption algorithm. The encryption process takes place transparently in the background, invisible to users.

SecureDoc implementation of the cryptographic algorithms was certified by NIST:

Algorithm	Cryptographic Function	Modes / Mechanisms	Key Size (bits)	Certificate #
AES	Encipherment	ECB, CBC	256	359
SHA	Hashing	SHA-1, 256, 384, 512		434
HMAC	Message authentication	SHA-1, 256, 384, 512	256	158
PRNG	Random number generation	ANSI X9.31 AES	256	172

### Does your product use a central Certificate Authority (CA), is this required, and is it compatible with Microsoft's CA?

SecureDoc does not use its own CA, but it can use any standard X.509 PKI certificates. SecureDoc supports token-based protection at pre-boot, and will use certificates from an existing PKI database.

**How can the data recovery agents be assigned?**

Computers managed by SecureDoc Enterprise Server (SES), have one-time remote challenge-response password reset capabilities in addition to the usual password hint, self-help password recovery and the ability to support unlimited users for a computer – and with that, unlimited passwords.

**Can your product store certificates on smartcard based storage?**

SecureDoc can store and use existing user certificates on smartcards, at pre-boot time.

## Compatibility

### Compatible with Motion Tablet PC?

Yes, WinMagic has tested our product on the LE 1600, LE 1400, and the LS 800 models.

### Do you offer a PDA Version?

Yes, WinMagic has a PDA version known as SecureDoc Mobile. Current Version is 1.2

### Do you support Hibernation?

Yes, our product supports Hibernation

### Is there a self-service recovery mode?

SecureDoc has the ability to use a self-service recovery mode. The administrator is capable of creating the questions if need be. The user will then be forced to answer a pre-configured number of questions to login into the system.

### Must support single-sign on with support for standard operating system calls?

SecureDoc disk filter driver is incorporated into the Windows kernel and works transparently for the user. SecureDoc also supports a single-sign-on possibility, Windows password synchronization, and Windows GINA integration. The product interoperates with Windows OS loader and allows having multi-OS configuration on the condition that each OS instance has SecureDoc installed.

### Must have full interoperability with other workstation security software, such as anti-virus, Cisco VPN client, and personal firewall software (Zone Labs Integrity Desktop Client)?

The user can install (Microsoft) Service Packs on a hard-drive that was encrypted by SecureDoc™. With most of our competitors' products, it is necessary to first decrypt the hard-drive, install the Service Pack and then re-encrypt the hard-drive. With SecureDoc the user can leave the hard-drive encrypted while installing the Service Pack. SecureDoc is fully interoperable with any other program such as anti-virus, software, VPN clients, and firewalls. Most of the competitors' products cannot encrypt the hard-drive while these types of programs are running. With SecureDoc™, there is no problem having these programs running while encrypting the hard-drive.

### Must recognize dual-boot and multiple operating systems and take appropriate action including notification.

Note that SD support multi-boot, and in a clean way. Some products don't do it cleanly by changing its executable software – e.g. the kernel driver -, which is not the best practice!

## Deployment

### Remote Deployment?

This is deployed by SecureDoc Enterprise Server (SES) that supports various file distribution software, such as Microsoft SMS, Tivoli, etc.

### Impact of Initial Install?

Initial conversion starts automatically once the user provided required information and pre-boot authentication is in place (requires reboot of the machine). The conversion is performed in the background which means that the user may continue to use the computer. Very few disk encryption products can tolerate interruption including shutdowns and power failure. SecureDoc has been tested to encrypt from the last known sector on the drive should an interruption occur.

### Describe the typical time needed to complete the initial encryption process.

SecureDoc is a fully transparent full disk encryption solution. The initial conversion to an encrypted computer takes place in the background. The user can work on the machine as normal. In day-to-day operations, the entire drive stays encrypted at all times. The process to install and encrypt the hard drive is contingent on the type of process and hard drive speed being used. A typical 80gig hard drive on a Pentium class machine takes between 2 – 3 for the drive to be fully encrypted.

### During the initial conversion process are power outages acceptable? Upon reboots does conversion complete normally?

SecureDoc's initial encryption speed, the ability to recover after any interruptions e.g. by power outage, and the ability to let user continue to work during the initial encryption are very good.

### Define the level of preparation that is required to perform the initial encryption. Does the system require special steps like de-fragmentation prior to installation?

SecureDoc can be installed and configured at any time. It is not necessary to have the computer in a particular state before installation.

### Does the software support the automatic deployment of patches and upgrades to the disk encryption software?

SecureDoc Enterprise Server contains a feature - AutoBoot that will allow unattended updates to be made to the selected users over the network. This feature permits the Admin to set either a set number of re-boots or conversely a time limit. Upon the conclusion of the updates the machine is places back under user control.

### Describe your initial deployment and installation process.

When installing SecureDoc, an administrator account is needed for installation and for access to the database used to store key information from SecureDoc. With the SecureDoc Enterprise Server, it is possible to create installation packages that can be used by the client machines for silent installs, where no user intervention is necessary.

If the client computer cannot run the setup file from a network folder, the initial Install packages are 7 MB long. Otherwise, the installation package can be stored on a network folder.

SecureDoc encrypts 30G per hour on a PC with 2G Pentium 4 – e.g. it therefore requires 2 hours for a 60G disk -. The initial encryption (conversion) runs in the background (user can continue to work) and tolerates interruptions (user can turn of the computer and the conversion will continue after re-start). If the computers do not contain existing sensitive data, SecureDoc can encrypt even faster, e.g. 15 minutes if the data occupies only 7G the 60G hard drive.

### What local discretionary controls are available to the user?

The administrator can set up the client packages with different control options such as administrative controls to encrypt/decrypt certain drives to no options where the user has no control over the options of SecureDoc.

## Directory Management

### **Does your product use Active Directory, if not what central user and group management tools are used?**

SecureDoc Enterprise Server (SES) uses LDAP to import existing user information from an existing Active Directory, Novell NDS, PKI, etc. SES synchronizes with these directories when new users are added, or existing user information is updated.

### **Is Active Directory used natively, or meta-directory or other directory used instead?**

SecureDoc uses LDAP to retrieve data, and uses native Active Directory API for the synchronization.

### **What rights are required for active directory for the following activities?**

- **Install the product.**
- **Manage the product.**
- **Device passwords reset/recovery.**
- **Add additional devices**
- **Sharing data with other AD users or groups.**
- **Root certificate recovery.**

Some administrative rights are required when setting up synchronization and data retrieval via LDAP.

### **Define the database requirements for the centralized key management server?**

Currently, we support the Microsoft SQL Server or MSDE SQL database engine for our SecureDoc Enterprise Server (SES). As mentioned; we will have full support the Oracle Database shortly.

### **Does the centralized key management console support roles associated with users and administrative staff?**

SecureDoc Enterprise Server (SES) provides a number such as Password Rules, length of passwords, the make-up of same, User Rights, how to deal with media such as memory sticks, pen drives etc. Number of password attempts can also be enforced. Also, the Admin has the ability to enable/disable the use of USB/FireWire, floppies, CD/DVD devices etc.

The rights of a regular user are defined by Authorization Vector (AV) and are kept encrypted and are not accessible in the user's key file. By default, these rights are limited to change the password and viewing (no modification) of available protection keys. No critical cryptographic or administrative operation is done under user privileges. Therefore there is no way a regular user might adjust the policy.

## Encryption

### Full Disk Encryption

WinMagic's SecureDoc hard disk 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.

### Folder or Partition Encryption

File and Folder Encryption tools are included as a component of the standard SecureDoc Disk Encryption product.

### Sector-based encryption / decrypt as used

Yes, WinMagic is capable of this feature.

### Follow-on: Conversion back to plaintext?

Yes, we can de-encrypt and en-encrypt back and forth. This operation is limited to authorized administrators only. Regular end-user cannot change encryption status of the machine.

### Corporate Data Access:

Data on the encrypted machine may be shared throughout the corporate network. Network protection though is out of scope of the product and therefore the data on the shared resources (Folder, Partitions) is seen in clear through the network.

### What encryption algorithms does your product support?

SecureDoc v4.x uses AES 256-bit will be supported.

### Does your product support content, device encryption, or virtual drive encryption?

SecureDoc full supports content and device encryption (including removable drives). Additionally, SecureDoc provides full configuration for removable media, e.g. preventing files from being copied to, from, etc.

Currently, SecureDoc does not support virtual drives. This feature has been implemented in the SecureDoc for PDA product; therefore virtual drives will be supported in the future.

### How are Windows system swap files and application temporary files protected against unauthorized access?

With SecureDoc, the entire hard-drive is encrypted, including swap/paging files, temporary files, spaces between sectors/partitions, etc. All these files are protected at all times.

### Define the level of encryption implemented (sector, block, byte)?

SecureDoc uses a low-level encryption approach. That means that it operates at sector level and so the whole hard drive is encrypted disregarding the content of the data. Therefore all the type of files mentioned above included OS itself is under protection.

### Can multiple partitions be encrypted separately?

Yes, different partitions can be encrypted by different keys – e.g. for selective sharing.

### Can the entire disk be encrypted?

Yes, note that SD encrypts the entire disks including the boot record itself (the first sector of a partition) and space between partitions. Network Computing review showed that among leading vendors only SecureDoc automatically encrypts new partitions when they are created.

## Hardware Support

### Support for multi-user workstations

SecureDoc unique key file concept provides powerful and flexible mechanism to support sharing computers among several users. The product allows both sharing encryption keys for common resources and keys separation to regulate access of different users to certain resources like partitions on the encrypted hard disk. Users sharing the same computer may have different sets of encryption keys that would enforce access control policies assigned to the computer protected by SecureDoc.

### Are there limitations in the size of partitions and the number of partitions that are supported?

Currently, we have not found any limits with SecureDoc. SecureDoc supports unlimited number of partitions, and uses 64 bit for sector numbers, meaning it supports disk size of more than 32 bit sector number (> 2 Terra bytes). Furthermore, individual partitions can be encrypted with different key, e.g. to regulate which users can access which partitions.

### Does the software allow for encryption of removable media? (USB drives, PCMCIA disks, ZIP, and memory sticks, SATA hard disks, CD-ROM)

SecureDoc full supports content and device encryption (including removable drives). Additionally, SecureDoc provides full configuration for removable media, e.g. preventing files from being copied to, from, etc.

### Does the software enforce encryption on a removable device? Can this be controlled with a centralized profile setting?

SecureDoc has offered removable media encryption since its inception in 1997. You can configure any partitions or removable media to be "not accessible; read-only; read access allowed, but write only if encrypted; read/write only if encrypted; full access. Etc...". Furthermore, user might only have the privilege to "select a disk access profile" set up by the administrator. Our removable media encryption encrypts the whole disk, not only certain files or folders. Further, you can configure SD to log which files user wrote to removable media. SecureDoc even supports MO (Magneto Optical) drives where sector size is e.g. 2048 instead of 512 bytes. And last but not least, SecureDoc key file concept allows flexible handling of key management for removable media: you can share a USB stick with yourself only, a group, a department or the whole company depending on how you configure it.

### Are PDA devices supported? If so list devices supported.

SecureDoc™ PDA utilizes the versatility and security of WinMagic's award-winning SecureDoc functionality, offering strong encryption through the AES 256-bit encryption algorithm. The encryption process takes place transparently in the background and protects mobile workforce PDA data. Currently, we support Pocket PC PDA's, Windows Mobile OS 5.x

## Management

### Centralized management console

Yes, our SecureDoc Enterprise Server (SES) is the administrative console that supports deployment of the product through the enterprise and then day to day maintenance and supervising of clients machines.

### Role-based policy enforcement

Yes, the administrator can set up the software to their own business security requirements. SecureDoc concept of rights and privileges allows the administrator to create different roles for various purposes of using the product.

### Follow-on: Uses AD (Active Directory) or own groups?

SES (SecureDoc Enterprise Server) support integration with MS AD and other LDAP servers or PKI. SES my import user's information stored in the Directory including personal data, certificates, etc. For MS AD real-time synchronization is available.

### How is policy distributed?

Policies distributed by SecureDoc Enterprise Server (SES) should be related to disk encryption and corresponding access control.

### Automated user key archiving:

Yes. SES centralized key management solution allows to keep all the keys (encrypted) in MS SQL backend database. The database can be backed up or replicated in the usual way.

### Separate Admin Key or Certificate:

Each user is issued a key file that contains encryption keys used by the user. The key file is protected either by strong password or token based on X.509 certificate.

### Audit – in management console

Yes, SecureDoc Control Centre incorporate Audit Console tab available for authorized administrators. It audits events such as:

- 1) All Authentication attempts at pre-boot and Windows
- 2) All Disk Integrity events at pre-boot and Windows
- 3) User actions within the SecureDoc in Windows
- 4) Administrator actions within the SecureDoc in Windows

The Audit Log is protected with a 256-bit HMAC to detect malicious modifications or removal.

### Audit integrated in Windows Event Log?

Yes, our product has this capability. All security related events are ported to the Windows Application Log and can be seen through MS Event Viewer.

### PBA events also logged?

Yes, SecureDoc auditing system starts working at pre-boot.

### Logs unsuccessful login attempts/Logs changes to security settings?

Yes our product can do this. Its sole purpose is an integrity check

## Recovery

### **What local discretionary controls are available to the user?**

The administrator can set up the client packages with different control options such as administrative controls to encrypt/decrypt certain drives to no options where the user has no control over the options of SecureDoc

### **What is the mechanism for supporting rescue disks during the installation process?**

The installation package has an option to create a rescue disk that can be used during an emergency.

### **What tools are available to recover data on an encrypted disk after either hardware or virus corruption?**

In order to recover data on an encrypted disk that is corrupted, the defective hard drive should be attached to another machine having SecureDoc installed. Once you gain access to the hard drive through a SecureDoc key file, it may be decrypted, repaired and encrypted again

### **Define the mechanism for recovering the data from an encrypted disk in the event of system corruption?**

In order to recover data on an encrypted disk it should be attached to another machine having SecureDoc installed. Once you gain access to the hard drive through a SecureDoc key file, you can decrypt the drive and copy the contents to another location.

### **Define the mechanism for accessing an encrypted disk if it is moved to another PC.**

Once the new drive is connected to another machine, you can gain access to the new drive if you provide it with the SecureDoc Key that was used to encrypt the drive. If you do not have the actual key, the Administrator can generate a new one that will allow access to the data.

## Appendix A: Glossary

Admin key file	A key file with full privileges for an encrypted computer, including the ability to create additional key files.
Algorithm	A detailed sequence of actions to perform some task (named Persian mathematician, Al-Khawarizmi). Technically, an algorithm reaches a result after a finite number of steps, thus ruling out brute search methods for certain problems. The term is also used loosely any sequence of actions which may or may not terminate.
Auto Login	SecureDoc function that requires users to log on to Boot Logon, after which SecureDoc automatically logs on to the SecureDoc Screen Lock and the Windows Login.
Boot #	Each key file enabled on an individual computer is assigned a number in Boot Control. This number can be used to select the key file to be used at Boot Logon.
Boot Logon	SecureDoc application that authenticates users to key files before giving them access to an encrypted computer. Also known as "pre-boot authentication prompt".
Challenge Question	An optional function that lets you define a series of "challenge" questions to help validate a user's identity. The user's correct answers must be stored in the SES database. For example, a challenge question might be "what is your favourite colour?" and user A's correct answer might be "red". If user A is asked that question and responds "blue", the administrator may choose to judge that the person's identity is in question.
Control Center	SecureDoc application used on client computers to perform SecureDoc management functions, such as changing a password.
Disk	A hard disk, floppy disk, zip disk, flash disk, and other removable or fixed media.
Disk access profile	Settings to control or monitor read/write access to both encrypted and non-encrypted disks.
Disk Integrity	The process that checks the computer's boot files to make sure they have not been tampered with, or corrupted, on boot-up. Depending on the user's privileges, the user may or may not be able to proceed if disk integrity is in doubt.
Emergency Disk	Used to restore Boot Logon on a client computer. This would be necessary if something happens to the computer's MBR and Boot Logon is missing, leaving the computer inaccessible. The "disk" can be any removable media: USB stick, CD, etc.
Encryption Key	The mechanism used to encrypt/decrypt a user's disks or removable media. Can act on a set of disks, a single partition, a single disk, etc. Can be assigned to different users in different

forms (e.g. to user A in a key file, to user B in a smart card, to user C in a USB device, and to user D in a key file protected by user D's Entrust profile). Must be stored in a key file.

GINA	Graphical Identification and Authentication. SecureDoc replaces Window's GINA with its own.
Key File	Contains the encryption keys, user privileges, password rules, and other information for a specific user. Can be stored on a token. Encrypted it and protected using a password or token.
MBR	Master Boot Record of a computer.
MachineInfo file	Contains data about the user and computer to be put in the SES database.
Password Hint	A hint to help the user recall their password. Should not contain the password itself, and should not contain enough information that someone other than the authorized user could guess. (For example, "name of your first pet".) This option is enabled and disabled in password rules.
Password Recovery	Process of enabling users with a lost or forgotten password to regain access to their PC. Once user is validated through answers to challenge questions, they are enabled to continue to boot and log on to Windows, but are immediately prompted to specify a new password.
Profile	In SecureDoc, an external file containing customization and other settings that can be imported by other SecureDoc users. See also disk access profile.
Protection Key	Key that identifies which administrators have administrative access to which encryption keys.
Screen Lock	SecureDoc function that uses a screen saver for added security. The screen saver requires users to log on to their key file or, for token-based key files, to insert their token, to continue working with the computer.
SecureDoc Control Center	SecureDoc application used on client computers to perform SecureDoc management functions, such as changing a password.
SecureDoc Logon	SecureDoc function that offers an alternative to using the Windows logon. The user logs on to Windows once after initializing this setting, but is subsequently required to log on to the SecureDoc Screen Lock with the key file information they entered at Boot Logon. Once the user has logged on, SecureDoc decrypts the file containing the Windows information and automatically log on to the Windows prompt with it. If the Windows information is correct, Windows starts to load.
Self-Help Password Recovery	Function that enables users to recover, without administrator help, from a lost password or token.

Strong Password

A password that is difficult for a person or program to guess. Passwords are made strong by being long (no shorter than eight characters) and including a mixture of alphabetic and numeric characters, mixing cases as desired. It is important to not have a password that corresponds to a recognizable word or phrase, particularly a user's name or login ID. The password also should be able to be remembered by the user, to avoid writing passwords down.

Token

In security terms, a physical device, such as a "smart card".

## Appendix B: References



Canadian Nuclear Safety Commission    Commission canadienne de sûreté nucléaire



Canadian Air Transport Security Authority    Administration canadienne de la sûreté du transport aérien



Canadian Space Agency    Agence spatiale canadienne



National Defence    Défense nationale



Environment Canada    Environnement Canada



Department of Justice Canada    Ministère de la Justice Canada



Health Canada    Santé Canada



Transport Canada    Transports Canada



Office of the Auditor General of Canada  
Bureau du vérificateur général du Canada



Royal Canadian Mounted Police    Gendarmerie royale du Canada



Bureau de la sécurité des transports du Canada    Transportation Safety Board of Canada



U.S. Department of Defense





**Knowing You're Protected**