



Encryption Solution for Data-at-Rest

May 3, 2007
WinMagic Inc.®



(This page left intentionally blank.)

Table of Contents

| | |
|---|-----------|
| 1.0 INTRODUCTION..... | 3 |
| 2.0 NEW CHALLENGES FOR BUSINESS | 4 |
| 3.0 ENCRYPTION METHODOLOGIES FOR DATA-AT-REST | 6 |
| 3.1 Full-Disk Encryption | 6 |
| 3.2 File and Folder Encryption..... | 7 |
| 3.3 Container Encryption..... | 8 |
| 3.4 The Role of File, Folder and Container Encryption | 8 |
| 3.5 DAR Requirements Summary | 9 |
| 4.0 CONSIDERATIONS IN CHOOSING A DAR ENCRYPTION SOLUTION | 10 |
| 5.0 INTRODUCTION TO SECURED OC..... | 13 |
| 5.1 Comprehensive Full-Disk Encryption | 13 |
| 5.2 Transparent Operation | 13 |
| 5.3 Support for File, Folder and Container Encryption..... | 14 |
| 5.4 Enterprise-Class Management..... | 15 |
| 5.5 Secure Information Sharing on Removable Media..... | 17 |
| 5.6 Dynamic Key Provisioning | 17 |
| 5.7 Committed to Standards..... | 17 |
| 5.8 Interoperability with Existing IT Infrastructure | 18 |
| 6.0 ABOUT WINMAGIC | 18 |
| 6.1 A Focus on Innovation | 19 |
| 7.0 CONCLUSION..... | 19 |
| 8.0 DISCLAIMER..... | 20 |

(This page left intentionally blank.)

1.0 Introduction

It is now generally accepted that data encryption is an important component of a comprehensive security strategy. It is the most effective technique for ensuring the confidentiality of sensitive or proprietary information.

Data encryption falls into 3 broad categories; data-in-transit, data-in-use, and data-at-rest. Encryption of 'data-in-transit' protects information as it moves from node to node across local networks, wireless networks and the internet. There are a number of widely adopted standards for this type of encryption, including SSL (Secure Sockets Layer), TLS (Transport Layer Security), and IPSec (Secure Internet Protocol). Encryption of data-in-transit prevents adversaries from intercepting or 'sniffing' sensitive data traffic as it transverses the network. It is also effective at preventing session hijacking and replay attacks.

'Data-in-use' refers to data being accessed or processed by applications or databases. Efforts to secure data-in-use include digital rights management (DRM) and content management / content filtering technologies. DRM prevents unauthorized access to files, databases, or specific records or fields within a database. Content management and content filtering technologies identify specific repositories of sensitive information and control access to and transfer of this information.

'Data-at-rest' ('DAR') refers to data in computer storage (and excludes data temporarily residing in computer memory). Examples include data stored on a computer hard drive, a database on a networked server, and files copied to a USB drive. Encryption of DAR is the encryption of data while resident on computer storage media.

There are 2 fundamental means of achieving encryption for data-at-rest. The simplest method (from a technology perspective) is to encrypt individual data files and folders. A more comprehensive approach (from a security perspective) is to encrypt the entire storage media. This latter approach, often referred to 'full-disk' or 'whole disk' encryption, has emerged as the 'best practice' for protecting data-at-rest on endpoint devices – desktops, laptops, and removable storage media. By encrypting data at the sector level, full-disk encryption provides the most comprehensive safeguards in the event of the loss or theft of an endpoint device.

Full-disk encryption is well suited to some applications, but not all. File, folder and container encryption (collectively 'FFCE') have a useful role to play in a comprehensive encryption strategy for protecting data-at-rest. These techniques extend cryptographic safeguards to shared files and folders on departmental servers and other common storage media. They offer protection for data files in transit (e.g. e-mail attachments) as well as additional security against internal threats.

Issues surrounding the protection of sensitive data or personal identifiable information (PII) are complex. While many solutions purport to protect the access and transfer of sensitive data and PII, this White Paper describes the principal methodologies for achieving data-at-rest encryption. It outlines the key factors sparking heightened interest in DAR encryption technology and offers some guidelines organizations should consider when choosing DAR encryption solutions. It also illustrates the unique capabilities of WinMagic's SecureDoc disk encryption solution.

2.0 New Challenges for Business

Corporations and government organizations are facing mounting pressures to better protect information assets and manage data security risks. These pressures come from:

- New rules, regulations and governance reforms
- The persistent threats of identity theft and fraud and,
- New, disruptive technologies that force organizations to take another look at where and how their enterprise data is stored.

Regulatory Compliance

Government concerns pertaining to the collection, use, retention and protection of sensitive and critical information are manifest in new regulations and scrutiny, especially for public companies and organizations in regulated industries, such as financial services and health care. Regulatory compliance has become a whole new discipline, rapidly changing the duties and policies of corporations around the globe.

Even where new government regulations don't exist, industry standards (e.g. the Payment Card Industry Data Security Standard) and the proliferation of best practices (e.g. ISO 17799) are raising the bar for data protection measures. Furthermore, the sheer magnitude of publicity surrounding data security breaches is creating a higher duty of care for all corporations and a potential legal liability for negligent ones. Ignorance of data security risks, and the means by which risks can be mitigated, is no longer an acceptable position for a responsible organization.

Corporate Governance

In today's business climate, corporations in virtually all sectors are being held to higher standards of accountability and transparency in their business operations. There is considerable interest in corporate governance practices which now extend well into the IT department. In particular, data management and protection are now governance issues, and very much within the purview of senior management and boards of directors. Corporate data is now regarded as a valuable off balance sheet asset that must be managed and protected like any other valuable corporate asset.

Privacy and Identity Theft

In response to growing concerns over individuals' privacy, and the threat of identity theft, we have witnessed the introduction of a complex array of privacy regulations in recent years. The Gramm-Leach-Bliley Act (USA), the Health Insurance Portability and Accountability Act (USA), EU Data Privacy Directive (European Union) and the Personal Information Protection and Electronic Documents Act (Canada) are examples of recent legislation that require corporations to collect, retain and use PII more responsibly.

To further protect PII, privacy and security regulations are now being updated to include breach notification clauses. Breach notification legislation (the foremost example being the California Senate Bill 1386) is intended to mitigate potential losses from data security breaches by giving victims the opportunity to protect themselves. Now introduced in over 35 states, this legislation effectively exposures organizations that fail to properly safeguard PII and experience a breach as a result. The risk of exposure has been particularly effective in changing organizational data security policies and practices.

Not surprisingly, the U.S. Government is demonstrating leadership in the protection of PII and other sensitive data. The Office of Management and Budget (OMB) issued a directive in June 2006 requiring that federal departments and agencies encrypt all data on mobile computers and devices carrying sensitive Government information.¹ In response to this directive, the U.S. Department of Defense recently formed a tiger team ('DARTT'²) to develop the DoD's technical requirements for DAR encryption and introduce a Government-wide procurement program.

Breach notification often includes an 'exemption clause' in which organizations are not required to disclose data security breaches if the compromised PII is encrypted. However, these rules are becoming increasingly sophisticated. Consider the example of a lost or stolen laptop containing sensitive PII. The hard drive of the laptop has been protected with full-disk encryption. The Gramm-Leach-Bliley Act does not exempt the owner of the laptop from disclosing the security breach if the key used to encrypt the PII was stored on the hard drive of the compromised laptop (along with the cipher text). This subtle change in exemption policy clearly highlights the need for pre-boot authentication methodologies that do not store encryption keys on mobile devices.

Information Risk Management

Risks to data-at-rest include hacking, spyware, malware, and loss or theft of storage media. The growing proliferation of mobile computing devices is causing increasing concerns among risk managers. Due to their small size and portability, these devices, which often store sensitive information including PII, are vulnerable to loss and theft.³

Insider attacks are gaining more attention as well since it has been demonstrated that the majority of security breaches that cause real economic damage are perpetrated by insiders.

Data security breaches, when they occur, can be expensive in terms of:

- Business disruption – the detection, investigation, escalation and remedy of the breach, as well as the communications campaign that may be required to mitigate negative fallout;
- Fines and / or remediation levied by governing bodies;
- Damage to corporate reputation, brand value and competitive position;
- Higher customer migration and lower new customer acquisition; and,
- Proprietary information loss.

There a number of additional costs associated with a breach of PII, including notification of affected individuals, identity theft support services (e.g. credit monitoring services), and the potential for class action lawsuits.

The Need for Increased Vigilance

Unlike encryption for data-in-transit, encryption for data-at-rest has been relatively underutilized to date. This is likely to change as all of the aforementioned factors suggest there a need for organizations to be more vigilant and to put greater emphasis on the protection of data-at-rest, no matter where it may reside. The goal must be to ensure data-

¹ M-06-16 Memorandum for the Heads of Departments and Agencies, 'Protection of Sensitive Agency Information', Clay Johnson III, Deputy Director for Management, June 23, 2006.

² 'DARTT' is an acronym for 'Data-at-Rest Tiger Team'.

³ In fact, the majority of attacks now occur against data-at-rest on endpoint devices.

at-rest is protected in a manner commensurate with the risk – and harm – of a security breach.

Protection for data-at-rest requires policies, procedures and technologies. When it comes to ensuring confidentiality for data-at-rest, encryption is the foremost technology consideration. As the next section illustrates, there are a number of methods for encrypting data-at-rest on endpoint devices and on removable media.

3.0 Encryption Methodologies for Data-at-Rest

Figure 3-1 provides an overview of the most common methodologies for encrypting data stored on laptops, PDAs, smart phones and removable media.

| | Full-Disk Encryption | File Encryption | Folder Encryption | Container Encryption |
|--------------------------------------|----------------------|-------------------|-------------------|----------------------|
| Protection for 'Data-at-Rest' | | | | |
| Individual Files | * | * | * | * |
| Files Names | * | | | * |
| Folder Contents | * | | * | * |
| Operating Systems | * | | | |
| Application Software | * | Some | Some | Some |
| Databases | * | Some | Some | * |
| Temporary / Paging Files | * | | | |
| Back-up / Auto-save Files | * | | | * |
| Deleted Files | * | | | * |
| Windows Registry | * | | | |
| Hidden Partitions | * | | | |
| Free Disk Space | * | | | |
| Removable Media | * | * | * | * |
| User Transparency | Full | Partial | Partial | Partial |
| Information Sharing | Media Level | Data Object Level | Data Object Level | Data Object Level |
| Performance | | | | |
| CPU Degradation | Negligible | Moderate | Moderate | Minor |
| Memory Usage | Negligible | Moderate | Moderate | Minor |

Figure 3-1: Comparison of Encryption Methods for Data-at-Rest

3.1 Full-Disk Encryption

Full-disk encryption refers to encryption of all data on sector-addressable storage media (e.g. hard disks or flash devices).

Full-disk encryption software encrypts the entire storage media⁴ in a single pass during an initial phase called 'conversion'. Once conversion is complete, subsequent encryption and decryption operations are transparent to users. Specifically, full-disk encryption software transparently intercepts and encrypts data just before it is written to the disk and intercepts and decrypts data immediately after it is read off of the disk. Interception and encryption / decryption occur at the point of sector-level disk access.

The principal benefit of full-disk encryption is more comprehensive protection for data-at-rest. As evident in Figure 3-1, full-disk encryption protects every file and all data saved to disk, including the operating system, executable files and users' documents. Full-disk encryption also protects temporary, recycled, paging and hibernation files – even the crash dump.⁵ No other method can thoroughly protect all of these files as well as data not addressable as a file, such as the hibernation file.

It is important to note that data, once written to magnetic media such as a hard disk, can be recovered even after it has been overwritten. Once conversion is completed, full-disk encryption solutions ensure data is never written to the media in plain text form. Clearly, file-based encryption solutions cannot make this guarantee since they operate on files that were once stored in plain text.

It is a common misperception that full-disk encryption degrades system performance more than file-based methods. Improved CPU speed and the intelligent disk caching features of newer operating systems have made system degradation negligible (typically in the order of 2% to 3%). In fact, when compared to FFCE, full-disk encryption is more efficient in terms of disk memory overhead and CPU usage. The efficiencies result from the architecture of disk encryption solutions, which perform certain cryptographic operations once for the entire disk rather than many times for each individual file, folder or container.

With more comprehensive safeguards, full-disk encryption is now widely regarded as the 'best practice' for ensuring the confidentiality of PII and proprietary digital assets stored on mobile computers and removable media.

3.2 File and Folder Encryption

File encryption is an application that enables users to manually encrypt individual files they wish to protect. Folder encryption applications allow users to move files into specific folders where they are encrypted automatically.

Both methods have limitations as viable security schemes for protecting DAR:

- As illustrated in Figure 3-1, only original files are encrypted. Many file copies are left in clear text.
- Manual file encryption relies on users taking the initiative to protect files. The methodology is prone to human error and forgetfulness, both of which can leave sensitive data unprotected. Automatic file encryption schemes remedy this shortcoming by automatically enforcing encryption of designated file types in accordance with security policies.
- Both techniques can be resource intensive, particularly when files get large.

⁴ There can be some exceptions. Not all disk encryption products encrypt the hibernation file or the crash dump for example.

⁵ Note – if a 'disk encryption' solution does not offer pre-boot authentication, it does not fully encrypt the entire disk. Specifically, it does not protect the windows boot and systems files.

3.3 Container Encryption

A container is a large file used by applications and users to store data files. Often referred to as 'virtual drives', containers appear to Windows as normal disk drives. Containers can be configured on local hard disks, networked drives or removable media such as USB drives and CD / DVDs.

Container encryption schemes create large, hidden files, which are organized and presented to the operating system as usable, logical drives. All information stored on these virtual drives is encrypted.

Like disk encryption, container encryption offers transparency for users. Files written to the container are encrypted automatically. As indicated in Figure 3-1, this method also provides protection for some file copies, specifically automatic backups and deleted files.

Container encryption also offers advantages for sharing removable media securely. Since container encryption does not have to occupy all sectors of the removable media, installation / setup files can be stored on the same media as the encrypted container. Authorized recipients can use these files to install and access the encrypted container without having to source a software driver first.

Container encryption has some disadvantages however, the main one being that it cannot properly protect the system disk data. Operating systems create some temporary or paging files on physical disks, not virtual drives. Consequently, container encryption does not protect these files.⁶ And when a disk accesses a virtual drive, it is redirected to the corresponding file. This extra step (i.e. overhead) degrades system performance.

3.4 The Role of File, Folder and Container Encryption

On first blush, file, folder and container encryption may seem to have too many limitations to warrant consideration. But in fact, FFCE has a useful role to play in a comprehensive strategy for data-at-rest encryption. It is effective in protecting data files in transit, secure information sharing, and defending against internal threats.

FFCE techniques are useful for securing files prior to transmission over the Internet. By shielding data files in transit, file transfers, e-mail attachments, etc., FFCE provides a strong complement to full-disk encryption, particularly when the functions are integrated under a single management scheme.

Perhaps where FFCE really shines is in secure data sharing applications. Employees and business partners often share computers and thus, hard drives. They certainly access shared files on a common server. Since full-disk encryption uses the same key for encrypting the entire disk, all authorized users have access to all encrypted data by default. Unlike disk encryption, FFCE uses different encryption keys for different data objects. Consequently, it can be used to control or restrict access to different data sets.

Consider as an example a security objective to ensure data is not written to a USB thumb drive in plaintext. The first consideration should be to encrypt the entire USB drive (meaning all sectors on the drive are encrypted) as this would make certain that all data written to the drive is encrypted automatically, without user intervention.

⁶ System files, such as paging and hibernation files, do not reside on removable media. This disadvantage is clearly immaterial when container encryption is used to protect removable media.

Now consider an additional requirement. The drive is to be shared amongst members of a group, but not all members have privileges to see all the files stored on the drive. Restricting data access on a 'need to know basis' is a standard technique for mitigating the risk of insider breaches.

With this additional requirement, full-disk encryption alone is not sufficient because it affords all members access to all files. In this media sharing application, container encryption could be considered instead of, or in lieu of, full-disk encryption. The files could be distributed between two or more containers, each encrypted with a different key. If more granular file access is required (perhaps each member has his own personal files) then file encryption could be considered as well.

FFCE is often used in conjunction with full-disk encryption to create a more secure system. Since FFCE creates 'secure compartments' on the encrypted disk for different users, insiders can share access to a secure system, but not access the data belonging to others.

There are also issues to consider when choosing between file, folder and container encryption. In general, the fewer encrypted data objects to manage the better. For example, grouping 10 files together in one encrypted container it is easier to manage than 10 separate encrypted files, particularly from data classification and key management perspectives.⁷

Finally, there are technical constraints to consider as well. Not all platforms – CPU, OS, storage media – support all encryption methodologies. Removable media has different characteristics than hard disks, and these differences often favor one encryption method over the others.

3.5 DAR Requirements Summary

The following table summarizes some of the principal requirements for data-at-rest encryption as well as preferred method for each.

| DAR Encryption Requirement | Preferred Method |
|--|--|
| Encryption for all data stored on the main hard disk | Full-disk encryption is the only solution that addresses this requirement. |
| Encryption for all data stored on / written to removable media | Full-disk encryption is the simplest – and therefore preferred – method for the encryption of removable media. When CDs and DVDs are used to distribute encrypted data to authorized recipients, container encryption should be considered however. Container encryption allows clear text client software – needed to decrypt the container – to be distributed on the same CD / DVD as the encrypted container. Co-locating the encrypted container and the client software needed to decrypt it, makes data extraction considerably easier for authorized recipients. |
| Encryption of data files and / or folders | File and folder encryption |
| Encryption of containers | Container encryption |
| Protection from internal threats in media sharing environments | In environments where media sharing is encouraged, granular encryption options are required to effectively 'compartmentalize' data. In these environments, consider encryption of granular data objects such as disk partitions, containers, folders, files or individual database columns. Encryption at these levels provides insiders with |

⁷ Clearly, object oriented encryption has a profound affect on the requirement for scalability within the key management system.

| | |
|---|--|
| | access to shared media while preventing access to restricted data. |
| Prevention of data leakage to removable media | Disk access controls that prevent the copying of data to removable media, and / or ensure that only encrypted files are copied to removable media. |
| Prevention of data leakage over the network | File encryption supporting selective encryption of files by type and application association. ⁸ |
| Prevention of data leakage via e-mail | File encryption supporting selective encryption of files by type. |

Figure 3-2: DAR Encryption Requirements and Preferred Solutions

In summary, a full-disk encryption solution, complemented with additional functionality for the encryption of more granular data objects, files, folders and containers, addresses a broad range of data-at-rest encryption requirements for hard disks as well as removable media.

4.0 Considerations in Choosing a DAR Encryption Solution

There are a number of issues to contemplate when choosing an encryption solution for data-at-rest. In this section, we provide a list of topics to consider when comparing options.

| | |
|--------------------------------------|---|
| Comprehensive Data Security | <p>The DAR encryption solution should protect all copies of sensitive information stored on hard disks and removable media. Multi-factor authentication at pre-boot provides the maximum defense against unauthorized access.</p> <p>All security products, including DAR encryption software, should provide an audit log that illustrates the products' efficacy.</p> |
| User Transparency / Ease of Use | <p>Users will circumvent security measures if they are intrusive, difficult to use, or impede day-to-day productivity. Transparent solutions operate in the background, with little, if any, user intervention. They require minimal user training, maintain users' productivity and cannot be easily bypassed, either inadvertently or deliberately.</p> |
| Full-Disk Encryption <i>and</i> FFCE | <p>Full-disk encryption is the preferred solution for protecting DAR. However, consider the need to transfer files securely between companies, or share files with some insiders but not all. FFCE addresses these secure data sharing requirements. A comprehensive solution offers both full-disk encryption and FFCE under a single management umbrella.</p> |
| Support for Removable Media | <p>A disk encryption solution is of limited value if users can easily copy sensitive information to unprotected, removable media such as USB thumb drives and CD / DVDs. A robust solution prevents this type of data leakage by encrypting removable media and enforcing acceptable use policies.</p> |

⁸ Please refer to section 5.3.1 for a description of these features.

| | |
|--|---|
| <p>Enterprise-Class Management</p> | <p>An enterprise-class DAR encryption solution provides a centralized management application to streamline the wide-scale deployment, installation and configuration of DAR encryption software across a large organization.</p> <p>It also provides the administration tools necessary to support end users remotely for important tasks such as password recovery.</p> |
| <p>Implementation of Security Policy</p> | <p>The design and implementation of security policy plays a key role in establishing an organization’s overall security posture. An advanced solution simplifies the implementation of policy decisions related to DAR encryption. In general, it is advisable to cross reference your policy decisions against the capabilities of the solutions under evaluation.</p> <p>For example, consider the policies around passwords (e.g. length) and password management (e.g. forced change). Configuration utilities should be extensive and flexible enough to ease the implementation of your password policies across large numbers of users. As another practical example, consider a policy decision to encrypt all removable media ‘attached’ to a secured system. The solution should perform this encryption automatically (when the removable media is first attached to the system) without reliance on user or administrator intervention.</p> |
| <p>Data Recovery</p> | <p>Encryption of DAR can be a long-term proposition. Administrators must have the tools to securely escrow encryption keys and recover encrypted data at any point in the future.</p> |
| <p>Information Sharing</p> | <p>Many organizations share sensitive PII (e.g. credit information, health records) with third parties in the normal course of business. This PII is routinely stored on removable media (e.g. CDs) and delivered via commercial services. Best practices now require encryption of this information to prevent the compromise of PII, in the event removable media is lost or stolen while en route.</p> <p>Clearly, these third parties need to decrypt the removable media they receive. They require the cipher keys – and only those cipher keys – necessary to do that. To support information sharing between parties, the disk encryption solution should provide a selective, secure key transfer capability from issuing to receiving party.</p> <p>The receiving party may or may not have the same disk encryption solution as the issuing party. Platform-independent client software (often referred to as a ‘disk viewer’) is required to support authorized receiving parties without access to the full encryption solution. Disk viewers provide decryption functions (only) for authenticated extraction of encrypted data on removable media.</p> |
| <p>Interoperability with your IT</p> | <p>Most organizations have considerable investment in IT infrastructure such as software distribution tools, disk imaging applications, user</p> |

| | |
|---|---|
| Infrastructure | authentication systems, and user / profile management applications (e.g. Active Directory Services, LDAP, etc.). An advanced DAR encryption solution interoperates with this infrastructure to ease deployment and management issues. |
| Full Support for Disk and Imaging Utilities | It is a common misperception that disk utilities and imaging utilities such as defrag, Ghost, and anti-virus software fail when a disk is encrypted. This should not be the case – a properly encrypted disk should behave no differently than an unencrypted disk. |
| Based on Open, Industry Standards | In the data security industry, standards are designed and rigorously scrutinized by the industry's best minds. It should not be surprising then that products built around industry standards offer the highest levels of assurance. Such products also offer greater interoperability with other products based on the same standards. Interoperability is frequently a key purchasing decision as it often provides buyers with greater utility for their investment. |
| Certifications and Evaluations | The solution must have the certifications and evaluations necessary for its intended use. FIPS 140-2 certification is mandatory for the protection of sensitive Government information. Common Criteria Evaluation Assurance is becoming increasingly important in a variety of markets. In addition, the solution should use mature, proven cryptographic technologies wherever possible. |
| Vendor's Pedigree | Designing and building a trusted, effective DAR encryption solution is a difficult undertaking. It takes years of product development effort, testing and experience in large scale, enterprise deployments. The vendor's expertise, experiences and tenure in the industry are therefore key considerations. Financial viability is important as well – it is a prerequisite for continued product enhancements, ongoing technical support and new innovations. |

Figure 4-1: Purchase Considerations for DAR Encryption Solutions

This is by no means a complete list of purchase considerations, but hopefully serves as a useful starting point for evaluating encryption solutions for data-at-rest.

5.0 Introduction to SecureDoc

The following sections provide an overview of WinMagic's award-winning SecureDoc encryption solution for data-at-rest. They serve to illustrate that SecureDoc provides provide robust safeguards for data-at-rest while meeting a wide variety of application requirements.

5.1 Comprehensive Full-Disk Encryption

SecureDoc's full-disk encryption fulfills the requirements of the most security conscious organizations.

- SecureDoc uses state-of-the-art, 256-bit AES to encrypt all data on mobile computers and devices. SecureDoc fully encrypts the hard drive and removable media of these devices, including the boot record, operating system, application software, user data, the recycle bin, paging / swap files, temporary files and slack space.
- SecureDoc employs multi-factor user authentication via smart cards, USB crypto-tokens, biometrics, TPM, password, Public Key Infrastructure (PKI) certificate verification, or any combination thereof. Multi-factor authentication by way of something known (e.g. a password) and something owned (e.g. a token) ensures that access to confidential data is limited to authorized personnel.
- SecureDoc authenticates users at pre-boot (after the BIOS post but before the operating system loads). Pre-boot authentication provides the maximum defense against hacking attempts.⁹
- Once a user is authenticated with a USB crypto-token or smart card, SecureDoc will 'lock down' the computer if the token or smart card is disengaged. In order to re-gain access to the system, the user must re-authenticate with the token or smart card.
- SecureDoc can be configured to force users to re-authenticate themselves at pre-set time-out limits.
- SecureDoc's comprehensive audit log tracks users' access to encrypted systems and failed login attempts. Audit logs are encrypted, signed and can be automatically uploaded to a central location and exported for analysis by third party applications.
- SecureDoc's security accreditations include FIPS 140 -2 Level 2 Certification and NIST Cryptographic Module Validation for AES (#1 and #359), SHA2 (#434), and HMAC (#158) and Common Criteria Evaluation Assurance (EAL-4).

5.2 Transparent Operation

SecureDoc's full-disk encryption is automatic and transparent to end-users. Once authenticated, users do not need to take additional steps to protect data. Furthermore, users cannot bypass SecureDoc's cryptographic defenses. SecureDoc is a certain, auditable implementation of a security policy for the continuous protection of data-at-rest.

⁹ For example, pre-boot authentication makes attempts to bypass the Windows Login Authentication pointless. Even successful attempts will yield only encrypted data.

5.3 Support for File, Folder and Container Encryption

As illustrated in Figure 5-1, SecureDoc supports full-disk, file, folder and container encryption across a variety of storage media.

| | | Storage Media | | |
|--------------------------------|--|---------------|---------------------|----------|
| | | Fixed Disk | Removable USB Drive | CD / DVD |
| Data Objects | Disk Sector | ✓ | ✓ | ✓ |
| | File | ✓ | ✓ | ✓ |
| | Folder | ✓ | ✓ | ✓ |
| | Container | ✓ | ✓ | ✓ |
| Key Management Features | SecureDoc Key / Group Key with SecureDoc Key File Concept | ✓ | ✓ | ✓ |
| | Password Support for External Entities | ✓ | ✓ | ✓ |
| | Dynamic Key Provisioning | ✓ | ✓ | ✓ |

Figure 5-1: SecureDoc's Broad Support for Encryption Methodologies

With full-disk encryption *and* FFCE support, SecureDoc is the most secure solution for data-at-rest, while providing enhanced cryptographic safeguards for data files in transit and data sharing applications. All encryption methodologies are configured and administered from a single management application.

5.3.1 Automatic File and Folder Encryption

With SecureDoc, users encrypt / decrypt files with intuitive functions such as 'dragging and dropping' and the 'right-click' menu. Automatic folder encryption means files are encrypted as they are moved into designated folders.

Application Association

Files with predefined extensions associate with specific applications. For example, files with a .doc extension are linked with Microsoft Word and in particular, Winword.exe, MS Word's executable program. SecureDoc takes advantage of these associations to make file encryption transparent to applications such as MS Word, and to users of these applications.

File and Folder Encryption with Application Association offers a number of benefits:

- Files can be selectively encrypted by type. Continuing with the example, security policy may require that all .doc files are to be encrypted. SecureDoc's Application Association ensures this policy is enforced.
- Transparent operation means that files opened by their associated applications are decrypted automatically. Users can then work on these files. When users exit the applications, the files are automatically encrypted again.

- If a file is moved or copied to a network server, or attached to an e-mail, it remains in an encrypted state. Even if one user is working on a file and another user copies it, the copied file remains encrypted.

File Encryption and Removable Media

SecureDoc's File Encryption offers unique features for enforcing security policies related to the encryption of files that are moved or copied to removable media.

When an encrypted file is moved or copied to removable media such as a USB drive or CD / DVD, SecureDoc will ensure the file either remains encrypted or is reverted to clear text, in accordance with predefined security policies. Similarly, when a clear text file is moved or copied to removable media, SecureDoc either encrypts the file or leaves it in clear text, depending on the security policies that have been configured for the removable media.

5.3.2 Encrypted Containers

SecureDoc's container encryption is transparent – files are automatically encrypted as they are stored in the container, and automatically decrypted as they are opened from the container. It is also platform agnostic – encrypted containers can be accessed from a PC or PDA with the appropriate SecureDoc client software.

SecureDoc's container encryption is useful for saving encrypted information on a local drive, shared drive or on removable media. It is great way to selectively share encrypted information amongst authorized users.

5.3.3 Comprehensive Media Support

As suggested in Figure 5-1, SecureDoc protects a comprehensive range of fixed and removable storage media, including:

- Fixed disks, Redundant Arrays of Independent Disks (RAIDs), Magneto Optical Drives; and,
- USB / firewall drives, CD / DVDs, Flash and SD cards, and PCMCIA, Jaz and Zip drives.

SecureDoc's defenses extend to large disks (larger than 2 TB) with unlimited partitions.

5.3.4 'Disk Lock' Media Access Controls

A strong complement to data encryption, SecureDoc's Disk Lock media access controls prevent unauthorized copying of data to removable media. With Disk Lock, Administrators can configure SecureDoc to: read-only from removable media; write only to encrypted removable media; or, disable access to removable media entirely. These powerful access controls prevent data leakage to unsecured media while enforcing security policies.

5.4 Enterprise-Class Management

SecureDoc Enterprise Server™ (SES) is a centralized management application for the enterprise-wide deployment, management and administration of SecureDoc encryption software. SES ensures SecureDoc can be deployed quickly and easily across organizations of all sizes. It empowers administrators with the following features:

- Custom configuration of user and / or group profiles;

- 'Background' or silent downloading and installation of SecureDoc software on client systems;
- Remote configuration and conversion¹⁰ of client systems without user intervention;
- Automatic synchronization of user profiles with LDAP directories or Active Directory services;
- An intuitive interface to define and implement a broad range of security policies, such as acceptable use policies for removable media and password policies;
- Remote control of client computers, including remote re-boot and lock down; and,
- Remote password recovery through a secure, one-time challenge / response scheme.¹¹

SES is also an enterprise-class key management platform. As such, it scales to accommodate millions of encrypted data objects – files, folders, containers – and millions of encryption keys. A single SES cluster can support the DAR encryption requirements of large enterprises from one central location.

SES ensures encryption keys can always be matched with the encrypted data objects they protect. It provides encryption key backup and restoration services to ensure encrypted data objects can always be recovered (i.e. decrypted) at any point in the future.

Ensuring your encryption solution will provide access to your data 10 or more years from now requires careful evaluation. You may have the encrypted drives and the encryption key repository intact, but how do you determine which keys are required to decrypt the different drives?

SecureDoc's key labeling feature allows administrators to 'name' encryption keys with human-readable text. Human-readable labels help simplify key management. They enable administrators to distinguish encryption keys, and quickly associate them with the corresponding encrypted drive – now and in the future. They accelerate data recovery from encrypted archives.

SES provides administrators with visibility to the many DAR encryption keys generated within their enterprise. Key labeling is one of several tools at their disposal to better manage these keys.

SES uses Microsoft SQL Server as its data repository. This ensures administrators have a scalable management application that supports database backup, replication, and clustering. SES communicates with distributed client systems securely over any IP-based network, via file transfer, e-mail, or an exchange of removable media such as a CD or memory stick.

Clearly, the long term repository of DAR encryption keys must be strongly protected itself. SES employs a number of safeguards, including encryption, to protect its encryption key database.

¹⁰ 'Conversion' is the term used for the initial encryption of a client system, after the encryption software is installed.

¹¹ SecureDoc's scheme does not rely on the outdated 'Master Password' concept, which WinMagic has proven to be insecure.

5.5 Secure Information Sharing on Removable Media

SecureDoc supports distribution of encrypted information – stored on removable media – to business partners and other trusted individuals.

SecureDoc encrypts removable media, which then can be delivered to one or more individuals. All data stored on the encrypted removable media is encrypted as it is written to the media.

The business partners need not have SecureDoc installed. WinMagic offers a free, downloadable 'DiskViewer' – client software that allows recipients of the encrypted removable media to read cipher text on the media. Recipients must first be authenticated, by providing either a password, or the key that was used to securely wrap the encryption key (i.e. the Key Encryption Key). Password support is particularly convenient when sharing data with external parties.

SecureDoc 'ContainerViewer', another free download, provides similar read capability for encrypted containers distributed on shareable media such as CD / DVDs. ContainerViewer offers additional conveniences for the secure distribution of data – the ContainerViewer client software and the encrypted container can be distributed on the same physical media to streamline data extraction.

5.6 Dynamic Key Provisioning

Dynamic Key Provisioning is sophisticated new functionality for SES. It supports seamless sharing of encrypted storage media, files, folders and containers within – and outside of – the enterprise.

Dynamic Key Provisioning effectively enables access to encrypted data by delivering the necessary encryption keys in real time, when needed, in accordance with preconfigured privileges. By disseminating encryption keys on a who, what, when, where and why basis, Dynamic Key Provisioning effectively implements access control policies through selective key distribution.

The benefits of Dynamic Key Provisioning are far reaching. Consider, as an example, a requirement to share encrypted files among a group of users within an organization. These files can be distributed to group members in any numbers of ways – e-mail, shared media, file server, etc. Dynamic Key Provisioning ensures that each member of the group can access encrypted files by providing the necessary keys over a secure network channel. In this example, group membership affords access to encrypted files – and provides sufficient privileges to receive the required keys.

Dynamic Key Provisioning at pre-boot offers the potential for networked-based authentication (at pre-boot), and 'anywhere' access to encrypted media.

5.7 Committed to Standards

WinMagic designed SecureDoc with industry standards 'from the ground up'. SecureDoc incorporates standard, vetted cryptographic technologies and other standards wherever possible, including:

- NIST standards for encryption, hashing, message authentication and random number generation;

- PKCS-11 standard for interfaces with cryptographic devices, such as smart cards and tokens;
- Open Card Framework proposed by IBM, Netscape, Oracle, Sun and others;
- X.509 standard for digital certificates; and,
- LDAP and MS Active Directory specifications.

The Company will also support emerging standards for data storage encryption such as IEEE 1619.

For end users, this translates to a more secure solution, compatible with a broader range of enterprise systems. In addition, since standards-based solutions offer greater design modularity, SecureDoc offers more flexibility to support customers' future requirements.

5.8 Interoperability with Existing IT Infrastructure

With a flexible, standards-based design, SecureDoc seamlessly interoperates with existing IT infrastructures, including:

- Distribution tools for enterprise-wide software deployment, including Tivoli, SMS and Active Directory;
- Disk imaging applications for data backup;
- Virtually all PKI suppliers, including Baltimore, CA, Digital Signature Trust, Entrust, Indentrus, Microsoft and Verisign.
- All major authentication solutions, including the DoD Common Access Card, HSPD-12 PIV Authentication Cards, and products offered by ActivIdentity, Aladdin, Datakey, Eutron, Kobil, Spyrus, Rainbow and many others; and,
- Anti-virus software, disk utilities and data recovery tools.

SecureDoc's interoperability with third party solutions enables administrators to leverage their investments in management tools, user management systems, and user authentication technologies to minimize operating costs and deploy solutions faster.

6.0 About WinMagic

WinMagic, the innovative leader in security solutions for the mobile workforce, provides the world's most secure, manageable and easy-to-use encryption software for data-at-rest.

WinMagic's SecureDoc provides full-disk encryption and multi-factor authentication to protect sensitive personal information and proprietary data stored on endpoint devices, such as desktops, notebooks, external USB drives and CD / DVDs. Enterprise and government organizations around the world depend on SecureDoc to minimize business risks, meet privacy and regulatory compliance requirements, and protect valuable information assets.

SecureDoc authenticates users at pre-boot, using any combination of passwords, smart cards, TPM, hardware tokens, PKI and biometrics. Built on open systems standards, SecureDoc Enterprise Edition employs a Microsoft SQL server to manage users and encryption keys at an enterprise level. Offering remote installation, centralized administration, integration with Active Directory and LDAP servers, and remote password recovery, it allows for easy, enterprise-wide deployments and reduced management costs.

WinMagic operates through direct and indirect channels in over 43 countries. For more information, please visit www.winmagic.com, call 1-888-879-5879 or e-mail us at info@winmagic.com.

6.1 A Focus on Innovation

Throughout its ten year history, WinMagic has been a driving force of change in the PC security industry. The company has been responsible for most, if not all, of the significant advancements in full-disk encryption technology. WinMagic was the first to introduce:

- The integration of smart cards and PKI with disk encryption in 2000;
- Biometric authentication at pre-boot;
- Encryption of removable media in 1998;
- Support for the Trusted Platform Module (versions 1.1 and 1.2) at pre-boot;
- Full-disk and file / folder / container encryption in a single product;
- Support for drives with non-standard 512 byte sectors, such as MO drives;
- Support for hibernation, imaging software and disk utilities such as defrag; and,
- A central management application for the remote installation, configuration, conversion and administration of large numbers of endpoint devices within an enterprise.

WinMagic continues to demonstrate its thought leadership as the company defines the next generation of security solutions for data-at-rest, including hosted services for disk and file encryption, dynamic key management, and network-based authentication at pre-boot.

7.0 Conclusion

A variety of factors, including information security risks, privacy and regulatory compliance requirements are motivating organizations to consider data-at-rest encryption with increased vigor.

When evaluating options, purchasers must consider full-disk encryption solutions that offer multi-factor user authentication at pre-boot, include FFCE encryption utilities, and use validated cryptographic modules. Solutions with these features provide the maximum protection for all data stored on laptops, desktops, PDAs and removable media, including CD / DVDs and USB thumb drives, without sacrificing user efficiency or system performance.

WinMagic's SecureDoc is such a solution. It is complemented with a scalable, centralized management application that accelerates enterprise-wide deployment and the administration of client encryption software. With a flexible, standards-based design, SecureDoc seamlessly interoperates with existing IT infrastructures including software distribution tools, disk imaging applications, anti-virus software and disk utilities.

With over 1.5 million deployments world-wide, WinMagic is a proven software vendor. SecureDoc is a mature solution offering many unique features and capabilities. As corporations and government organizations begin to address new requirements for DAR encryption, many will discover that WinMagic and SecureDoc meet their needs.

8.0 Disclaimer

This White Paper is provided for information purposes, and to promote active consideration and discussion of encryption for data-at-rest. It is not an exhaustive discussion of the issues, and should be considered only as a starting point for a more complete assessment methodology.

To the best of the knowledge, information and belief of WinMagic, the information in this White Paper is accurate, but WinMagic cannot be held liable for any errors or omissions, or for any decisions based on its content.

SecureDoc, SecureDoc Enterprise Server, Compartmental SecureDoc, SecureDoc PDA, SecureDoc Personal Edition, SecureDoc RME, SecureDoc Removable Media Encryption, MySecureDoc, MySecureDoc Personal Edition Plus, MySecureDoc Media, and SecureDoc Central Database are trademarks of WinMagic Inc. Other products mentioned here in may be trademarks and / or registered trademarks of their respective owner

(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

E-mail: 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 e-mail 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.