



Stay Out of the Headlines – Next-Generation Encryption for Notebooks, Tablet PCs and Desktops

Technical White Paper

July 2006

**CREDANT Technologies
Security Solutions**



Table of Contents

INTRODUCTION:	
Never Has Information Been Less Secure	3
WHY THE NEED FOR A NEW ENCRYPTION APPROACH?	3
Traditional Encryption Methods	3
Full Disk Encryption (FDE)	4
File/Folder-Based Encryption	5
CREDANT MOBILE GUARDIAN SHIELD	5
Credant Intelligent Encryption	6
Total Data Protection: four levels of defense	6
Minimum Overhead, Maximum Protection	7
Protecting User and Shared Sensitive Information	7
Protecting Temporary Files	7
Protecting the Windows Paging (Swap) File	8
Protecting the Windows Password	8
Enhancing Windows Access Control	8
Protecting Removable Media	10
Recovering Encrypted Data	11
CONCLUSION	12
Table 1. Comparing and Contrasting CREDANT Intelligent Encryption with Full Disk Encryption, and File/Folder-Based Encryption	13
Contact Us	15

INTRODUCTION: Never Has Information Been Less Secure

In a business world threatened by negligence, regulatory compliance, sabotage and terrorism, never has corporate data been less secure. The Privacy Rights Clearinghouse lists 214 companies or public institutions that have reported data breaches since February 2005. These breaches have impacted over 88 million individuals, a number that may be grossly underestimated due to some organizations not knowing how much information actually was stored on the lost or stolen computer.

This white paper focuses specifically on how best to secure vital, sensitive information stored on Windows Notebook PCs, tablet PCs and desktops. However, there is, of course, a vast amount of data on a notebook or desktop hard drive that does not have to be protected, because it does not contain sensitive information. While Full Disk Encryption (FDE) encrypts everything on the hard drive—including non-sensitive operating system and application program files— and encrypting the whole disk may initially seem to be the most secure and thorough approach, companies have found that the deployment of this technology poses significant challenges to the business in a number of key areas, including manageability, recovery, security and usability.

The requirements for protecting data at rest on a Windows-based desktop or notebook are quite simple: ensure that only authorized users can gain access to any sensitive information stored on the computer and ensure data is protected when moved to an external storage device. The only way to effectively protect sensitive information is to enforce the use of a strong password and provide a second layer of defense with industry-standard and validated encryption. Encryption scrambles the information making it inaccessible to unauthorized users. Sensitive information needs to be encrypted regardless of where it is stored on the hard drive or on removable media such as a USB storage device or iPod®. However, one must also ensure that encryption is as transparent as possible to the end user to ensure acceptance and discourage work-arounds.

WHY THE NEED FOR A NEW SECURITY APPROACH?

Protecting sensitive information is critical. Up until now, organizations have had only two encryption choices: count on an end user to store a file in a special folder that ensures the file is encrypted, or encrypt the entire hard drive. However, full-disk encryption products are riddled with management support, data recovery and corruption issues, and productivity losses.

Traditional Encryption Methods

Encrypting binary files, such as the Windows Operating System (OS) and program files, which do not contain sensitive data, can significantly impact an organization's every day support and maintenance procedures. Worst case, encrypting these files can have catastrophic consequences. Corruption of an encrypted OS file or program file could cause system instability and possibly prevent the machine from booting, or a user from logging in, causing remote or traveling employees to be unproductive or, worse, to lose all their data.

This section examines two existing approaches to protecting mobile information: full-disk encryption and file-folder encryption.

Full Disk Encryption (FDE)

FDE products ensure that mobile information is secure by encrypting the entire hard drive, including Windows OS and program files, as well as a variety of pre-Windows boot files. While this approach may, on the surface, seem like the easiest and most secure approach to data security, FDE solutions can be extremely costly in the long run due to the following limitations:

Reduces End User Productivity

- Requires a non-Windows/non-standard authentication process unfamiliar to end users, resulting in possible increase in help desk calls, training needs and unforeseen security issues.
- Incompatible with standard Windows features, such as Hibernation and Defragmentation.
- Modification of the master boot record by third-party software (for example, Altiris Backup, TurboTax, Partition Magic, etc.) can cause the full disk encryption program to fail, rendering the hard disk and PC unusable and resulting in the loss of all data.
- Requires a long initial encryption process that cannot be successfully accomplished by many end users.
- Windows system and program files are encrypted, slowing boot time and affecting application performance.

Expensive Recovery and Support

- Requires administrator to manually define users and groups before solution can be deployed due to lack of integration with enterprise directory services such as LDAP or Microsoft Active Directory.
- Ghost image is recommended before deployment, not just data backup.
- Increases support cost and extends instant recovery time from minutes to hours, in many cases, even days for "broken" computers because IT must decrypt the entire disk, whereas before they could simply use a Windows Recovery disk.
- May not be compatible with all versions of BIOS and manufacturers of hard drives/computers.
- In-person IT provisioning is usually recommended for FDE products, due to issues with the time to encrypt the entire hard drive and potential hardware compatibility issues.
- Requires end-user training to ensure successful deployment due to changes in login behavior.
- Causes significant costs associated with end-user downtime and time/resources to restore data lost due to increased number of hard drive failures.

Security Limitations

- Many companies have administrators who perform routine maintenance and ongoing support, including the upgrade of existing applications, troubleshooting and reinstalling an existing application, or modifying the local operating system settings. An FDE solution requires an administrator to have an administrative login for the pre-boot authentication that provides access to the machine and all encrypted data on the drive. This pre-boot authentication means that an administrator performing routine maintenance will have access to all encrypted data on the drive, even though access to this data is not required to perform routine maintenance.

Data Loss

- With FDE, some data may never be recovered from a corrupted device.

The successful adoption of security policies and solutions requires a balance of easy and efficient deployment and management, support costs and end user acceptance. While considered "secure", FDE's lack of this balance has caused many deployments to fail, resulting in frustration, lack of trust in the solution, unprotected mobile information, and significant back-end costs for recoveries.

File/Folder-Based Encryption

Another alternative encryption method is a file-based solution that can enforce that the contents of specified folders (for instance, the C:\Secure Folder) are encrypted automatically. File/folder based solutions have a number of serious security limitations that include:

Encryption of only specific folders and files

- Does not protect sensitive information stored on removable media, in the Paging File, or in any files that are not stored in specified secure folders

End-user controlled security

- End-users must store sensitive information in specified secure folders, otherwise the data is not protected

Microsoft's Encrypting File System, a standard part of Windows 2000 and XP, is a widely available file-based solution which also suffers from these security limitations and from the availability of certain utilities, such as LC 5 and EFS Crack, which can be used to bypass the Windows password or to crack the EFS encryption keys and gain access to sensitive information.

In summary, neither full disk or file-based encryption meet all the security, management and ease-of-use capabilities required by organizations looking to ensure that their sensitive information is protected at all times.

CREDANT MOBILE GUARDIAN SHIELD

CREDANT Mobile Guardian (CMG) Enterprise Edition takes a new approach to protecting information assets against loss, theft, attack and unauthorized use. It provides a cost-effective deployment and management infrastructure that greatly eases the burden on IT (Figure 1). A component of CMG, the CREDANT Mobile Guardian Shield for Windows (CMG Shield), provides a next-generation, patent-pending Intelligent Encryption method that fills the security gaps left by file-based products and avoids the management, recovery issues, data corruption and productivity issues associated with full, or hard, disk encryption. The CMG Shield is virtually transparent to authorized end users while enabling them to always have access to their PC and information without changing the way they work.

CMG Shield for Windows has received FIPS 140-2 validation for the CREDANT Cryptographic Kernel under. This independent validation ensures the product correctly performs cryptographic operations and that sensitive information is secure.



Figure 1. CREDANT Mobile Guardian Enterprise Edition

CMG Shield for Windows allows organizations to:

- **Reduce risk** with enforced, policy-based on-device security, including mandatory access control, stored data encryption, and data destruction capabilities;
- **Minimize recovery and support costs** by not having to decrypt the complete hard drive which can add hours or days to the recovery process;
- **Ensure compliance** with regulations such as HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, California SB1386 and others by ensuring encrypted data stays protected – even during routine maintenance such as an administrator upgrading existing applications, troubleshooting or simply modifying the local operating system settings;
- **Enable productivity and ease-of-use** with the ability for secure recovery and password reset at all times, whether connected or not; and
- **Leverage investment in existing IT infrastructure** by integrating with enterprise directories such as Microsoft Active Directory and providing the ability to control security for diverse mobile devices from a single console.

Combining the end user's acceptance of security, the ease of IT deployment, its cost-effective long-term management and support capabilities, and the use of CMG Shield for Windows' Intelligent Encryption method to effectively secure data, CMG Enterprise Edition enables organizations to enforce security policies enterprise-wide.

CREDANT Intelligent Encryption

The CMG Shield for Windows' Intelligent Encryption technology reduces overall management, eliminates data corruption and recovery issues, and helps prevent productivity losses associated with full disk encryption, and closes the security gaps created by file/folder-based encryption.

Total Data Protection: four levels of defense

The CMG Shield for Windows Intelligent Encryption process enables a security administrator to easily define rules that govern the application of encryption on a machine. This method is extremely flexible, and can be as simple as defining entire drives or partitions, or as detailed as your environment dictates. Credant's Intelligent Encryption applies a "defense in depth" approach, consisting of the following four levels of defense:

1. **Volume and removable media encryption** automatically encrypts data written to any fixed disk or removable media attached to the machine. Encryption of the operating system is not required, guaranteeing faster recovery time and less impact on performance. And, no integration is required to support strong authentication.
2. **File type encryption** automatically encrypts all new and previously created files of a specified type (or multiple types) regardless of where they are stored on the hard drive. This process ensures protection of legacy data, and temporary and swap files.
3. **Application data encryption** automatically enforces encryption of any data written by applications to protect against user error or malicious renaming of a file type that would leave data exposed. This patent pending approach requires no modification to the application and is transparent to both the application and the user.
4. **User level encryption** automatically enforces encryption of user specific data ensuring that local administrators and other users with machine access cannot access any other users' sensitive data.

This "defense-in-depth" approach of CREDANT Intelligent Encryption provides a significant number of company and user benefits. It provides the protection necessary to secure corporate data, but offers the flexibility and ease-of-use that cannot be matched by older, first generation encryption products:

Minimum Overhead, Maximum Protection

CMG Shield for Windows provides a single security policy which defines any/all of the four levels of encryption and allows all the data files created or owned by a user to be encrypted automatically, wherever the data files are saved on the disk, and whatever their name. This approach means that only the data that needs to be secured is encrypted – no unnecessary encryption of system or program files to slow down system performance. Furthermore, there is no ability for a malicious end user to bypass the encryption process by saving the file into a certain folder, changing the file name, or changing the file extension.

Protecting User and Shared Sensitive Information

Both user information and shared information can be encrypted by CMG Shield for Windows. Shared data can be encrypted and shared between multiple users on a machine, or encrypted for an individual user. The CMG Shield utilizes two separate encryption keys to accomplish this flexibility: a common encryption key and user encryption key. The application of the encryption keys are determined by simple security policy settings that are defined in the administration console (e.g. Encrypt 'My Documents' – applies user encryption key).

In addition, unlike full disk encryption products, this option allows a number of users to share the device, but with each user having their own private data files that only they can read. This option is especially important when the machine needs to be serviced due to a disk fault—technicians are able to read all data on the disk with full disk encryption products. This risky capability isn't so with CREDANT's user and common encryption capabilities—helpdesk personnel can use standard tools to diagnose and fix faults, but the CFO's data always stays secure.

Protecting Temporary Files

Many applications create temporary files during routine file operations. These files are typically stored in undisclosed locations on the hard disk. The CMG Shield provides security policies that enforce the encryption of temporary files and temporary internet files that are saved to disk. Once the CMG Shield is installed, it seeks out these files and automatically encrypts and

protects the contents. Any future temporary files are automatically encrypted as well, ensuring complete protection.

Protecting the Windows Paging (Swap) File

CMG Shield for Windows protects the Window Paging or Swap file to ensure that any sensitive information that is contained in the file is protected.

A unique encryption key is generated each time the PC boots and is used to protect the Paging file for all users. The Paging file is encrypted when not being used by Windows, and is decrypted on the fly when being accessed by Windows.

Protecting the Windows Password

Windows stores a hash (a cryptographically manipulation) of the Windows domain password (which is used to login to the domain and to gain access to a disconnected PC) in the registry. There are several generally available programs, such as LC 5 (formerly known as LOphtCrack) that take advantage of the stored hash to do a brute force attack of the password by generating passwords, calculating their hash and comparing them to the hash stored in the registry. If the two hashes match, the attacker knows that he has the correct password. Another type of attack simply resets the password saved in the registry by booting the computer from a floppy disk or CD and running a simple program.

CMG Shield for Windows protects from these types of attack by removing the hash from the registry and storing it in a secure location protected by CREDANT encryption.

The user would login to their PC using their Windows password which is checked by CMG Shield for Windows. If they successfully login to their device, then the Windows password hash will be decrypted, placed in the registry only when needed by Windows, and then removed and stored securely in a CREDANT encrypted location.

This approach dramatically improves the security of the Windows password mechanism and ensures that the encrypted information stored on the PC cannot be compromised by using tools to determine (or reset) the Windows password; such tools no longer work because the Windows password hash is only available for a short period of time in the registry—WHEN A USER IS ACTUALLY logging in—and is encrypted the rest of the time.

Enhancing Windows Access Control

Data access and the encryption process are controlled with a CREDANT-enhanced Windows login process. CREDANT provides two modes of the enhanced Windows login process: a full GINA replacement and a GINA-less option.

Enterprises that are looking to implement strong two-factor authentication with a PKCS11 smartcard, RSA SecurID for Microsoft Windows, biometric authentication, or another authentication mechanism can use the GINA-less option. This option provides seamless integration with the Windows login process without modifying or associating with the Microsoft GINA. Your existing GINA replacements will continue to work with the CMG Shield installed and operating in this mode. Furthermore, end users are not required to login twice using this option. Once the user has successfully authenticated to Windows using the strong authentication, the necessary authentication credentials are automatically passed to the CMG Shield giving the user access to the encrypted data.

Enterprises that do not have a preferred authentication mechanism in house and are looking for a stronger, more secure authentication process than the Windows login can use the CREDANT GINA replacement option (**Figure 2**). The login process looks and acts like the standard Windows login procedure, but uses a patent-pending approach to protect the user's Windows

password hash and encryption keys until the user successfully logs in. Upon successful login, the active user's encryption keys are unlocked. Encrypted files are then ready to be decrypted on-demand as needed.



Figure 2. GINA Replacement Option Offers Enhanced, Patent-Pending Windows Access Control

The GINA-replacement option offers a self-service password reset capability to ensure that users can always gain access to their device, even if they have forgotten their Windows password and aren't connected to the network. The user merely answers the question they selected during the initialization process and are then allowed to reset their Windows password, without calling the help desk or having a network connection. In the event this procedure fails, the user can call the help desk for an over-the-phone password recovery using a secure challenge/response recovery mechanism (**Figure 3**). The use of this challenge/response procedure ensures that users are always productive by enabling them to immediately regain access to their PC while traveling, without requiring them to connect to the Windows domain controller.



Figure 3. Help Desk Password Recovery to Regain Immediate, Secure Access

In both modes of enhanced Windows login, only the encryption keys for the active user are unlocked upon successful authentication. Because individual users have individual encryption keys, users are unable to access another user's private information, allowing multiple people to share the same computer securely without sharing passwords and without having access to others' private information.

Both modes provide seamless help desk recovery capabilities in the event a user has forgotten their password. The GINA-less option follows the normal Windows recovery model. An end user calls the help desk and has the password reset on the domain controller by an administrator. Upon the next login, using the new domain password, the CMG Shield will automatically detect that the user has successfully authenticated to Windows and will perform an automated and transparent HTTPS based challenge/response recovery with the CMG Enterprise Server. The end user will not notice this process and, within a very short time after login, will have access to all encrypted data.

In summary, CMG Shield protects Windows password and removable media, and all sensitive information stored on a mobile PC such as a notebook or tablet, or on a desktop PC. The CMG Shield provides flexible authentication mechanisms that allow enterprises to use strong two-factor authentication products, existing GINA replacements, or the CMG Shield GINA replacement for added protection.

Protecting Removable Media

More and more users are employing USB thumb drives, portable media players (e.g. iPods), and other low-cost data backup devices. Use of these portable media represents a significant security hole in many solutions designed to only protect data at rest on a disk drive. All it takes for a security breach, is one connection of the USB cable and end users easily can transfer millions of bytes of sensitive data and transport within an unprotected state outside the walls of the enterprise.

CREDANT provides easy to configure security policies to allow administrators to specify exactly what happens to data when it's copied to any kind of removable media. Administrators have the option to set a security policy called "Encrypt Removable Media", which ensures that all user data written to any removable media will be encrypted. They can also specify a "Scan Removable Media" policy, which forces all existing data on removable media to be encrypted upon insertion to a CREDANT protected machine. In addition, any data encrypted on removable media will be encrypted with the user's roaming credentials (encryption key). Controlled by policy, this feature enables companies to contain the use of USB drives within the company while maintaining maximum portability and confidentiality. Roaming Credentials permit encrypted data to be read on any CREDANT protected machine in the enterprise once the end user logs in—an ideal situation for the user who needs to do a PowerPoint presentation on another computer.

For enterprises that are looking to provide their end users with the maximum flexibility in transferring data, CREDANT also provides a built-in encryption option, CREDANT2go (added to the SendTo menu), which allows a user to create self-extracting encrypted archives of one or more files. CREDANT2go produces an executable file that can be run on any Windows machine regardless of whether or not CREDANT is installed. This feature is especially useful if files need to be sent to other users that are not part of the enterprise, if files need to be archived on a separate system, or if an end user needs to take a file to a home office machine to work.

Recovering Encrypted Data

One of the challenges with any type of data security solution is how to recover data if the encryption keys are lost. The simple answer is that if the keys are lost, then the data is lost too. It is, therefore, imperative that every precaution is taken to securely protect the keys.

Unlike competitive products, all encryption keys are generated and securely escrowed by the CMG Enterprise Server before being passed down to the device, thereby ensuring the keys can never be lost.

Other solutions generate the keys on the device, requiring the end user to manually store them on a separate device (i.e., floppy) or initiate an out of band process to store them centrally (e.g. copy the encryption keys to a network drive). The problem with these approaches is that immediate recovery of the encryption keys is not guaranteed and is left up to the control of the end user. If the end user loses the recovery device (i.e. floppy) or the encryption keys are never sent back (e.g. stored on a network drive), then recovery of encrypted data may not be possible. From an enterprise's point-of-view, this risk is significant and unnecessary.

With CREDANT, recovery of encrypted data can always be done, from the time the first bit of data is encrypted until the machine's end of life. Keys are generated and escrowed on the server, then passed to the device. Recovery is automatically facilitated and does not require repeated decryption and encryption, and is completely transparent to the end user.

CONCLUSION

CREDANT Mobile Guardian (CMG) was specifically designed to provide mobile data security with the least possible impact on the user experience. CREDANT Mobile Guardian Shield (CMG Shield) for Windows, a component of CREDANT Mobile Guardian, helps protect your brand and ensure regulatory compliance by securing valuable information on notebooks and desktops against loss, theft and unauthorized use. The CMG Shield for Windows encryption process is automatic, with all data remaining encrypted when not in use. This approach to encryption is far superior to the more antiquated solutions on the market today. CREDANT's patent-pending Intelligent Encryption process uses four levels of defense to enforce the protection of vital information no matter where it is stored, yet avoids the data corruption, productivity losses and back-end costs associated with full hard disk encryption and fills the security gaps left by file/folder-based products. **Table 1** (p. 13) presents a compact overview of Credant Intelligent Encryption compared to other encryption approaches.

Table 1. Comparing and Contrasting CREDANT Intelligent Encryption with Full Disk Encryption, and File/Folder-Based Encryption

Manageability	CREDANT Intelligent Encryption	Full Disk Encryption	File/Folder-Based Encryption
Centralized administration for all mobile platforms	Yes	No	No
Integrates with LDAP/ Microsoft AD so administrators don't have to manually define users/groups	Yes	Some	Some
Will work on all computers regardless of BIOS, hardware, and installed programs	Yes	No	Yes
Works with software deployment tools (e.g. SMS, Marimba, Tivoli, etc.)	Yes	Yes	Yes
Detect and report handheld usage across Windows platforms	Yes	No	No
Enables enterprises to enforce encryption of only sensitive data based on simple encryption settings	Yes, Intelligent Encryption	No, entire hard disk is encrypted	No, only folders and/or files
Support multi-user environment with user and shared encrypted data functionality	Yes	No	Some
Provides a flexible deployment scheme where full data protection can be turned on over time and not all at once	Yes	No	No
Recoverability	CREDANT Intelligent Encryption	Full Disk Encryption	File/Folder-Based Encryption
Requires decryption of the entire disk drive to restore the operating system or recover end user data	No	Yes	No
Self-service password recovery	Yes	Some	No
Modifies the Master Boot record making system recovery more complex	No	Yes	No
Secure Key Generation and Escrow	Yes Keys are generated and escrowed on the server, then passed to the device	No Keys are generated on the device and must be manually escrowed	No Keys are generated on the device and must be manually escrowed

Table 1. Comparing and Contrasting CREDANT Intelligent Encryption with Full Disk Encryption, and File/Folder-Based Encryption (cont.)

Security	CREDANT Intelligent Encryption	Full Disk Encryption	File/Folder-Based Encryption
Enforces automatic encryption for external storage devices	Yes	Some, but may be a separate product	Some, but may be a separate product
Prevents access to encrypted data during routine maintenance by administrators	Yes	No	Some
Encrypts swap file	Yes	Yes	No
Encrypts Windows password hash preventing brute force attack	Yes	Yes	No
Encrypts temporary files	Yes	Yes	No
Securely overwrites clear text residual	Yes	Yes	No
FIPS 140-2 Validated	Yes	Some	Yes
Supports Two-Factor Authentication	Yes	Some	Some
Control and secure handhelds across Windows platforms	Yes	No	No
Usability	Intelligent Encryption with CMG Shield for Windows	Full Disk Encryption	File/Folder-Based Encryption
Requires minimal end user training	Yes	Yes	No
Requires end user to be encryption aware	No	No	Yes
Requires pre-boot authentication adding an additional password	No	Yes	No
Encryption transparent to end user	Yes	Yes	No

Contact Us

More information, including data sheets, case studies, analyst reports and additional business and technical white papers are available in the CREDANT Technologies Resource Center (registration required): www.CREDANT.com/login.php. Please let us know how we can help meet your Windows and mobile device security needs:

CREDANT Technologies

15303 Dallas Parkway, Suite 1420

Addison, Texas 75001

1-866-CREDANT (273-3268) or 972-458-5400

www.CREDANT.com

info@CREDANT.com

This white paper is not intended to take the place of informed legal counsel. The information and recommendations contained herein are for informational purposes only, and should be expanded upon by trusted legal sources. For specific advice about formulating an information security policy that is compliant with current laws and regulations, or for further information about complying with information security laws, it is recommended that you seek professional counsel.

© 2006 CREDANT Technologies, Inc. All rights reserved. CREDANT Technologies, CREDANT, the Be Mobile Be Secure tagline, the CREDANT logo are, or will be, registered trademarks of CREDANT Technologies, Inc. All other trademarks, service marks, and/or product names are the property of their respective owners. Product information is subject to change without notice.