CREDANT® TECHNOLOGIES
Be mobile. Be secure.

CREDANT® Mobile Guardian®
Technical Brief

Policy-Based Intelligent Encryption

CREDANT’S next-generation, Policy-Based Intelligent Encryption technology delivers the protection necessary to secure corporate data no matter where it is stored, yet offers the flexibility and ease-of-use unmatched by older, first generation encryption products. This new encryption method enables a security administrator the flexibility to easily define rules that govern the application of encryption on devices, rules that can be as simple as defining entire drives or partitions, or as detailed as the environment dictates. Policy definition is simple yet powerful, and encryption is enforced transparently, without changing the way users interact with their systems.

Four Levels of Defense:

Tighter Security, Easier Management, Greater User Acceptance

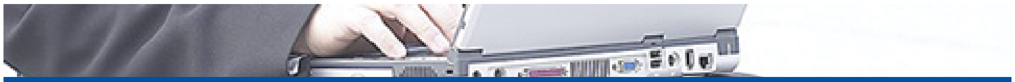
1. **Volume and external media encryption** automatically encrypts data written to any fixed disk or removable media. Encryption of the operating system is not required, guaranteeing faster recovery time and less impact on performance. All data on external media is encrypted with special encryption keys to ensure end user access to the data from any CMG Shield protected device.

2. **File type encryption** automatically encrypts all new and previously created files of a specified type or types, including temporary and swap files, regardless of where they are stored.

3. **Application data encryption** automatically enforces encryption of any data written by heavily used business 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 code base. Administrators simply define a list of application executables, and the CMG Shield automatically monitors any files created by these applications and saved to disk.

4. **User level encryption** enables set policies that force encryption of data for individual users who share a notebook computer or workstation. The administrator can also specify common encrypted locations accessible to all authorized users, ensuring access by multiple authorized users on the same machine while user-specific data remains protected.

- Secures data no matter where it is stored, including external media, paging files, password hash and temporary files and folders.
- Enables flexible definition of security policies, depending on the needs of the enterprise environment.
- Is transparent to end users, balancing security with usability.
- Does not encrypt operating system or application files, utilizing existing support processes and preventing increased support costs and risks of exposure to confidential data.
- Does not replace or alter the Master Boot Record and therefore guarantees interoperability with existing applications.
- Prevents local administrator access to encrypted data
- Enables easy and immediate data recoverability.
- Allows multiple users to securely share information on the same desktop or laptop, yet still allows individuals to access data permissible only to them.
- Enables administrator to encrypt in-use applications, force application requests to wait until initial encryption is complete, or delay initial encryption upon policy changes.
- FIPS 140-2 validated AES 128 and AES 256.



CREDANT Mobile Guardian (CMG) Enterprise Edition is the only truly integrated, centrally managed policy-based mobile data security and management solution protecting the broadest number of mobile device platforms. Because mobile device operating systems differ across varying device platforms, there are some functional differences in how CREDANT Policy-based Intelligent Encryption technology operates across handhelds (PDAs, Pocket PCs, smartphones) versus Windows-based devices.

Note: for additional information on CMG and Policy-based Intelligent Encryption, refer to CREDANT published whitepapers.

Handhelds and Smartphones

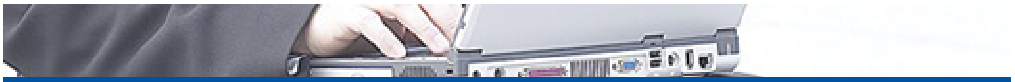
CMG can be configured to encrypt all PIM databases, third party application databases, and email databases including attachments, media files, and information stored in My Documents. For example, CMG Shield for Pocket PC also allows the administrator to create a "secured" folder on the device or on removable media. When the mobile user turns on the device and authenticates to CMG Shield, none of the data is decrypted. When the user requests a specific database or file, the CMG Shield decrypts that information "on-the-fly" so information remains encrypted at all times, except when actually in use by an authorized user.

Windows Laptops, Tablet PCs, Desktops and External Media

CREDANT Intelligent Encryption technology for Windows-based devices fills the security gaps left by file-folder based encryption products and avoids the management, data recovery, security and productivity issues associated with full, or hard disk encryption methods. The CMG Shield for Windows provides a single security policy that defines any/all of the four levels of encryption, both user and shared information, and allows all the data files 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.

Easy and Immediate Data Recovery: Automatic Key Escrow

One of the challenges with any type of data security solution is how to recover data if the encryption keys are lost. Unlike competitive products, CREDANT's key escrow process is completely automated and transparent. All encryption keys are generated and securely escrowed on the CMG Enterprise Server before being passed down to the device, thereby ensuring the keys can never be lost. Recovery is automatically facilitated and does not require repeated decryption and encryption, and is completely transparent to the end user. The CMG Shield utilizes two separate encryption keys to accomplish this flexibility: a common encryption key and user encryption key. Temporary and Windows Paging, or Swap, files are also automatically encyrypted. The Windows password hash is stored securely in an encrypted location when not in use, dramatically improving the security of the Windows password mechanism and ensuring that the encrypted information stored on the PC cannot be compromised.



Windows Laptops, Tablet PCs, Desktops and External Media (cont.)

Encrypting Temporary and Paging Files, Password Hash

Temporary and Windows Paging (Swap) files are also automatically encrypted. Many applications create temporary files during routine file operations, files that are typically stored in undisclosed locations on the hard disk. Once the CMG Shield is installed, it seeks out these files and automatically encrypts and protects the contents. For the Windows Paging, or Swap file, a unique encryption key is generated each time the PC boots. The Paging file is encrypted when not being used by Windows, and is decrypted on the fly when being accessed by Windows.

Windows stores a hash (a digital fingerprint) of the Windows domain password (which is used to log in to the domain and to gain access to a disconnected PC) in the registry. When the Windows password hash is not it use, it is stored securely in an encrypted location, dramatically improving the security of the Windows password mechanism and ensuring that the encrypted information stored on the PC cannot be compromised.

User and Shared Sensitive Information

Encrypted data can be shared between multiple users on a machine, but the individual user may also have private data files that only he or she can read. This flexibility is accomplished by the CMG Shield utilizing two separate encryption keys: a common encryption key and user encryption key. This feature is especially important when the machine needs to be serviced — with FDE products, technicians are able to read all data on the disk, whereas this risk is avoided with both user and common encryption capabilities.

External Media

CMG automatically encrypts data written to any fixed disk or external media attached to the CMG-protected Windows device (Figure 1). Easily configurable security policies allow administrators to specify exactly what happens to data when it's copied to any kind of external media. Additionally, 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.

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.

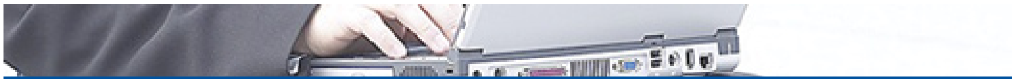
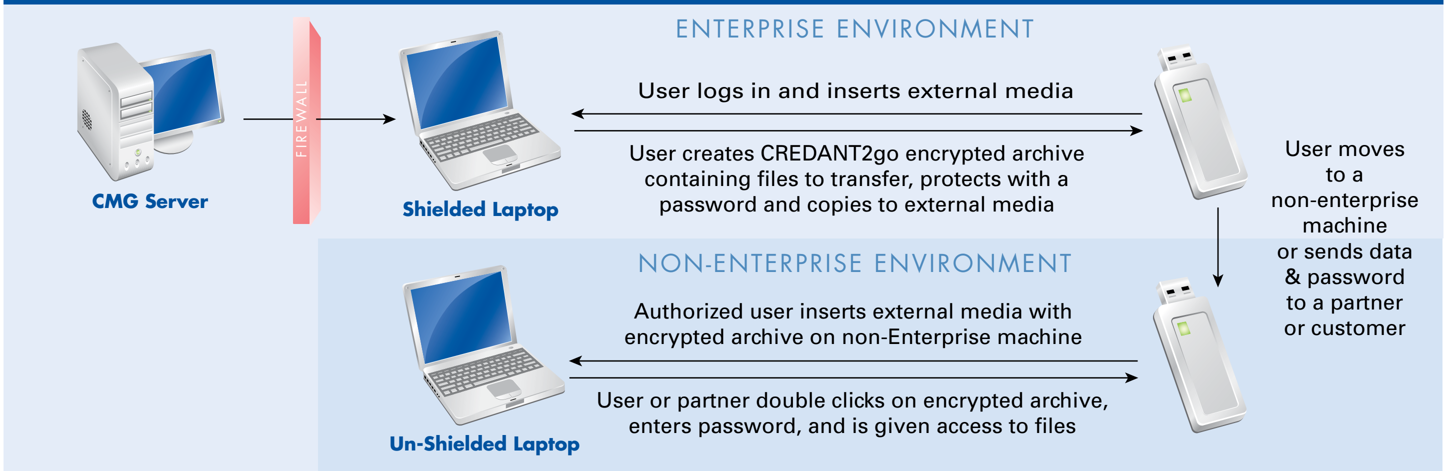


Figure 1. Data Portability and Protection Beyond the Enterprise


ENTERPRISE ENVIRONMENT
CMG Server
FIREWALL
Shielded Laptop
User logs in and inserts external media
User creates CREDANT2go encrypted archive containing files to transfer, protects with a password and copies to external media
User moves to a non-enterprise machine or sends data & password to a partner or customer
NON-ENTERPRISE ENVIRONMENT
Authorized user inserts external media with encrypted archive on non-Enterprise machine
User or partner double clicks on encrypted archive, enters password, and is given access to files
Un-Shielded Laptop

FIPS Validation

CMG supports a variety of industry standard encryption algorithms, including AES 128, AES 256, 3DES, and Blowfish. CREDANT has achieved FIPS 140-2 Level 1 validation for the CREDANT Cryptographic Kernel (CCK), which is used by the CMG Shield across all CREDANT supported platforms. Implementation of the AES, 3DES, SHA-1, HMAC-SHA-1, and RNG algorithms are all FIPS approved.

Summary

Unlike older, outdated encryption technology, CREDANT's patent-pending Policy-based Intelligent Encryption, with a four-layered defense approach, provides critical business controls that ensure data is always secure across a broad range of devices — handhelds, smartphones, laptops, tablets, desktops and external media — while enforcing security policies that are flexible, easily controlled and transparent to the end users. CREDANT Mobile Guardian was specifically designed to provide mobile data security with the least possible impact on the user experience. And, because CMG is not concerned with operating system or program files, the same support procedures that companies have been using for years will still apply, with no increased support effort, cost, or risk of exposing confidential data.

Policy-based Intelligent Encryption also supports multi-user and shared computer environments, allowing each user access to the data they are authorized to access. Furthermore, with CMG, all encryption keys are centrally generated and securely stored automatically on the server, freeing end users from having to manually store encryption keys on a separate device or use some out-of-band process to store keys centrally. For additional information on CMG and its encryption technology, refer to CREDANT published whitepapers.