



# Full Data Encryption<sup>2</sup>

CREDANT Mobile Guardian's Policy-based Intelligent Encryption technology delivers Full Data Encryption for laptops, desktops, handhelds and external media. Enterprises can now implement the thorough protection needed to secure their corporate data no matter where it is stored, yet have the flexibility and ease-of-use not found in older, first-generation encryption technologies, such as full disk and file/folder encryption. With CREDANT Intelligent Encryption, a security administrator can easily establish and enforce policies governing the application of encryption on all mobile endpoints. Policies can protect entire drives or be more granular to control certain file types for a particular user or group — whatever the environment dictates. Policy definition is simple yet powerful, and encryption is enforced transparently, without changing the way users or IT administrators interact with their systems.

| <b>CMG Full Data Encryption<sup>2</sup></b>   |   |
|---|---|
| Five Levels of Policy-based Intelligent Encryption for Tighter Security, Easier Management, Greater User Acceptance |   |
| PRIVACY   | <p><b>User Data Encryption</b><br/>Protects each user's data from being accessed by any other user, authorized or not; guards against even insider threats</p>                  |
|   | <p><b>Application Data Encryption</b><br/>Protects all data written by specified applications, irrespective of where/how the data is written</p>                                |
| COMPLIANCE  | <p><b>External Media Encryption</b><br/>Protects data written to external media such as a USB stick, external drive, iPod, SD card, CD/DVD, etc.; fights data leakage risks</p> |
|   | <p><b>Common Data Encryption</b><br/>Protects data from being accessed by an unauthorized user</p>  |
|   | <p><b>System Data Encryption</b><br/>Protects data on a hard disk that is not protected by other encryption layers</p>  |

## With CMG Full Data Encryption<sup>2</sup>, you get:

- More security benefits than Full Disk Encryption and without the operational limitations.
- Security, manageability and flexibility that surpasses file/folder encryption.
- Automatically secure data no matter where it is stored.
- Protection for all sensitive data, including local and domain credentials, paging files, and temporary files and folders.
- No replacement or alteration of the master boot record, therefore avoiding interoperability issues with existing applications.
- Administrative proof of data that is encrypted and in compliance.
- Transparency for end users; offers unique usability features to ease adoption.
- No need for pre-boot authentication, which complicates operations.
- Routine maintenance enabled by IT personnel without exposing sensitive data; local administrators are blocked from accessing encrypted data owned by other users.
- Automated encryption key escrow provides guaranteed data recoverability from the moment encryption begins.
- User-specific encryption policies ensure that only the owner of the data can access information, even while allowing multiple users to share the same computer.
- A platform to manage future, data-centric solutions.
- FIPS140-2 validation.

## Overview

Unlike older encryption technologies, CREDANT's Policy-based Intelligent Encryption delivers a multi-layered encryption approach that provides comprehensive, critical business controls to ensure data is always within compliance. This layered technology fits nicely into a phased security implementation, and can be especially helpful for enterprises that prefer to roll out security methodically to minimize the impact on users, or for those who have different security policy requirements by user role or department.

Because portable and 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 and Smartphones) versus Windows computers.

## Windows Laptops, Tablet PCs, Desktops

CREDANT Intelligent Encryption technology for Windows computers fills the security gaps left by file-folder based encryption products while avoiding the management, data recovery, security and productivity issues associated with full (FDE) or hard disk encryption solutions. The CMG Shield for Windows is driven by security policies that enforce any or all of the five levels of Intelligent Encryption and allows all sensitive data to be encrypted automatically, wherever that data is saved. CREDANT recently added System Data Encryption (SDE) for securing data-at-rest on Windows computers. SDE provides the encryption simplicity associated with Full Disk Encryption technologies, but without the headaches associated with such an outdated approach. SDE Intelligent Encryption ensures that all sensitive data within the operating system is encrypted without affecting system performance and complicating essential IT operations and system maintenance processes.

### Easy and Immediate Data Recovery: Automatic Key Escrow

One challenge for any data security solution is how to recover data if the encryption keys are lost. Unlike competing products, CMG's key escrow process is automated, transparent to the end user and ensures that data is never encrypted until keys have been properly escrowed. Data is recoverable by the CMG administrator from the moment the first bit of data is encrypted, and does not require sending the system to a third party or the use of special tools.

Intelligent Encryption utilizes multiple encryption keys for each protected system. Unlike older encryption technology, this process architecture enables CMG's user- and data-specific protection, which restricts sensitive data access so that Local administrators and other users who may require access to the system can do their job without compromising protected data. All of CMG's encryption keys are automatically and securely archived at the CMG Server to ensure that keys are never lost and are easily accessible if data recovery is ever necessary. *(See System Data Encryption Technical Brief for more information on System Data Encryption key generation and recovery.)*

**Windows Laptops, Tablet PCs, Desktops (cont.)**

**Encrypting Temporary Files, Paging Files and Windows Credentials**

Simple policies enable automatic encryption of files created by the Windows operating system and various applications, including temporary files and Windows paging, or swap, files. Applications often create temporary files, which can contain sensitive information, and stores them in a variety of locations on the hard disk. CREDANT's Intelligent Encryption seeks out these files and automatically encrypts them, thus ensuring total protection of all sensitive information.

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.

The Windows local and domain logon credentials are protected by encrypting the local SAM Database and the domain password cache in the registry. This protection dramatically improves the security of sensitive data by reducing the risk that the Windows logon mechanism can be compromised, particularly for offline attack scenarios.

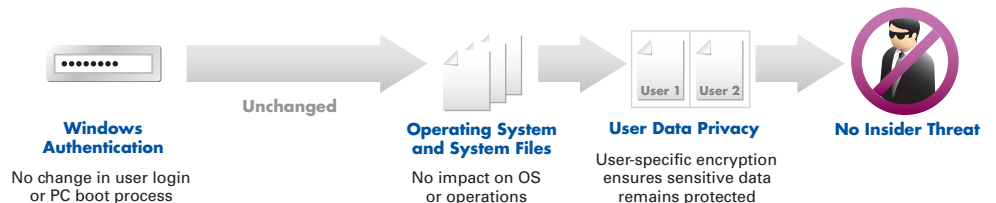
**User- and Data-specific Encryption**

CREDANT's user- and data-specific encryption, via multiple encryption keys, transparently encrypts data while allowing flexible and secure access to encrypted data. Simple CMG policies can be defined so that all authorized users on a computer have access to all encrypted data. For heavily regulated environments, administrators can define policies so that multiple users can share some encrypted data while other encrypted data is available only to the user who created it. This is an important and unique security function that older encryption technologies are unable to offer. Such granular control over access to sensitive, encrypted data is essential in environments where multiple users may work on a single computer yet, but where some of those users may also have private data. Furthermore, this segmentation of data access allows IT professionals to perform normal system maintenance without exposing sensitive information that they should not have access to, such as financial or human resources data. Companies that outsource their IT are especially vulnerable when all data is available to any user logged into the system, as is the case with older encryption technologies, such as FDE.

**Full Disk Encryption**



**Full Data Encryption2**



## 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. When the mobile user turns on the device and authenticates to the CMG Shield, data remains encrypted on the device. As the user requests a specific database or file, the CMG Shield decrypts that information “on-the-fly;” therefore, this information remains encrypted at all times, except when actually in use by an authorized user.

## External Media

The CMG External Media Shield (EMS) provides automatic encryption of data on external media, including CD/DVD media, tablet PCs, USB flash drives, iPods and MP3 players, or handheld devices. When an unprotected removable storage device is inserted into the protected computer or handheld for the first time, the user is prompted to Shield that media device and set a password restricting any future access to it. From this point forward, the device is password protected and all data added to it is automatically scanned and encrypted per Intelligent Encryption policies. Administrators can establish policies to encrypt all data or allow encrypted and non-encrypted data to coexist—a critical option due to the ever increasing popularity of device use for personal content like audio and video files. *(For more information, see CMG External Media Shield Technical Brief.)*

## 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 outdated encryption technologies, such as full disk (FDE) and file/folder encryption, CREDANT’s Policy-based Intelligent Encryption provides comprehensive controls to ensure data is always secure across a broad range of devices without compromising IT operational processes or security. This five-layered approach protects handhelds, smartphones, laptops, tablets, desktops, CD/DVD media, USB flash drives, iPods and other portable storage devices, while enforcing security policies that are flexible, easily managed and transparent to the end users. Intelligent Encryption also supports multi-user and shared computer environments, allowing each user to work with only the data they are authorized to access. Furthermore, CREDANT’s automated and transparent key escrow process allows organizations to accomplish quick and easy data recovery without sacrificing security or increasing their operational costs. CREDANT Mobile Guardian was specifically designed to provide rigorous mobile data security and proof of encryption with the least possible impact on user experience or existing IT maintenance and operations processes, and with no increase in support effort, cost, or risk of exposing confidential data.

|                      |   |   |                 |                       |
|----------------------|---|---|-----------------|-----------------------|
| CREDANT Technologies | 15303 Dallas Parkway, Suite 1420,<br>Addison, Texas 75001 USA | 866-CREDANT (273-3268)<br>or 972-458-5400 | www.credant.com | info_emea@credant.com |
|----------------------|---|---|-----------------|-----------------------|