

CREDANT Mobile Guardian Key Management Overview



This paper provides an overview of the different types of encryption keys used within the CREDANT Mobile Guardian solution for Windows[®] based devices.

MULTI-KEY ARCHITECTURE

One of the main differences between CREDANT Mobile Guardian and first-generation Full Disk Encryption solutions is the ability to go beyond “power off” protection by providing additional layers of protection for external and internal threats. This is based on CREDANT’s multi-key architecture, where up to three different keys per user can be employed to encrypt and protect data. While providing added security, the multi-key architecture still delivers a transparent end-user experience and administrative overhead is kept to a minimum. All encryption policies are set by the administrator through CREDANT’s web-based console and cannot be circumvented or altered by the end-users, regardless of how files are altered or moved.

COMMON KEY

The Common Key is the most widely used level of encryption and is used to lock down data and make it only available to CREDANT managed domain users. There is one Common Key per device and it is only released for use once a valid CREDANT-managed domain user logs into the machine. This ensures that the data on the device is still protected and cannot be compromised by various security attacks, even if the device is at the Windows login prompt.

A typical Common Key policy will exclude non-sensitive data such as OS and program files. This allows a local admin to log into the PC and service and maintain the OS without getting access to any sensitive data. However, a domain admin may be able to log in and access all files on the device for those organizations that require administrative access to file content.

USER KEY

User Key encryption can be optionally layered on top of (i.e. take precedence over) Common Key encryption and allows only the user who generates or saves the file the ability to access that file. This is typically used with users who have highly sensitive data such as executives, human resources, or finance departments. A typical User Key encryption policy would be to encrypt a user’s profile so that not even a domain administrator would be able to access the content of a user under this policy. This type of encryption can be used to thwart intentional or inadvertent internal threats and to enforce a “right-to-know” policy in the organization. There is one User Key per user and the User Key is only released once the associated CREDANT-managed domain user logs into the machine. However, in the event that a user leaves the company or a forensics audit is required, CREDANT provides an administrative utility to access all data on a machine. The administrator would require elevated administrative privileges that would be set in the CREDANT web console in order to use the utility and access the keys for decryption. This access would also be logged and auditable.

SYSTEM DATA KEY

System Data Key (SDE) encryption is the final layer of encryption and is typically used to encrypt anything not covered by Common Key or User Key encryption policies—most notably the OS and Program files. The majority of CREDANT’s 1000 enterprise customers choose not to encrypt the OS and executables, resulting in reduced performance overhead, but the SDE key can nonetheless be used to encrypt such files with a flick of a switch in the web console.

CREDANT Mobile Guardian Key Management Overview



The SDE key also provides protection against miscellaneous attack vectors such as encrypting the SAAM database, password hashes, paging files and registry. There is one SDE key per device. SDE key authentication occurs only when certain conditions are met. This includes integrity verification of a variety of hardware and software parameters preventing a hacker, for example, from removing the drive and placing it into another PC to access the encrypted data or hack the registry to execute an injection attack.

MULTI-KEY ARCHITECTURE SUMMARY

CREDANT provides multiple layers of security to protect against different kinds of threats while maintaining the operational benefits of not having a pre-boot password or breaking IT processes such as patch management. The different layers of encryption can be set up so that any data not specified to be encrypted with the User Key is encrypted with the Common Key, and any data not specified to be encrypted with the Common Key is in turn encrypted with the System Data Key.

The combination of Common Key, User Key and System Data Key encryption also offers a would-be hacker a much more daunting task to try to hack a user's data compared with the single key architecture of legacy Full Disk Encryption solutions as they may need to try to hack multiple keys to gain access to any or all data.

KEY ESCROW AND MANAGEMENT

CREDANT generates Common and User encryption keys at the enterprise server using an ANSI X9.31 compliant random number generator. Keys are generated automatically in response to an activation request from a client device. The process requires no user or administrator involvement. The SDE key is generated on the client using a similar method, and then automatically escrowed to the server at activation.

Recovery is of paramount importance when encrypting data, and the keys are the most important element to recovery. CRE DANT automatically escrows all keys to the CRE DANT database before any encryption occurs on the clients, guaranteeing that the keys are available for recovery as long as the database is properly protected and backed up.

The keys themselves are encrypted within the database and in any process, whether that be storage in the database, storage on the clients, during the transport of keys, or during download for recovery. The key material is never made directly accessible to a user or admin, but is instead wrapped in a bundle that can only be opened through proper authentication. Keys are managed within the database and distributed to clients, the administrative utility, and administrators for offline operations by the CRE DANT Enterprise Server so no third party key management is necessary. CRE DANT is compliant with FIPS 140-2 Level 2, Common Criteria EAL 3 and the Government quality C E S G Claims Tested Mark (CCTM).