

CREDANT Solutions for BITS Compliance

Data security depends on the safety and soundness of IT products.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) ensures that BITS encryption and security requirements are consistently and efficiently enforced – regardless of where the data resides.

Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

CMG's Intelligent Encryption provides centrally managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:

- › Ensure data security without the risk of users placing data in areas that are not encrypted.
- › Provide confidentiality, privacy and auditing of data residing on any endpoint.
- › Protect sensitive data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

BITS, the business strategy and technology group for The Financial Services Roundtable, was formed by the CEOs of the largest financial institutions in the U.S. The BITS Product Certification Program was created by financial IT experts, together with technology providers and other stakeholders. It serves as a proactive means to improve the safety and soundness of the products used by leading financial institutions and to help them make informed technology decisions.

To earn the BITS Tested Mark, products undergo an evaluation process by independent, third party testing facilities to assure conformance to the program's security criteria.

The compliance challenge

The BITS Product Certification Program (BPCP) collaboratively addresses security challenges by providing a mechanism for testing software used in the industry. The BPCP is also an important self-regulatory measure, helping to mitigate technology risk and protect the nation's critical infrastructure.

BPCP criteria represent the minimum baseline security features and functionality of various types of commercial software products. Criteria are developed for certain classifications of products based on function and application.

Compliance is based on several criteria, profiles and specifications. Master Security Criteria define the overall security requirements and functions that are expected in all classes of products. Products with similar functions and applications are grouped into a product class. Product Security Profiles are more specific security requirements applicable to that product class but are derived from, and consistent with, the requirements in the master security criteria. Product Specific Security Test Plans and Test Scripts define the actual testing strategy and supporting test cases for a product submitted for testing by the vendor. The testing is designed to measure compliance with the applicable product security profile.

CREDANT

More than 700 enterprises and government agencies -- including 50 of the Global 500 -- rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.