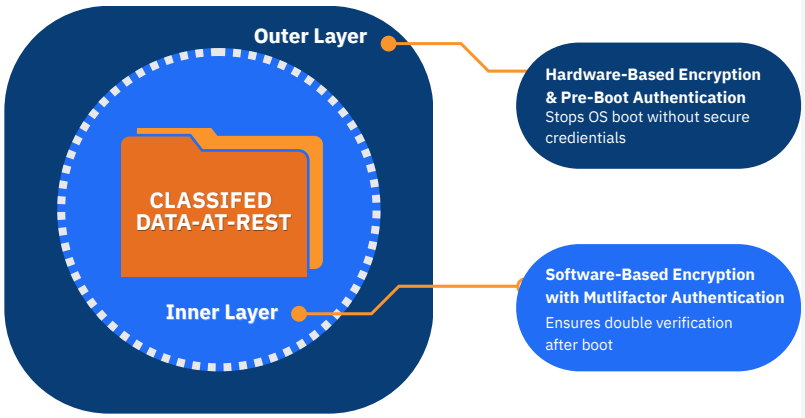
Cigent **PBA Data Sheet**

NSA CSfC-Compliant Outer Layer Protection

Cigent Pre-Boot Authentication (PBA) secures mission-critical data by combining Hardware Full Drive Encryption (HW FDE) with a secure pre-OS boot authentication environment to deliver the outer layer solution required under the NSA's CSfC Data at Rest (CSfC DAR) capability package. Employing quantum-resistant AES 256-bit encryption, Cigent PBA ensures comprehensive protection for classified and sensitive information against unauthorized access and potential breaches.

The solution complements Software Full Drive Encryption (SW FDE) to provide a complete dual-layer solution to meet CSfC DAR guidelines. Additionally, Cigent PBA can be independently deployed, offering secure hardware-level encryption and pre-boot authentication in environments where full CSfC implementation is not required.

CSfC for DAR Protection



Key Features:

- **Meet CSfC DAR Requirements:** Cigent Pre-Boot Authentication (PBA) with certified Hardware Full Drive Encryption (HW FDE) provides NSA CSfC-compliant outer-layer encryption required by the NSA's Data at Rest (DAR) Capability Package.
- **Multi-Factor Authentication Ready:** Supports single and multiple authentication factors including username/password, smartcards (PIV), and Security Keys ensuring comprehensive and robust authentication aligned with federal standards.
- **Independent Layered Protection:** Operates independently from software encryption solutions, ensuring the cryptographic and functional isolation mandated by CSfC architectural requirements.
- **Administration at Scale:** Command line interface provides management of PBA with ability to integrate into existing enterprise management.
- **Wide Device Compatibility:** Supports deployment on various endpoints including Intel/AMD/ARM (NVIDIA Jetson Orin) laptops, desktops, workstations, and servers.

CIGENT
AlwaysPROTECTED™

PROTECTED DATA AT THE EDGE

Protecting your data, enabling your mission

Cigent PBA is NIAP-listed on the NSA's CSfC DAR component list and is integrated into Cigent Secure Storage drives, providing a simplified, single-vendor outer-layer solution. While designed to seamlessly integrate with Cigent drives for optimal ease of deployment, Cigent PBA remains fully compatible with other CSfC-certified drives.

Its CSfC-certified HW FDE utilizes independent and distinct cryptographic libraries from Cigent Software FDE, satisfying the NSA's CSfC Data at Rest (DAR) manufacturer diversity requirement. Cigent's flexible architecture allows Cigent PBA to be implemented either independently as the outer encryption layer or paired seamlessly with Cigent or third-party SW FDE solutions as the inner encryption layer, delivering a complete, dual-layer CSfC-compliant encryption strategy.

A Complete CSFC for DAR Solution

Cigent PBA can be deployed alongside Cigent FDE as complementary, independently operating solutions to deliver both the inner and outer layers required by the NSA's CSfC Data at Rest (DAR) Capability Package. This combination forms a complete solution for meeting CSfC's dual-layer encryption mandate.

Each layer operates independently, with no crossover in cryptographic libraries or functional roles, ensuring full compliance with CSfC architectural separation requirements. The result is a highly flexible deployment model that reduces complexity while assuring compliance.

By sourcing both layers from Cigent, organizations can simplify procurement, accelerate deployment, and ensure compatibility, all while meeting the most stringent security standards set by the NSA.

How Cigent FDE Secures Your Data

Cigent PBA safeguards sensitive data through robust hardware-based encryption, enforcing pre-boot authentication as mandated by the NSA CSfC DAR Capability Package. This ensures compliance and protection of mission-critical data at rest.

1. **Device Powered Off:** All data remains encrypted, unreadable, and inaccessible.
2. **Pre-boot Authentication**: Upon powering the device, authentication via supported methods including username/password, smartcards (PIV), or Security Keys is required prior to the operating system boot sequence, establishing secure access controls before any data is decrypted.
3. **Authentication Boot**: Once authentication is successful, the operating system boots, and the drive's encrypted data becomes accessible to the authorized user.

Schedule a Demo

See how Cigent keeps you AlwaysPROTECTED.

Book a Demo

www.cigent.com
info@cigent.com
844.256.1825