EINPRESSWIRE

Cigent PBA 2.0 Achieves NIAP Listing and CC Certification, Advancing Pre-Boot Authentication for CSfC DAR Protection

New release adds NIAP-tested and approved authentication options, enhanced security, and administration utilities

CIGENT

Data Secured. Mission Assured.

Cigent secures sensitive data at rest on every device, from the edge to the command post

FORT MYERS, FL, UNITED STATES, September 30, 2025 / EINPresswire.com/ -- Cigent today announced PBA 2.0, the latest version of its Pre-Boot Authentication (PBA) software, which controls hardware full drive encryption (HW FDE) for the outer layer protection in CSfC Data-at-Rest deployments. PBA 2.0 is NIAP-listed and Common Criteria certified (NIAP Product ID 11638), reflecting independent laboratory evaluation against the applicable Protection Profiles.

While self-encrypting drives (SEDs) are often assumed to secure data out of the box, they offer no real protection unless paired with an independently validated PBA. Without enforcement of authentication before boot, data is automatically decrypted and exposed as soon as the system powers on. Cigent PBA 2.0 provides the critical outer layer protection in CSfC-aligned Data-at-Rest architectures by enforcing authentication before the operating system loads. By pairing a secure pre-OS environment with hardware full drive encryption, Cigent PBA keeps mission data locked until authorized credentials are presented.

What’s new in PBA 2.0

-NIAP-tested and approved authentication methods: Password, smart card (such as CAC and SIPR tokens), security key with touch and PIN, and USB drive key. Approved combinations include password + smart card and password + security key.

-USB drive authentication: Enables automatic pre-boot authentication using a user-specific key stored on a USB drive, ideal for remote, server, headless, selected IoT, and unmanned platforms where no GUI or input is required. Devices can be configured to prevent boot without the USB drive key present.

-Enhanced security: Cryptographic module updated to the latest libraries validated against FIPS 140-3 criteria. Additional cryptographic steps in the key chain improve key protection, security, and administrative flexibility.

-Administration utilities: Exportable system report that collects platform and drive details directly from installation media for faster troubleshooting. PSID Revert is integrated to allow wipe/erasure via the drive's PSID without separate utilities prior to PBA installation.

Why it matters

PBA 2.0 enforces authentication before the operating system loads, keeping storage locked and keys out of reach of OS-level exploits. It serves as the outer layer protection, typically paired with software full drive encryption as the inner protection in CSfC-aligned DAR architectures. With NIAP-tested and approved authentication methods (password, smart card, security key with touch and PIN, and USB drive, including approved combinations), programs gain added confidence that pre-boot access controls meet rigorous evaluation criteria and can be deployed consistently across varied mission environments without adding operational complexity.

"By expanding NIAP-tested authentication options and advancing our cryptographic foundations, PBA 2.0 strengthens the Data-at-Rest protection that federal programs rely on across PCs, servers, manned and unmanned vehicles, and IoT, without adding complexity," said Tom Ricoy, Chief Product and Technology Officer.

Availability

PBA 2.0 is available today through Cigent and select OEM and storage partners. The NIAP listing is public at: Cigent PBA Software v2.0 (NIAP Product ID 11638).

About Cigent

Cigent secures sensitive data on every device, from the edge to the command post. Through an integrated and modular combination of hardware and software capabilities, Cigent enables NSA Commercial Solutions for Classified (CSfC) compliance by delivering layered protection. Data remains secure throughout its lifecycle with data access controls, persistent data monitoring, and verified sanitization capabilities. Device coverage includes PCs, servers (with multi-drive support), manned and unmanned vehicles, industrial control systems (ICS), and IoT platforms.

The Cigent team includes cleared TS/SCI personnel with decades of operational experience and a U.S.-based software development team. The Cigent portfolio is available through leading drive and device manufacturers and is integrated by top federal systems integrators (FSIs).

Kelvin Quezada
Cigent

email us here
Visit us on social media:
LinkedIn
X