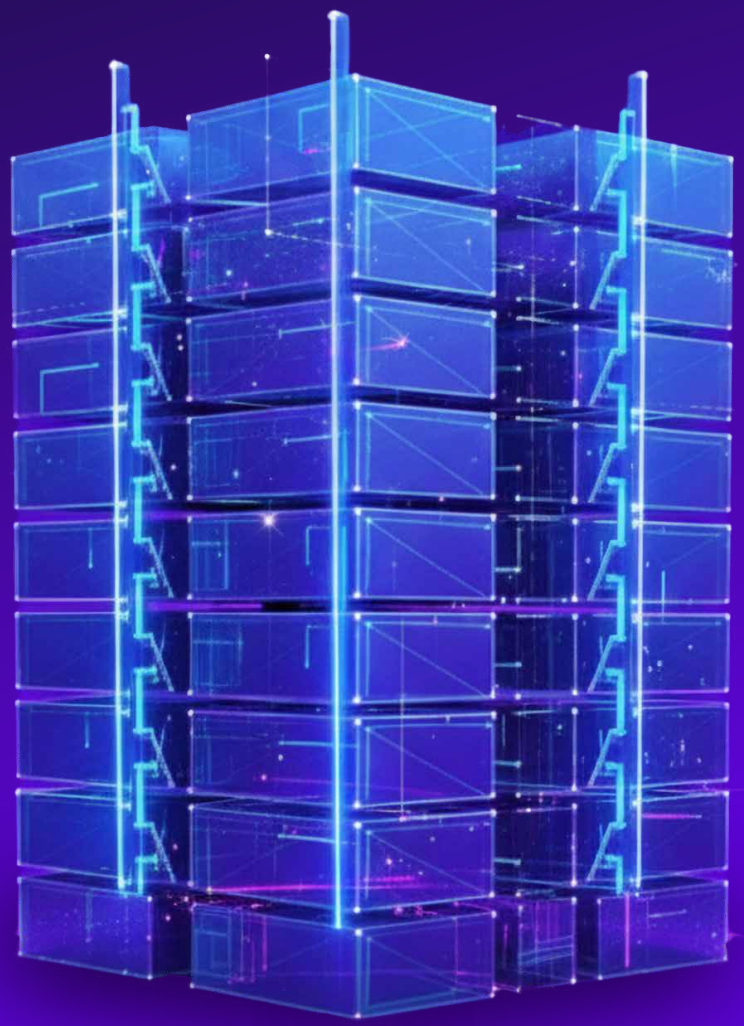
CleanStart™

FIPS Compliance

Building Government-Grade Cryptography for Cloud-Native Infrastructure



About This Paper

This paper explains operational and technical requirements for FIPS 140-3 compliance in container-based environments and outlines how CleanStart embeds validated cryptography at the infrastructure layer. It is part of the CleanStart Technical Foundations Series and focuses on practical steps to maintain validation boundaries, automate evidence generation, and accelerate government market access.

NIST CMVP Validation Authority
Official validation certificates and module registry

Validated Cryptographic Modules

- OpenSSL FIPS Module (Cert #XXXX)
- BoringSSL (Cert #YYYY)

CleanStart OS FIPS Foundation

- Validated modules in approved configuration
- Cryptographic boundary enforcement

Application Container Layer

- All crypto operations use validated modules
- Non-approved algorithms disabled

Validation Documentation & Audit

- Certificate metadata in container labels
- Security policy documentation

Continuous Compliance

- Daily builds with validated modules
- Automated testing in FIPS mode
- CMVP update monitoring

CleanStart's compliances model to support FIPS Architecture

The Cryptographic Trust Foundation

For organizations handling government data, defense systems, healthcare records, or financial transactions, cryptographic assurance is mandatory. FIPS 140-3 defines security requirements for cryptographic modules protecting sensitive information and serves as a global benchmark for cryptographic security (NIST CSRC, 2025). Achieving genuine CMVP validation requires formal testing, documentation, and an active certificate number; implementing approved algorithms alone does not satisfy federal validation requirements.

Understanding FIPS 140-3 and the CMVP Process

FIPS 140-3 references ISO/IEC standards for module requirements and testing, aligning U.S. standards with international frameworks. The CMVP validates test results from accredited laboratories and issues official certificates listed on the validated modules registry (NIST CSRC, 2025). Modules validated for FIPS 140-2 remain acceptable for existing systems until September 21, 2026, after which new acquisitions require FIPS 140-3 validation (NIST CSRC, 2025).

Technical Requirements for Container FIPS Compliance

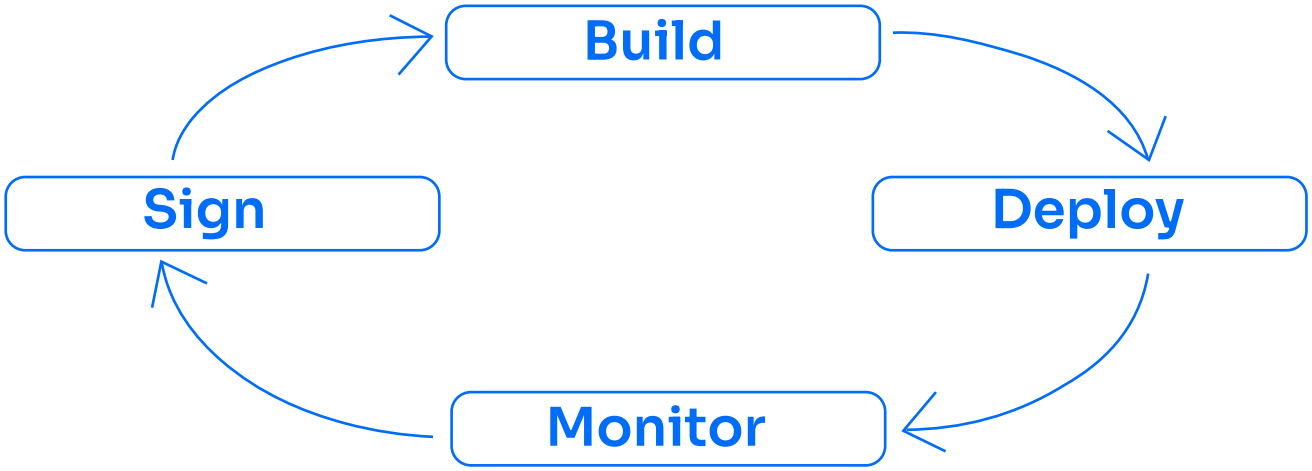
Containers must incorporate validated cryptographic modules and preserve validation boundaries across build, deployment, and runtime. Key technical considerations include validated module integration, approved algorithms and key lengths, self-test requirements, and secure key management.

Validated modules are certified in specific configurations. Containers must use these validated configurations and ensure applications cannot bypass the cryptographic boundary. Approved algorithms and key sizes must be enforced at compile time and runtime to prevent non-compliant operations.

Self-tests must run at container startup and during operation, with proper error handling and audit logging. Key management in ephemeral container environments must rely on secure provisioning mechanisms such as hardware security modules or secrets managers rather than embedding keys in images.

The FIPS Implementation Challenge for Cloud-Native Infrastructure

Implementing FIPS compliance in containers challenges organizations on multiple fronts: maintaining validation across frequent image updates, activating FIPS mode appropriately, ensuring application compatibility, and generating audit evidence at scale. These challenges increase with large container portfolios and heterogeneous runtime environments. A retrofit approach that updates existing images risks configuration drift and operational fragility. A foundational approach that embeds validated modules in the operating system reduces per-image effort and centralizes configuration and evidence generation.



Continuous Validation Lifecycle
Cleanstart integrates FIPS validation directly into the build & deployment pipeline, maintaining cryptographic assurance accross build, runtime, & audit phases

Quantifiable Benefits of Validated Cryptography

Organizations that implement genuine FIPS validation realize measurable improvements in security posture, operational efficiency, and market access. Benefits include accelerated FedRAMP authorization, reduced validation and audit costs, lower risk through independent verification, and competitive differentiation when bidding for government contracts.

CleanStart: FIPS Compliance Built Into the Foundation

CleanStart embeds validated cryptography within CleanStart OS, providing pre-validated images that preserve validation boundaries and include required self-tests and operational modes. Validated modules such as OpenSSL and BoringSSL are integrated in their certified configurations, and container metadata carries certificate numbers and tested configurations for audit verification

Automated FIPS mode activation, daily builds that incorporate validated module updates, and certificate metadata in image labels simplify maintenance and auditing. CleanStart's approach transforms FIPS compliance from a specialized engineering project into an infrastructure capability.

FIPS Architecture in Container Infrastructure

CleanStart's architecture places validated cryptographic modules at the foundation, with clear boundaries enforced at the OS layer and only approved algorithms accessible to applications. Validation documentation and automated evidence generation support continuous compliance and rapid auditor verification.

Next in the Series

The next paper in this series, 'FIPS 140-3 and the Quantum Imperative: Advancing Cryptographic Foundations for the Post-Quantum Era', examines the transition to FIPS 140-3 alongside post-quantum cryptography and how foundations can support both simultaneously.

Part of the Built-In Compliance Series

01 Embedding FIPS 140-2 Compliance at the Foundation.

02 FIPS Compliance: Building Government-Grade Cryptography for Cloud-Native Infrastructure (You are here).

03 FIPS 140-3 and the Quantum Imperative: Advancing Cryptographic Foundations for the Post-Quantum Era.

04 FIPS-Traces: Automating Cryptographic Compliance from Manual Documentation to Continuous Assurance.

References

NIST CSRC. (2025). FIPS 140-3 Transition Effort.

Keyfactor. (2023). FIPS 140-3 Overview.

CCCS. (2024). FIPS 140-3 Security Levels and Requirements.

Entrust. (2024). What is FIPS 140-3?

SignMyCode. (2024). FIPS 140-3 Certification and Levels.'

NIST CSRC. (2017). Post-Quantum Cryptography.