CleanStart™

Embedding FIPS 140-2 Compliance at the Foundation

Building Cryptographic Assurance into Modern Container Infrastructure

About This Paper

Federal Information Processing Standards (FIPS) define the cryptographic assurance baseline for all federal and defense systems. As compliance expectations expand to the commercial sector, organizations must evolve from reactive validation toward architectures where compliance is inherently built in. This paper explains how CleanStart OS integrates validated cryptography at the foundational level to make FIPS compliance automatic, auditable, and sustainable.

The Cryptographic Compliance Imperative

Federal agencies, defense contractors, and organizations serving government markets face a clear mandate: cryptographic operations must use validated modules that comply with **Federal Information Processing Standard (FIPS) 140-2** or its successor **140-3**. This requirement stems from regulatory frameworks such as **Federal Risk and Authorization Management Program** (FedRAMP), which relies on **National Institute of Standards and Technology** (NIST) **Special Publications** (SP) 800-53 security controls mandating FIPS-validated or **National Security Agency** (NSA) approved cryptography. The obligation extends to commercial cloud providers and regulated industries including healthcare, financial services, and critical infrastructure.

A crucial distinction often overlooked is that FIPS-validated means a cryptographic module has been formally certified by the Cryptographic Module Validation Program (CMVP). FIPS-compliant is only an industry term for products that rely on validated modules but have not been validated themselves. Only validated modules satisfy federal requirements.

The Foundational Alternative: Built-In Cryptographic Compliance

A more effective approach embeds FIPS-validated modules directly in the container operating system, transforming compliance from a retrofit task into a foundational property. This shifts responsibility from the application layer to the infrastructure layer and reframes the question from 'How do we make our apps FIPS compliant?' to 'How do we ensure all cryptography is validated by design?'.

Purpose-built operating systems designed for compliance integrate validated modules during build time. All cryptographic operations automatically route through validated libraries. System configurations block access to non-validated modules, self-test frameworks verify module integrity, and policy enforcement ensures only approved algorithms execute.

Quantifiable Benefits: From Months to Minutes

Organizations implementing foundational FIPS compliance experience measurable improvements:

Compressed timelines.

Containers inherit validation instantly instead of waiting months or years for application-level certification.

Operational efficiency.

Teams eliminate the need for specialized cryptographic expertise and focus on application logic rather than validation.or years for application-level certification.

Simplified auditing

Validation can be verified at the operating-system level rather than for each application individually.

Improved vulnerability management

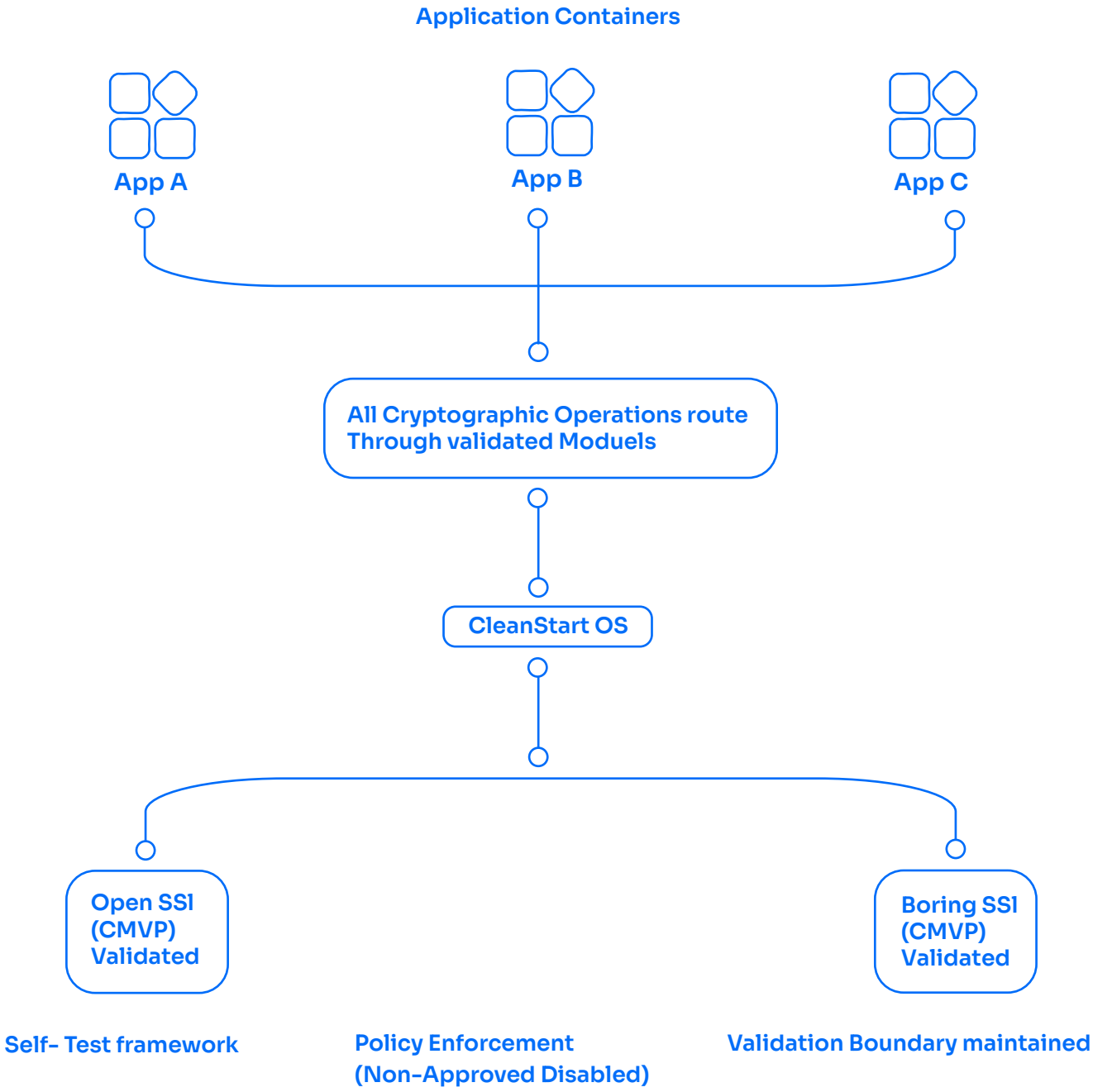
Security updates follow standard OS patching workflows without breaking validation.

Lower Cost

Organizations avoid direct validation expenses and ongoing maintenance costs while improving overall assurance.

CleanStart's Foundational Approach

CleanStart embeds FIPS compliance at the infrastructure layer through CleanStart OS, a container operating system engineered with validated cryptography as a core principle. The system incorporates cryptographic modules that have completed the **Cryptographic Module Validation Program** (CMVP)process and received official FIPS 140-2 or 140-3 certificates, including validated OpenSSL and BoringSSL implementations.



CleanStart embeds FIPS compliance at the infrastructure layer through CleanStart OS, a container operating system engineered with validated cryptography as a core principle. The system incorporates cryptographic modules that have completed the CMVP validation process and received official FIPS 140-2 or 140-3 certificates, including validated OpenSSL and BoringSSL implementations.

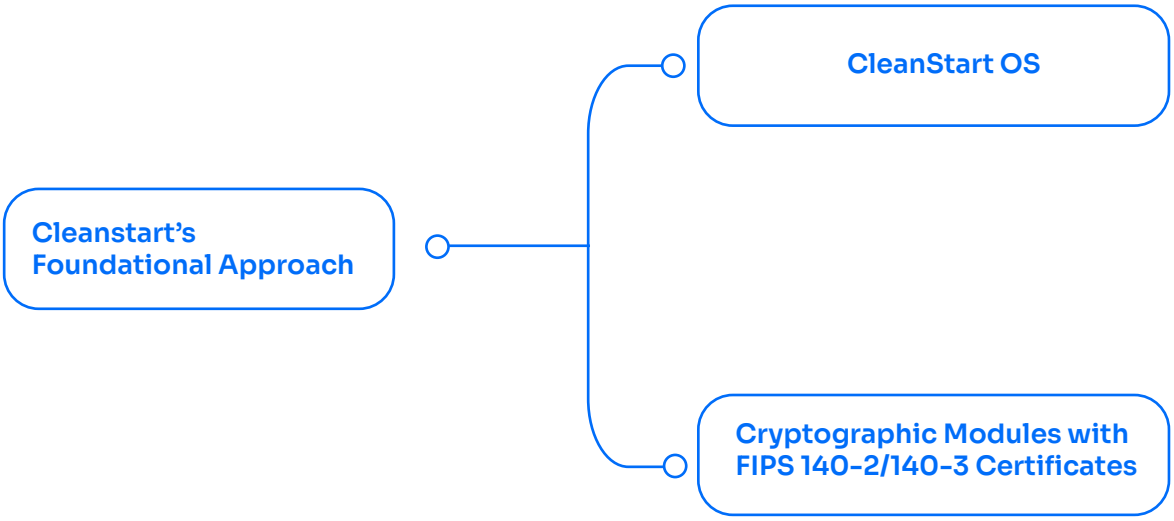
The Retrofit Compliance Challenge

Most organizations treat FIPS as a retrofit problem, adding validated cryptographic modules after systems are already deployed. In container environments this introduces serious architectural complexity. Teams must ensure validated modules run correctly across heterogeneous Kubernetes clusters, activate FIPS mode properly for every deployment, prevent applications from bypassing validated cryptography, and maintain compliance across container lifecycles with continuous audit evidence.

Validation costs are substantial. Achieving certification can take up to two years and cost hundreds of thousands of dollars. By the time validation completes, new security vulnerabilities often emerge, forcing organizations to choose between preserving validation and applying critical patches.

Compliance as Infrastructure

The future of cryptographic assurance lies in architecture, not retrofitting. Foundational compliance reduces authorization timelines, improves security posture, and simplifies operations for organizations pursuing FedRAMP authorization or government contracts. CleanStart OS demonstrates that compliance can be an infrastructure property rather than a development burden.



CleanStart extends FIPS-validated assurance from the base operating system to container images, workloads, and runtime environments, maintaining continuous validation across the stack.

Next in the Series

The next paper in this series, 'FIPS Compliance: Government-Grade Cryptography for Cloud-Native Infrastructure', examines how validated cryptographic modules scale across distributed container ecosystems and how CleanStart enables compliance continuity across diverse environments.

Part of the Built-In Compliance Series

01 Embedding FIPS 140-2 Compliance at the Foundation (You are here).

02 FIPS Compliance: Building Government-Grade Cryptography for Cloud-Native Infrastructure .

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.