CleanStart

# FIPS - Traces

Automating Cryptographic Compliance from
manual Documentation to Continous Assurance

## About This Paper

This paper explores the transformation of FIPS compliance from a static documentation process into an automated, continuous assurance framework. It examines how CleanStart automates cryptographic validation, audit evidence generation, and traceability across container environments.

## The Problem with Traditional Compliance Documentation

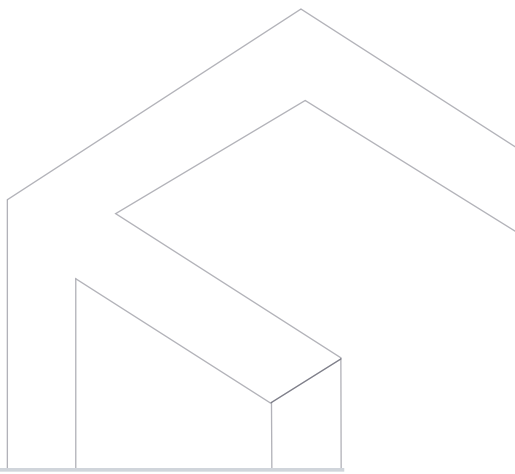
Traditional FIPS compliance processes depend heavily on manual documentation, audits, and evidence collection. These activities are slow, prone to error, and difficult to scale in modern containerized environments where builds and deployments occur continuously (Coalfire, 2025). As systems evolve faster than audit cycles, evidence often becomes outdated before it can be reviewed, leading to compliance gaps.

In many organizations, compliance documentation still involves spreadsheets, screenshots, and audit reports produced quarterly or annually. This method is no longer viable in cloud-native ecosystems that update images daily or hourly.

## Toward Continuous Cryptographic Assurance

Continuous assurance replaces retrospective compliance with real-time verification. Instead of checking compliance after deployment, systems continuously verify cryptographic configurations and module integrity during operation. This approach aligns with modern compliance standards such as NIST SP 800-53 Rev. 5 and FedRAMP Continuous Monitoring (ConMon) requirements.

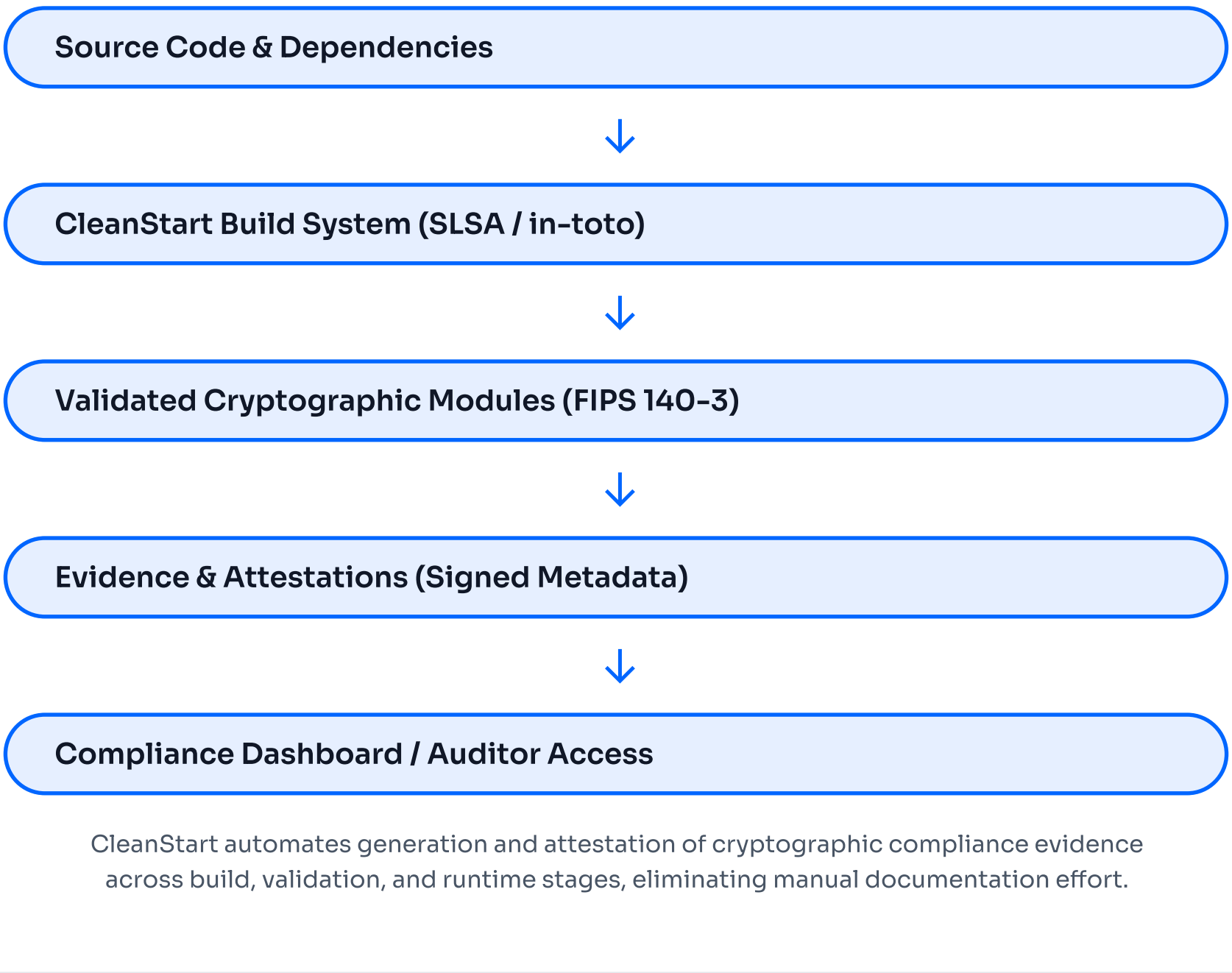
Automated evidence generation provides auditable proof that cryptographic modules remain validated, configured correctly, and operating within FIPS-approved boundaries throughout their lifecycle.



## Introducing FIPS-Traces

FIPS-Traces is CleanStart's automated compliance framework that converts manual FIPS documentation into structured, machine-verifiable evidence. It integrates directly into CleanStart_OS and CleanStart's build pipeline, capturing validation metadata, cryptographic configurations, and operational states automatically.

Each container build produces an attestation report documenting validated modules, certificate identifiers, and configuration states. These attestations are signed and stored as immutable records, forming a verifiable compliance ledger.




CleanStart automates generation and attestation of cryptographic compliance evidence across build, validation, and runtime stages, eliminating manual documentation effort.

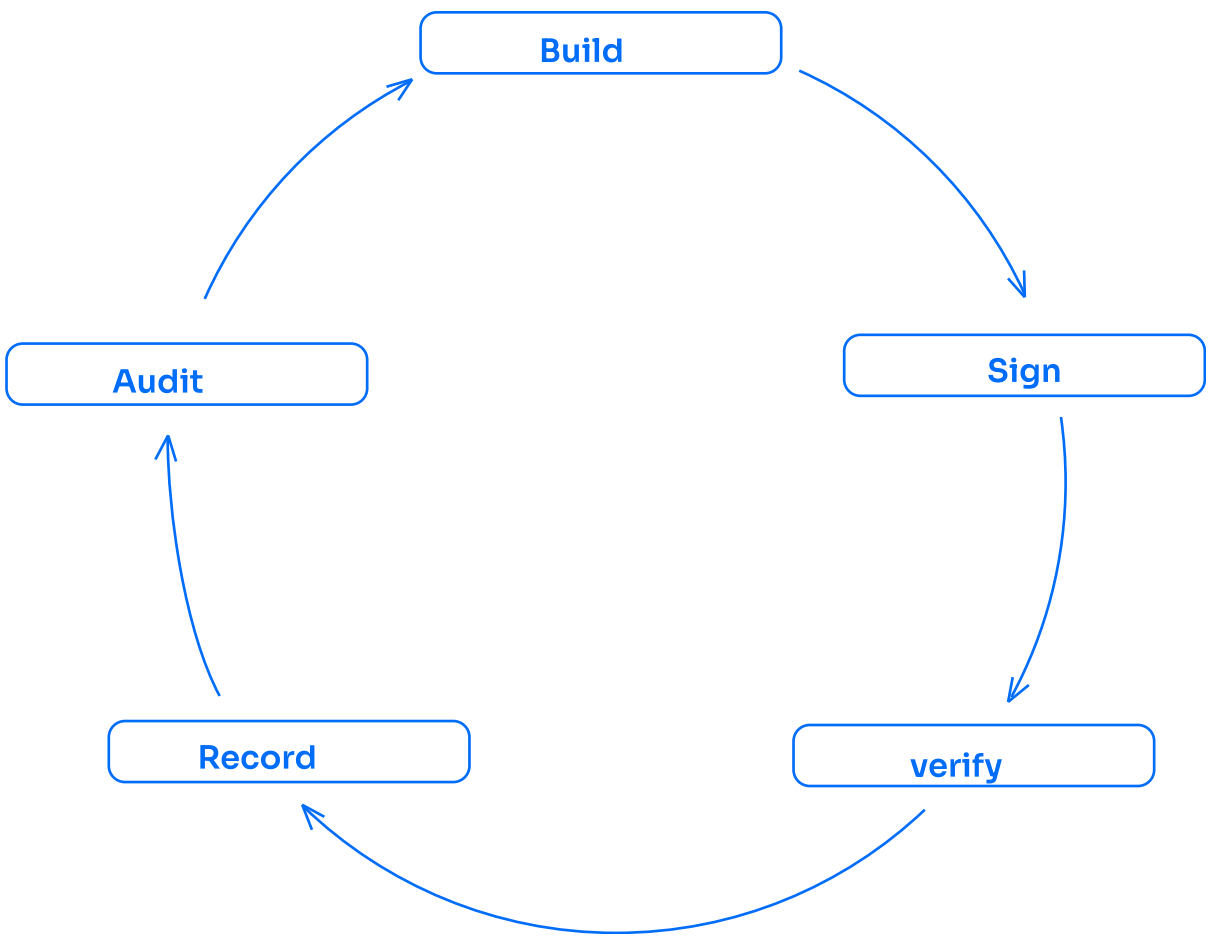
## Automated Evidence Generation

FIPS-Traces automates evidence generation by embedding compliance metadata into container manifests. Every container image includes cryptographic fingerprints, validation certificate references, and algorithm configuration details that auditors can verify instantly.

This automation reduces audit preparation time from weeks to minutes, minimizes human error, and provides real-time visibility into compliance status across distributed workloads.

## Traceability and Attestation Workflows

CleanStart's attestation workflow builds on in-toto provenance and SLSA Level 4 integrity guarantees to provide verifiable traceability across build and deployment pipelines. Each build step includes cryptographic attestations, validated module identifiers, and policy enforcement records. This ensures compliance evidence is trustworthy, tamper-proof, and continuously updated.




Continuous attestation enables verifiable, audit-ready cryptographic compliance where every build and deployment produces immutable proof of validation.

## CleanStart's Compliance Automation Architecture

CleanStart's compliance automation architecture integrates FIPS validation, attestation generation, and monitoring into a single pipeline. The architecture ensures that cryptographic assurance is an outcome of the build process rather than an afterthought. By unifying cryptographic operations, validation, and evidence, CleanStart provides compliance as a service layer within its container ecosystem.

## Benefits of Automated FIPS Assurance

- Real-time visibility into cryptographic compliance status.
- Reduction in manual documentation and audit preparation efforts.
- Consistent, verifiable, and tamper-resistant compliance records.
- Improved response times for security incidents and audit requests.
- Sustained compliance during continuous delivery cycles.

## Continuous Compliance in Action

CleanStart customers using FIPS-Traces can demonstrate compliance continuously through generated attestations and dashboards showing module validation status. Auditors can verify compliance in near real time using evidence embedded in the infrastructure itself, reducing friction and eliminating audit lag.

## Conclusion

FIPS-Traces represents a paradigm shift in compliance management. It automates the entire evidence lifecycle, reduces manual intervention, and brings cryptographic assurance into the operational workflow. With CleanStart's automation-first approach, compliance evolves from a static checkbox to a continuous, measurable state of assurance.

## Next in the Series

This concludes Volume II – Built-In Compliance. The next volume in the CleanStart Technical Foundations Series explores supply chain security and provenance, focusing on in-toto attestations and SLSA Level 4 compliance.

**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

Part of the Built-In Compliance Series

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 **(You are here)**

## References


Coalfire. (2025). 'Continuous Monitoring and FedRAMP ConMon Practices.'

NIST. (2020). 'NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.'

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

In-toto. (2024). 'Software Supply Chain Provenance Framework.'

SLSA.dev. (2025). 'Supply-chain Levels for Software Artifacts Framework.'