

CODE SIGNING SECURITY

Code signing in milliseconds for a financial services firm

A leading financial services firm, operating under strict regulation, lacked a streamlined, secure code signing process, exposing its software deployments and client data to risk. CodeSign Secure delivered HSM-backed signing fast enough for developers and strict enough for regulators.

SECTOR

Financial services

HSM

FIPS 140-2 validated

SOLUTION

CodeSign Secure

FIPS 140-2

Validated HSM keys

1

Platform, all file types

CA/B

Forum compliant

A regulated firm, missing a step

This firm is a leading financial services provider, recognized for an innovative approach to data protection and a commitment to the confidentiality and integrity of client financial information. It operates in a highly regulated industry.

Its code signing practices were the gap. Without a streamlined, secure process, the firm's software deployments, and the critical systems and client data behind them, were exposed to avoidable vulnerabilities.

Unsigned or loosely signed software is a direct risk to client data. In finance, every deployment has to be provably trusted.



Secure, fast, and compliant, at once

Key theft, developer friction, compliance gaps, performance limits, and missing timestamps all pointed to one fix.

1

Theft of signing keys

Poorly managed, improperly protected private keys are a prime target, and stolen keys let attackers pass off malware as authentic code, made worse by limited revocation.

2

Developer productivity

Without code signing built into DevSecOps, security checks couldn't be automated, slowing developers and straining collaboration with security teams.

3

Compliance requirements

In a regulated industry, the firm needed signed artifacts and audit trails to prove its software hadn't been tampered with, and its process couldn't provide them.

4

Performance requirements

Signing had to confirm legitimate, unmodified software without slowing development, a balance the firm's existing process couldn't strike.

5

Lack of timestamping

Without timestamping, signatures would lose trust once certificates expired or were revoked, and the firm stayed exposed to replay attacks and waning customer confidence.

“

The firm needed code signing that was fast enough for developers, secure enough for regulators, and comprehensive enough to cover every platform and file type in their environment.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CODESIGN SECURE

Signed in 2ms, secured in HSMs

CodeSign Secure protected keys in FIPS 140-2 HSMs, generated signatures in 2ms, customized access by risk, logged every request, and covered every platform on one platform.



FIPS 140-2 HSM keys

Private keys are stored in FIPS 140-2 validated HSMs from vendors like Entrust and Thales, protecting them from theft and misuse.



Developer-friendly

Developers produce signing keys seamlessly without special tools, striking a balance between strong security and productivity.



Custom access control

Security teams tailor access levels by project type, acceptable risk, and request source, while simplifying compliance reporting.



2ms HSM signing

Client-side file hashes and key aliases are sent to the HSM, which generates a signature in just 2ms, beating the 4ms target.



Comprehensive logging

A robust logging mechanism captures timestamps, client IPs, file hashes, HSM signatures, and certificate names for every request.



One platform, every type

A single platform handles Windows, Apple, Linux, Docker and container, and firmware signing across the whole environment.

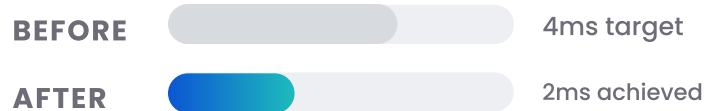
Fast for devs, strict for auditors

CodeSign Secure hit the firm's performance, security, and compliance targets at once, with 2ms signing, HSM-protected keys, and coverage across every platform.

2ms



HSM signature generation



Keys protected in HSMs

Private keys live in FIPS 140-2 Level 3 HSMs, guarded against theft and misuse and lifting the firm's security posture.



Developers move faster

Engineers sign without special tools, keeping security tight while productivity and workflows improve.



Compliance made easy

Tailored access controls and streamlined reporting simplified regulatory adherence and made audits efficient.



One platform, every target

Windows, Apple, Linux, Docker and container images, and firmware all sign on a single, CA/B-compliant platform.

— IN SUMMARY

One platform, every signature

CodeSign Secure transformed code signing for this financial services firm. Private keys now sit in FIPS 140-2 Level 3 HSMs, safe from theft and misuse, while developers sign without special tools and without losing speed. Signatures generate directly from the HSM in two milliseconds, comfortably beating the firm's four-millisecond requirement, and a robust logging mechanism captures timestamps, client IPs, file hashes, HSM signatures, and certificate names for full transparency and audit-ready compliance. Best of all, a single platform now handles Windows, Apple, Linux, Docker and container, and firmware signing, with integrity checks and CA/B Forum compliance built in.

GET STARTED

Sign every release in milliseconds.

[Talk to our code signing team →](#)