ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Code signing, centralized and secured for a financial institution

A leading financial institution, spanning retail banking, investment banking, and asset management, relied on manual code signing with keys in under-protected places, slowing developers and risking trust. CodeSign Secure centralized signing with Thales HSM-backed keys.

SECTOR	SCOPE	SOLUTION
Financial services	Banking + asset mgmt	CodeSign Secure

10+
File types supported

LDAP
Access-controlled signing

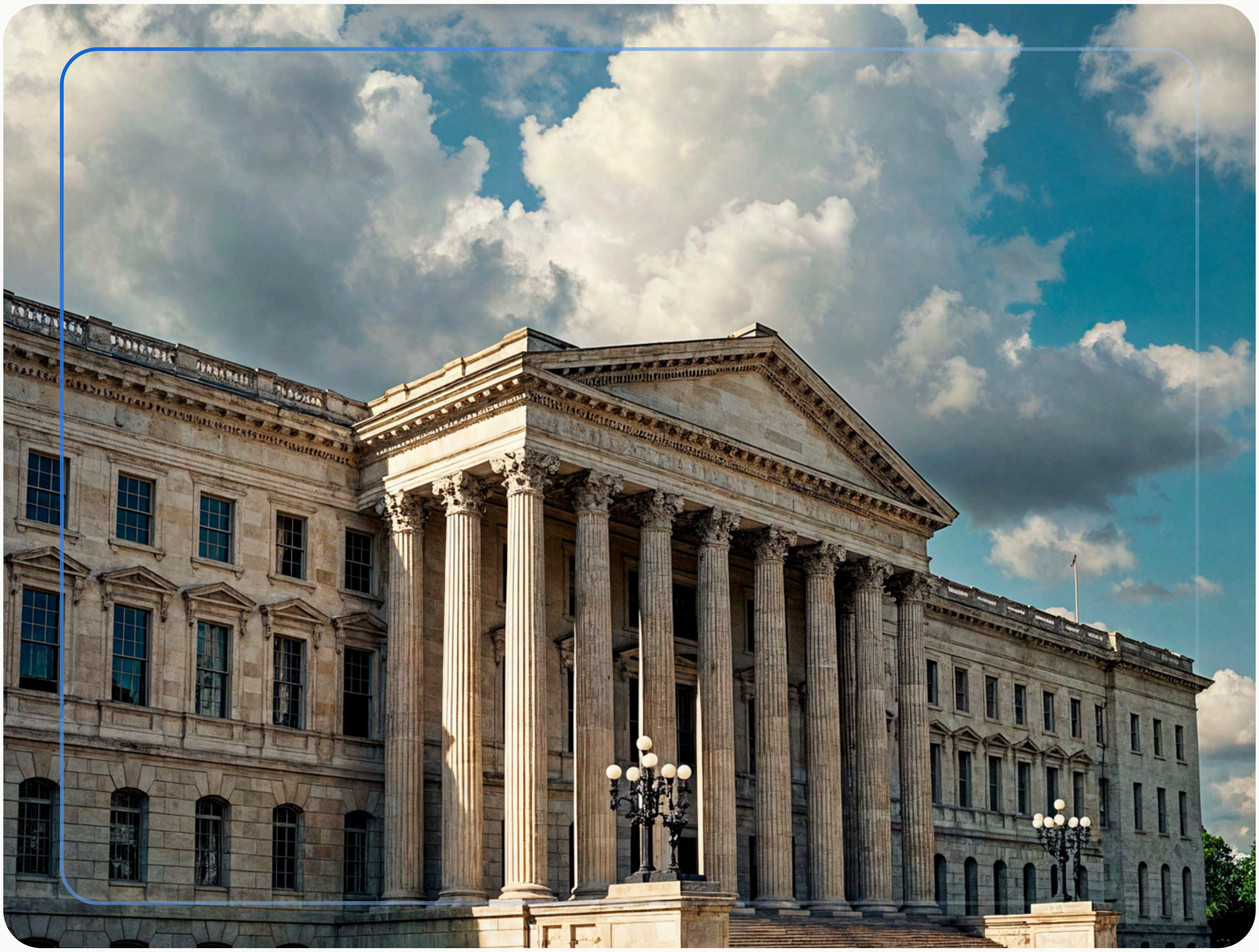
HSM
Thales-protected keys

A finance leader, across three arms

This financial institution is a leading entity in the finance sector, known for a comprehensive array of services across retail banking, investment banking, and asset management. It has a strong reputation for stringent data protection.

Multi-layered encryption, regular audits, and continuous monitoring guard its IT infrastructure. But its code signing told a different story: manual, time-consuming, error-prone processes, and private keys sometimes kept in less protected environments.

Strong everywhere else, the institution's code signing stayed manual and fragmented, exactly where regulators and clients expect rigor.



Manual signing, mounting risk

Stolen-key risk, compliance gaps, no timestamping, and misplaced trust all undermined a manual signing process.

1

Theft of signing keys

Improperly protected private keys are a prime target, and stolen keys let attackers disguise malware as authentic code, made worse by limited revocation.

2

Compliance pressure

In a regulated industry, signed artifacts and audit trails are how the firm proves software hasn't been tampered with, but its manual process couldn't deliver them.

3

No timestamping

Without timestamping, signatures would stop being trusted once certificates expired or were revoked, eroding confidence in the firm's software.

4

Misplaced trust

An inexperienced operator could sign with untrustworthy keys or certificates, and verifiers extending trust opened the door to attacks.

5

Manual, fragmented signing

Time-consuming, error-prone manual processes, with private keys sometimes left in poorly protected environments, made signing slow, inconsistent, and risky.

> For a financial institution where regulatory compliance and client trust are foundational, code signing needed to move from a manual, fragmented process to a centralized, auditable, and secure operation.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CODESIGN SECURE**

Centralized signing, locked down

CodeSign Secure centralized the institution's signing on Thales HSM-protected keys, broadened file-type support, and added the access controls, workflows, and audit trails it had been missing.

Thales HSM key protection

CodeSign Secure stores and manages signing keys in a Thales HSM, bringing centralized control to a process that had been manual.

Broad file-type support

Signing now covers Windows .exe, .dll, .msi, .cab, and .ocx, plus Linux RPM, Jar, macOS, Android, iOS, and Docker images.

LDAP access control

Access control integrated with LDAP ensures only authorized users can sign, removing the risk of keys sitting on servers or endpoints.

Approval workflows

Customizable approval workflows for key usage let the firm enforce its security policies consistently across every function unit.

Trusted certificate list

A trusted list of signing certificates gives the anti-malware team a clear basis for policy enforcement and assured key protection.

Audit trails and reports

Audit processes and metric reports for key usage bring the transparency and accountability that compliance demands.

04 THE IMPACT

Centralized, secure, and auditable

CodeSign Secure replaced manual, fragmented signing with a centralized, HSM-backed operation, broadening coverage and giving the firm the audit trail and control it needed.

Auditable

Code signing, end to end

BEFORE — no trail

AFTER — full audit

Centralized on HSM

Signing keys now live in a Thales HSM under centralized management, ending insecure, scattered key storage.

Sign almost anything

Broad support for Windows, Linux RPM, Jar, macOS, Android, iOS, and Docker images widened the firm's security coverage.

Unauthorized access blocked

LDAP access control and customizable workflows ensure only the right people can sign, closing off unauthorized use.

Trusted by clients and regulators

Structured workflows and detailed audit trails improved transparency, reinforcing trust with clients and regulators.

IN SUMMARY

A new standard for signing

For a financial institution answerable to clients and regulators, code signing has to be airtight. CodeSign Secure transformed the firm's signing from a manual, fragmented practice into a centralized, auditable operation. Private keys moved into a Thales HSM under centralized management, file-type support broadened across Windows, Linux, macOS, mobile, and Docker, a trusted certificate list and policy enforcement strengthened defenses against malware, and structured approval workflows with detailed audit trails brought real transparency and accountability. The result is stronger security, smoother developer workflows, and the kind of rigor that keeps clients and regulators confident.

GET STARTED

Centralize and secure your code signing.

Talk to our code signing team →