ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Secure code signing at retail scale for a US retail giant

One of the largest US retailers, serving millions of shoppers online and in stores, had no code signing in place, leaving its software supply chain exposed to tampering and malware. CodeSign Secure made signing fast, automated, and tightly controlled.

SECTOR	REACH	SOLUTION
Retail (US)	Millions of customers	CodeSign Secure

HSM
Tamper-proof key storage

LDAP
Access-controlled signing

Pre-sign
Antivirus validation

A retail giant, online and in store

This organization is one of the foremost retail giants in the United States, with an expansive presence both online and in stores nationwide. Known for its diverse range, from household goods to high-tech electronics, it serves millions of customers every year.

It runs a solid data security stack, with firewalls, encryption, and intrusion detection, but its approach had been more reactive than proactive. The biggest gap was code signing: without it, software updates could be tampered with before reaching its retail operations and customer data.

At retail scale, unsigned software updates are an open door. Any tampered release could reach millions of customers.

A software supply chain at risk

Unprotected keys, unauthorized certificates, misplaced trust, and weak cryptography all put the software supply chain at risk.

1

Private key theft

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

2

Unauthorized certificates

Weak protection of CA private keys or loose vetting could let attackers obtain unauthorized code signing certificates.

3

Misplaced trust

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

4

Weak cryptography

Weak algorithms or insecure key generation made brute-force and cryptanalytic attacks far easier as threats grew more sophisticated.

5

Signing malicious code

Without a proper signing process, anything from a simple mistake to an intrusion into development systems or poor governance could result in malicious or unauthorized code being signed.

> “As the organization scaled its retail operations, the need for a secure, automated code signing process became critical to protect millions of customers and maintain trust in every software deployment.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CODESIGN SECURE**

Signing in seconds, secured by design

CodeSign Secure replaced slow, manual signing with an automated process, protecting keys in HSMs, controlling access through LDAP, and validating every build before it's signed.

Signing in seconds

CodeSign Secure cut signing from hours, even days, to a few seconds, removing the CI/CD delays that slowed software development.

Keys in HSMs

Private keys move into tamper-proof HSMs, replacing manual key handling and removing the risk of stolen, corrupted, or misused keys.

LDAP access control

Access controls integrated with LDAP and customizable workflows ensure only authorized users can sign, curbing insider threats.

Pre-sign antivirus checks

Code is validated against up-to-date antivirus definitions before signing, so only clean, trusted code is ever released.

Policy-driven compliance

Support for InfoSec policies and customizable workflows aligns signing with industry-specific retail regulations.

Centralized monitoring

Centralized monitoring gives the visibility and control needed to detect any unauthorized or malicious signing activity.

Faster shipping, tighter security

CodeSign Secure sped the retailer's software to market while locking down its keys, access, and code, turning signing into a security strength.

Seconds

To sign code, from hours

BEFORE — hours to days

AFTER — seconds

Faster time to market

Signing in seconds lifted developer productivity and sped retail applications to deployment.

Stronger key security

Keys protected in HSMs with centralized monitoring sharply cut the risk of breaches and unauthorized access.

Insider threats contained

Precise, LDAP-based access control reduced unauthorized code changes and contained insider risk.

Only trusted code ships

Pre-sign antivirus checks mean only clean, verified code is ever signed, preserving integrity across releases.

IN SUMMARY

Trusted code, at retail scale

For a retailer serving millions, every software release has to be trustworthy. CodeSign Secure transformed the organization's code signing from a slow, manual, and risky process into a fast, automated, and secure one. Signing dropped from hours to seconds, private keys moved into HSMs with centralized monitoring, LDAP-based access control and customizable workflows locked down who can sign, and pre-sign antivirus validation ensures only clean code is ever released. With InfoSec policy support and streamlined compliance, the organization ships faster, contains insider risk, and protects customer trust across its entire retail operation.

GET STARTED

Revolutionize your code signing.

Talk to our codesigning team →