ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Code signing that protects patient care for a healthcare leader

A US healthcare leader, rigorous about HIPAA and patient privacy, struggled to manage code signing across its software, devices, and macros, slowing deployments and risking patient trust. CodeSign Secure made signing governed, automated, and HSM-backed.

SECTOR	COMPLIANCE	SOLUTION
Healthcare (US)	HIPAA	CodeSign Secure

FIPS 140-2
Validated HSM keys

LDAP
Role-based signing

Pre-sign
Hash validation

A healthcare leader, bound by HIPAA

This healthcare firm stands at the forefront of medical technology and patient data protection, delivering innovative health solutions across the United States. It's known for rigorous adherence to HIPAA and for advanced encryption that safeguards patient information.

Even so, its code signing operations, crucial for the authenticity and integrity of its software, were hard to manage. Inefficient handling of signing certificates and processes slowed software deployment and put patient care continuity and trust at risk.

In healthcare, software integrity is patient safety. Unsigned code and unmanaged keys are risks no provider can carry.

Software risk, across the board

Unmanaged downloads, insecure firmware, unsigned software, and malicious macros all threatened clinical systems and patient data.

1

Unmanaged software downloads

Staff often installed tools on their own to work faster, and unauthorized software introduced far-reaching risks to the organization's infrastructure.

2

Insecure devices and firmware

Outdated firmware across IoT-connected medical devices left an exposed attack surface that attackers could exploit for breaches or disruption.

3

Unprotected software

Without code signing, there was no guarantee that only legitimate code reached systems, weakening the firm's overall software security posture.

4

Malicious macros

Macros that speed data entry in EHR and Excel workflows could be replaced by malicious macros, causing real harm to clinical systems.

5

Code signing as an afterthought

Scattered keys, inconsistent practices, and limited visibility meant signing was slow and hard to control, just when patient data and care continuity needed it to be reliable.

> “In healthcare, the integrity of every piece of software directly impacts patient data and care continuity. Code signing needed to become a governed, automated process rather than an afterthought.
>
> **ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CODESIGN SECURE**

Governed signing, HSM-backed

CodeSign Secure brought the firm's code signing under control: LDAP-based access, FIPS 140-2 HSM key protection, unified visibility, hash validation, and even secure macro signing.

Role-based access control

LDAP-based authentication and customizable workflows ensure only authorized users can request and sign code, blocking malicious certificates.

HSM-protected keys

FIPS 140-2 validated HSMs protect private keys, replacing keys scattered worldwide with consistent, centralized management.

Unified key and cert visibility

Key and certificate management is unified through HSMs, giving the visibility and control that a large, dispersed inventory had lacked.

Pre-sign hash validation

Hash validation checks every build against the latest antivirus definitions before signing, so potentially malicious code is never signed.

Secure macro signing

A 32-bit signtool was bridged onto 64-bit Windows 10, letting the firm sign Excel macros securely with a Luna HSM.

Works with any HSM

CodeSign Secure integrates seamlessly with leading HSM vendors like Entrust, Thales, and Luna for flexible, robust key administration.

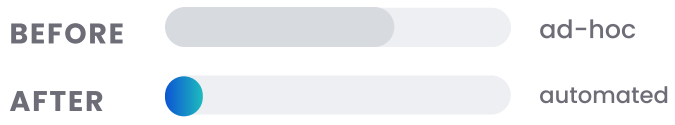
04 THE IMPACT

Signed, secured, and trusted

With CodeSign Secure, the firm signs only trusted code, protects its keys in HSMs, and even secures its macros, all under governed, automated control.

Governed

Code signing, end to end



Only authorized signers

LDAP-based access control stops unauthorized users from signing with malicious certificates, reinforcing trust in signed software.

Keys secured in HSMs

FIPS 140-2 HSMs protect private keys from misuse, while consolidated management keeps practices uniform across the firm.

Macros signed safely

A 32-bit signtool now runs on 64-bit Windows 10, letting the firm sign Excel macros securely with a Luna HSM.

Only trusted code ships

Pre-sign hash checks against current antivirus definitions ensure only clean code is signed, cutting security incidents.

IN SUMMARY

Software integrity, built for healthcare

In healthcare, the integrity of every piece of software touches patient data and care. CodeSign Secure turned the firm's code signing from a scattered, ad-hoc practice into a governed, automated one. LDAP-based access control keeps signing in the right hands, FIPS 140-2 HSMs protect private keys with unified, vendor-flexible management, hash validation against current antivirus definitions ensures only clean code is signed, and a 32-bit signtool bridge even enables secure macro signing on 64-bit Windows with a Luna HSM. The result is stronger software security, contained insider and malware risk, and renewed trust in every signed healthcare application.

GET STARTED

Govern your code signing.

Talk to our code signing team →