ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Code signing, built into the pipeline for an automation leader

An industrial automation leader, known for its PLC and automation software, had no code signing in its Azure DevOps pipeline and slow AppLocker launches. We integrated CodeSign Secure to automate signing, protect keys, and speed delivery.

SECTOR
Industrial automation

PIPELINE
Azure DevOps CI/CD

ENGAGEMENT
CodeSign Secure

CI/CD
Signing automated

HSM
FIPS 140-2 L3 keys

0
Manual signing steps

An automation leader, built on trust

With innovative software for programmable logic controllers and automation solutions, this company is one of the market's best providers of industrial automation, with an impressive regional presence automating processes in even the most complex industrial settings.

As a leading technology company, software authenticity, validation, and data integrity sit at the center of its operations. But implementing code signing inside its Azure DevOps pipeline proved difficult, slowing development, and AppLocker was making applications slow to launch.

For a company whose product is trust in automation, unsigned code moving through the pipeline was a risk it could no longer carry.

Unsigned code, and slow launches

Without code signing in the pipeline, manual checks slowed delivery, security suffered, and compliance was at risk.

1

No signing in the pipeline

Without code signing in their Azure DevOps CI/CD pipeline, manual checks slowed every deployment and held back their operational agility.

2

Security vulnerabilities

The absence of signing left the door open to code tampering and malicious injection, putting user applications and the whole software infrastructure at risk.

3

Slow AppLocker launches

Applications took too long to open, frustrating customers during critical tasks, disrupting workflows, and cutting productivity.

4

Compliance breach

Unauthenticated software could be installed and software authenticity was questioned, risking non-compliance with frameworks like HIPAA and GDPR.

5

Trust, speed, and compliance at stake

Together these gaps meant software authenticity, application performance, and regulatory compliance were all exposed, leaving every release resting on unverified trust.

> “Without code signing in the pipeline, every deployment was an unverified trust assumption. Software authenticity, regulatory compliance, and application performance were all affected.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · CODESIGN SECURE

CodeSign Secure, in the pipeline

We integrated CodeSign Secure into their Azure DevOps pipeline, automating signing, protecting keys in an HSM, and tightening access, all while speeding up their workflows.

Automated CI/CD signing

CodeSign Secure slots into their Azure DevOps pipeline, signing PDF, XML, Authenticode, and Java automatically on every push, with no manual steps.

Keys protected in an HSM

An HSM secures the private keys behind their signing certificates, with access controls so no one can use them without permission.

Signed audit trails

Every signing operation is recorded in tamper-free, audit-proof logs, giving the team full transparency over how code signing is used.

Faster AppLocker launches

One rule, requiring a CodeSign Secure signature, replaced many certificates and hashes, cutting app launch from 2m 30s to 30s.

Granular access controls

P12 certificates, user permissions, and per-environment certificate rules ensure only authorized users and systems can sign code.

Timestamp security

RFC 3161 and Authenticode timestamps plus a FIPS 140-2 Level 3 HSM met the CA/Browser Forum June 2023 requirement.

Faster, safer, and trusted

With CodeSign Secure in the pipeline, the organization signs every release automatically, protects its keys, and delivers software faster, earning customer trust along the way.

30s

Unencrypted databases remaining

Faster, automated delivery

Signing now runs automatically in the Azure DevOps pipeline, cutting manual work and speeding up software delivery.

Keys safe in an HSM

Private signing keys are protected in an HSM with strict access control, sharply reducing the risk of unauthorized use.

Compliance made easy

The solution met market and policy standards, including CA/Browser Forum requirements, keeping the organization compliant.

Trust that drives growth

Customers trust software backed by secure signing, lifting the company's market standing and sustaining growth and loyalty.

IN SUMMARY

Trust, signed into every release

For a company whose reputation rests on trustworthy automation, code signing couldn't stay a manual afterthought. By integrating CodeSign Secure into their Azure DevOps pipeline, we automated signing across PDF, XML, Authenticode, and Java on every push, protected their private keys in a FIPS 140-2 Level 3 HSM, and added tamper-proof audit trails, granular access controls, and RFC 3161 timestamping that meets CA/Browser Forum requirements. AppLocker launches dropped from two and a half minutes to thirty seconds, manual work fell away, and customers gained real assurance that the software they run is authentic, secure, and compliant.

GET STARTED

Bring code signing into your pipeline.

Talk to our code signing team →