# Effortless Code Signing with Uncompromised Security

Manual processes, security gaps, and operational bottlenecks can make code signing a challenge, but it shouldn't slow you down! CodeSign Secure simplifies and secures code signing, ensuring every piece of code is protected, automated, and compliant. Focus on delivering secure software while we handle the trust and integrity behind it.
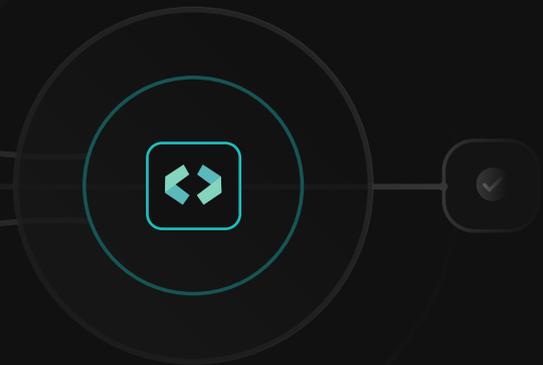
Introduction

Code signing isn't just a security measure, it's a critical foundation of digital trust. Yet, traditional code signing methods are plagued by security gaps, operational inefficiencies, and compliance challenges. CodeSign Secure redefines how enterprises protect their software by offering a highly secure, automated, and scalable code signing solution. Designed to eliminate private key exposure and integrate seamlessly into your development pipeline, CodeSign Secure empowers organizations to sign with confidence, accelerate software delivery, and maintain compliance effortlessly.
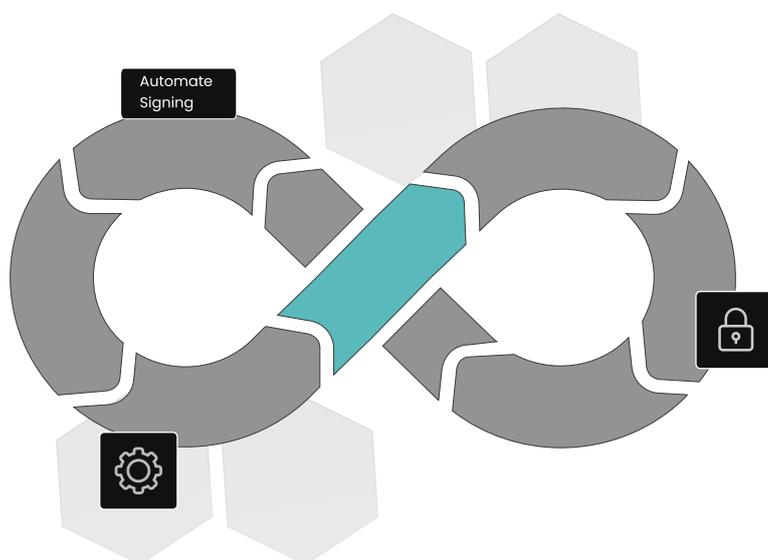
Key Features

- **HSM-Backed Keys:** HSMaaS provides complete administrative control over cryptographic keys, user permissions, and security configurations. You define access policies, configure cryptographic algorithms, and track every administrative action with detailed audit logs.

- **Policy Enforcement & Access Control:** Define and enforce granular security policies, automate key usage permissions, and streamline code signing lifecycle management across teams and workflows.

- **CI/CD Integration:** Seamlessly integrate with your DevOps pipelines and automated build workflows, supporting Jenkins, GitHub Actions, Azure DevOps, Okta, and Bamboo, so security never slows down innovation.

- **Event Logs & Tracking:** Gain complete visibility with detailed audit trails, multi-tier approvals, and "M of N" quorum control, ensuring every signing action is tracked, validated, and compliant.

Decode the Full Potential of Secure Code Signing

Your software's security is only as strong as your code signing process. With CodeSign Secure, you don't just sign code, you secure your entire development lifecycle.

Complete Key Protection: Private signing keys remain secured within FIPS 140-2 Level 3 HSMs, ensuring zero exposure.

Seamless Automation: Native integration with CI/CD pipelines to maintain security without slowing down development.

Granular Access Control: Enforce strict role-based policies to prevent unauthorized signing.

Multi-Platform Compatibility: Sign code for Windows, macOS, Linux, mobile applications, and containerized environments.

Regulatory Compliance Made Simple: Ensure adherence to NIST, CISA, and other global regulations with audit-ready logging and reporting.

Key Features

- **Authentication Integration:** Integrate directly with Azure AD, Okta, SAML, and OAuth, eliminating manual scripts and enabling secure, seamless authentication across your organization.

- **Scalable Deployment:** Support multi-cloud, hybrid, SaaS, and on-premises environments with a fully automated, high-performance signing service that scales effortlessly across multiple CAs, HSMs, and DevOps tools.

- **Client-Side Integration:** Enhance performance with client-side cryptographic processing, reducing server load, minimizing data transfer, and ensuring high-speed, bandwidth-efficient code signing.

The CodeSign Secure Difference

Traditional code signing solutions often come with security gaps, operational inefficiencies, or integration challenges. CodeSign Secure is designed to bridge these gaps, providing a unique approach to securing your software supply chain. Integrating HSM-backed security, automation, and policy enforcement ensures that every signed artifact maintains its integrity while aligning with leading compliance standards.

End-to-End Protection: Eliminates key theft, misuse, and unauthorized signing through robust security mechanisms.

Operational Simplicity: Fully managed deployment options reduce infrastructure overhead while ensuring enterprise-grade security.

Seamless Developer Experience: API-driven integrations and automation-friendly architecture allow security without friction.

Advanced Policy Controls: Enforce signing policies at scale, ensuring compliance without compromising agility.

Use Cases

Whether you are securing software updates, DevOps pipelines, or IoT firmware, CodeSign Secure is designed to protect your code throughout its lifecycle:

Software Vendors & Application Developers:

Ensure your customers receive trusted, tamper-proof software.

IoT & Embedded Systems:

Secure firmware and software running on connected devices to prevent supply chain attacks.

DevOps & CI/CD Pipelines:

Automate secure code signing across cloud-native and on-prem environments.

Enterprise IT & Compliance Teams:

Ensure regulatory compliance and mitigate risks associated with unauthorized software distribution.

Deployment Options

We offer flexible deployment models tailored to your security and operational needs:

On-Premises

Install CodeSign Secure directly on your infrastructure, either on physical servers or virtual machines while safeguarding private keys within your existing or newly deployed HSM.

Cloud

Deploy CodeSign Secure in containerized environments on AWS, Azure, or private cloud platforms, with seamless integration to cloud-based HSMs for protected key management.

SaaS

Access a fully managed, cloud-hosted version of CodeSign Secure with built-in HSM support, delivering the full power of on-prem features through APIs, without handling the underlying infrastructure.

Hybrid

Combine on-premises deployments with secure key storage in cloud or local HSMs, or both, offering unmatched deployment flexibility and control.

Secure Every Type of Code You Sign

Linux Signing: RPM package to ensure authenticity and integrity throughout the software supply chain.
- **File Extensions Supported by CodeSign Secure:** GPG, XML, and more

Apple Signing: Sign all your Mac OS software, tools, updates, utilities, and applications.
- **File Extensions Supported by CodeSign Secure:** (.dmg, .ipa, .app) and Apple's ProduSign used with signing installer packages and archives (.pkg, .mpkg)

Java Signing: Sign all your java code-signing certificates securely.
- **File Extensions Supported by CodeSign Secure:** (.jar, .war, .sar, .ear) and Android (.apk) with JarSigner.

Windows Signing: It supports EV and OV public code signing, and private code signing. Authenticode Files Signing with Windows SignTool, Mage, Nuget, Clickonce, HLK, HCK.
- **File Extensions Supported by CodeSign Secure:** *.exe, *.dll, *.cab, *.msi, *.js, *.vbs, *.ps1, *.ocx, *.sys, *.wsf., *cat, *.msp, *.cpl, *.efi, *.arx, *.dbx, *.crx, *.xsn, *.deploy, *.xap, and more.

Docker & Container Image Signing: Digital fingerprinting to docker images while storing keys in HSM and supports Docker Notary.

Firmware Code Signing: Sign any firmware binaries to authenticate the manufacturer to avoid tampering with the firmware code.
- **File Extensions Supported by CodeSign Secure:** .bin, .img, .hex, .fw, .dfu (device firmware upgrade file format)

OVA/OVF Code Signing: Ensure authenticity, prevent unauthorized modifications, and protect against malware with a verifiable trail of trust.
- **File Extensions Supported by CodeSign Secure:** .ova, .ovf