Effortless Code Signing with Unbreakable Key Protection

Manual code signing is slow, risky, and difficult to scale. Exposed private keys, inconsistent signing workflows, and missing audit logs create major supply chain vulnerabilities. Qcecuring simplifies and secures code signing with automated, HSM-protected workflows that let your developers ship trusted software faster and safer.

Introduction

Code signing proves that software is authentic, trusted, and untampered. But traditional code signing approaches rely on manual steps, locally stored private keys, and disconnected tools—making it easy for attackers to target signing processes or steal sensitive keys. These vulnerabilities put the entire software supply chain at risk.

Qcecuring Code Signing Platform modernizes and secures the entire signing lifecycle. Signing keys stay protected inside HSMs, approvals and policies are enforced automatically, and developers can sign code directly from their CI/CD pipelines without touching private keys. This delivers secure, reliable, and fully traceable signing for all software, firmware, and container images.

The Problems

Private keys stored insecurely

Manual signing slows releases

Hardcoded scripts in CI/CD

No approval process

Multiple signing formats unmanaged

The Solutions

HSM-backed key protection

Secure API-based signing

Automated CI/CD integration

Policy-based approvals & Multi-platform signing

Full traceability for-every signing event

Key Features

HSM-Protected Keys

All private keys remain inside certified HSMs—never exposed to developers or servers.

CI/CD Pipeline Integration

Works with GitHub, GitLab, Jenkins, Azure DevOps, Bitbucket, and more.

Policy Enforcement

Control who can sign, what can be signed, and what approvals are required.

Multi-Platform Signing

Supports Windows, Linux, macOS, mobile apps, containers, and firmware.

Detailed Audit Logs

Every signing action is logged for compliance and incident investigation.

How It Works

Business Benefits

Protects against malware injection

Prevents key theft & Ensures compliance

Accelerates release cycles

Centralizes signing workflows

Use Cases

Software release signing

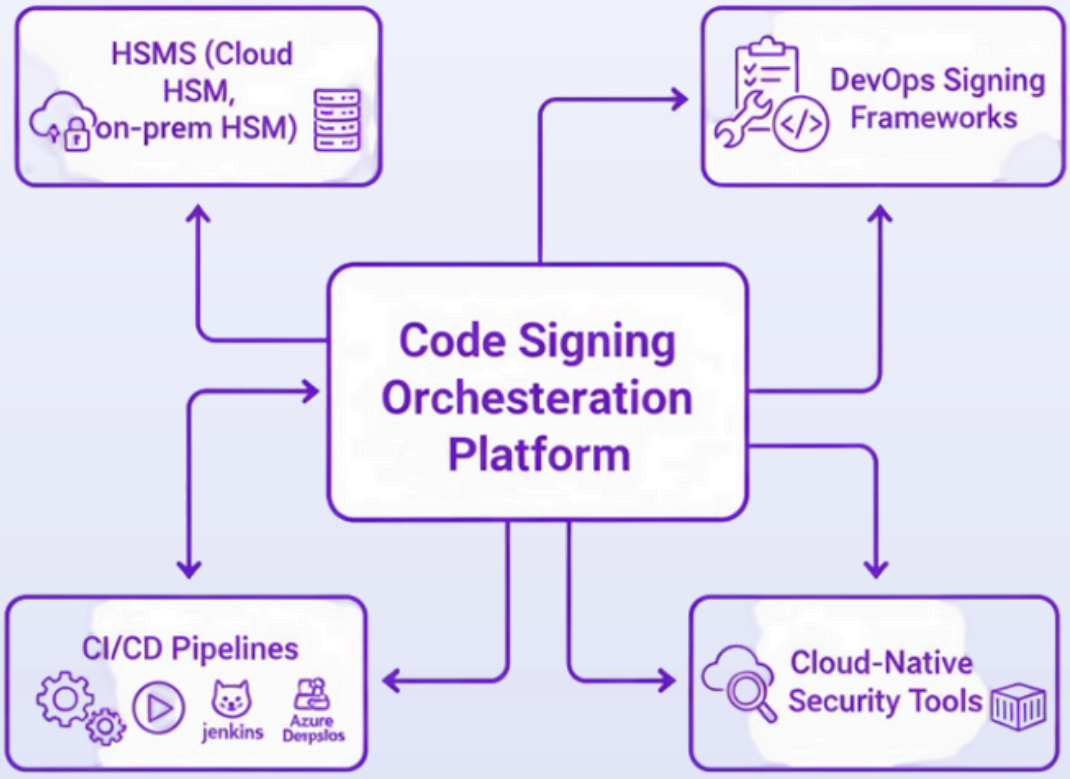
Firmware signing (IoT, embedded)

Container image signing

Enterprise script signing

Mobile app signing

Integrations



Deployment Options

On-Prem (FIPS HSM)

Deploy within your datacenter using FIPS-certified HSMs for complete control and strict compliance needs.

Cloud (HSM-backed)

Run code signing in the cloud with secure, hardware-protected keys. Scales easily and integrates smoothly with CI/CD.

SaaS

A fully managed service with built-in HSM protection — sign code via API without managing any infrastructure.

Hybrid

Keep signing keys on-prem while using cloud automation for workflows, scaling, and approvals.

The Value We Deliver

- Zero key exposure
- Scales with enterprise workloads
- Fast signing operations
- Complete supply-chain protection
- Developer-friendly APIs
- Enterprise-grade automation

Ready to protect your software supply chain with safer, automated code signing? Our Code Signing platform safeguards private keys, automates signing workflows, and integrates seamlessly with your DevOps pipelines—without adding friction. Talk to **info@qcecuring.com** solution experts to schedule a live walkthrough and discuss how secure code signing can accelerate delivery while maintaining trust and integrity.