AppViewX Code Signing | Solution Overview

AppViewX

# Centralize Code Signing. Protect Your Software Supply Chain Without Slowing It Down.

## Challenge

Every release you ship carries your signature. Code signing protects the integrity of your software and the trust your customers place in it, but traditional signing processes, siloed tools, and inadequate key storage turn the signing step into a weak link in your software supply chain.

### Private keys are exposed to theft and misuse

Private keys are at the heart of code signing. Left in inadequate storage, they are open to theft and misuse, exposing you to code signing attacks, software supply chain compromise, and data breaches. A stolen signing key lets attackers sign malware that carries your name.

### Signing slows DevOps down

Ad hoc signing processes, one-off requests, and manual uploads pull developers out of their tools and into ticket queues. Siloed signing tools across teams make it harder to sign securely at the pace your pipelines release.

### Security teams can't see who is signing what

Security teams struggle to monitor and control signing keys, access, and signing events across distributed development teams. Without a clear inventory, you can't trace which keys and certificates signed the software running in production.

### Compliance evidence is hard to produce

When auditors ask who signed a release, when, and with which key, fragmented tools and logs turn a simple question into weeks of evidence gathering. Inconsistent signing policies across teams leave compliance gaps you can't easily close.

**AppViewX Code Signing**

## Speed for DevOps. Control for security.

AppViewX Code Signing is a centralized solution that secures your software supply chain by protecting keys, enforcing consistent signing policies across your CI/CD pipeline, and giving security and DevOps teams full visibility and control of code signing operations. It protects the integrity of code, containers, software, and firmware, so every release is signed securely and consistently. Developers sign from the native tools and pipelines they already use, while security teams keep private keys in FIPS-certified HSMs under policy-driven control.

### Visibility

Maintain a clear inventory of every code signing certificate and signing task across teams and tools. Trace each key and certificate back to the software it signs, so you know exactly what is trusted in production.

### Automation

Replace one-off signing requests and manual uploads with signing from native tools, CI/CD pipelines, API workflows, or the AppViewX Code Signing console. Policy-driven automation keeps the right signing rules following your teams, apps, and environments as they change.

### Security

Generate and store private keys in FIPS-certified HSMs to prevent compromise and ensure root of trust. Stay audit-ready at all times with precise records of who signed what, when, and with which key.

**What It Delivers**

## Secure Your Code, Streamline Your Delivery

### Strong Private Key Protection

Generate and store private keys in FIPS-certified HSMs that meet CA/Browser Forum requirements to prevent key compromise. Connect directly to cloud-based or on-premises HSMs or consume code signing as a service. Supports standard asymmetric algorithms, including RSA, ECDSA, and DSA, and is ready for post-quantum algorithms once they are enabled by the HSM.

### Integrated Code Signing

Sign from native signing tools, CI/CD pipelines, API workflows, or directly from the AppViewX Code Signing console. Out-of-the-box integrations connect public and private CAs, HSMs, and DevOps toolchains such as GitHub, GitLab, Jenkins, Bitbucket, and Azure DevOps.

### Fast and Seamless Signing

Custom PKCS#11 and CSP interfaces plug directly into popular signing tools such as SignTool and Jarsigner, and into your existing build processes. Client-side hashing keeps signing fast, reliable, and efficient for distributed development teams.

### Policy and Compliance Engine

Automate policy enforcement for users and signing operations, including key usage permissions, approvals, key expiry, CA type, key size, and signing algorithm. Role-based access control eliminates unauthorized signing, and secure timestamping keeps signatures valid long term.

### Centralized Visibility and Audit Trails

Give security teams one place to manage key and certificate access, monitor signing events across the enterprise, and enforce policies. Detailed audit logs and reports track every file signed, the time of signing, timestamping usage, and the certificate and key used.

### Versatile File Support and Flexible Deployment

Sign Windows applications, libraries, OCX files, kernel drivers, Apple software, Microsoft Office VBA objects, JAR files, .air and .airi files, containers, and Android APKs from one solution. Deploy on-premises or as SaaS.

## What DevOps and Security Teams Get

| | |
|---|---|
| Private keys protected at the root of trust | A continuously updated, centralized inventory across all CAs and environments—discovered agentlessly, with full metadata, cryptographic scoring, and ownership mapped. |
| Signing at DevOps speed | Certificates renew and provision automatically before they expire, even at 47-day renewal frequency. No manual intervention, no missed deadlines. |
| Consistent policy, no unauthorized signing | Switch CAs, add new ones, and adapt to new mandate and cryptographic changes without re-architecting your certificate program. |
| Full traceability for every release | Discover quantum-vulnerable certificates, prioritize by risk, and migrate to PQC through the same automated workflows already in place. |
| Signatures that stay valid | Pull compliance reports, access logs, and policy evidence from the platform. No manual evidence assembly required. |

## Sign with AppViewX. Ship with Confidence.

Schedule a demo and see how AppViewX Code Signing fits into your build and release pipelines.

AppViewX
info@appviewx.com
www.appviewx.com
+1 (212) 400-7541