Modern Secure Software and Code Signing for DevOps

DigiCert® Secure Software Manager automates security and enables trust and ease-of-use in code signing

Traditional code signing and pitfalls

Code signing is a requirement in product development to ensure code integrity and compliance with industry standards. Traditional code signing typically means key sharing, storing keys on desktops, and no visibility into signing activities. Consequently, traditional code signing can lead to key misuse and malware signing which in turn can cause reputation damage and financial losses.

Companies developing software or applications today are seeking software or code signing solutions that address private key security, track signing activities, and integrate signing into their Continuous Integration/ Continuous Delivery (CI/CD) process.

What is Digicert Secure Software Manager?

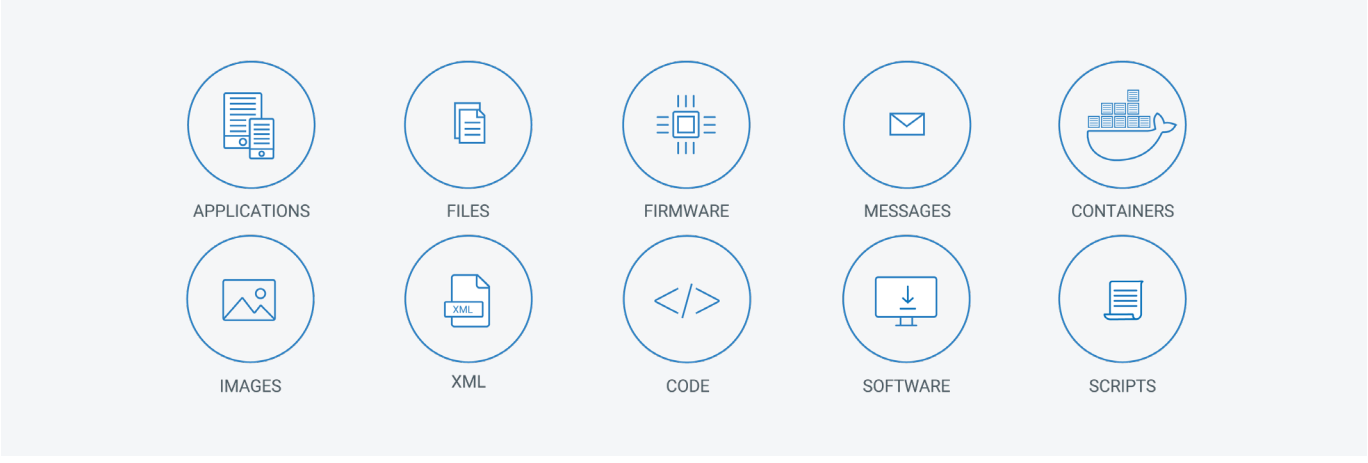
DigiCert Secure Software Manager makes it easy to secure code signing keys, enforce role-based user access, monitor and manage signing activities, and incorporate signing into DevOps processes.

Signing options

Sign all sorts of software including tools, applications, scripts, libraries, plug-ins, and other "code-like" data including containers, firmware and messages. All major file types are supported. In other words, we sign everything you need secured.

Deployment options

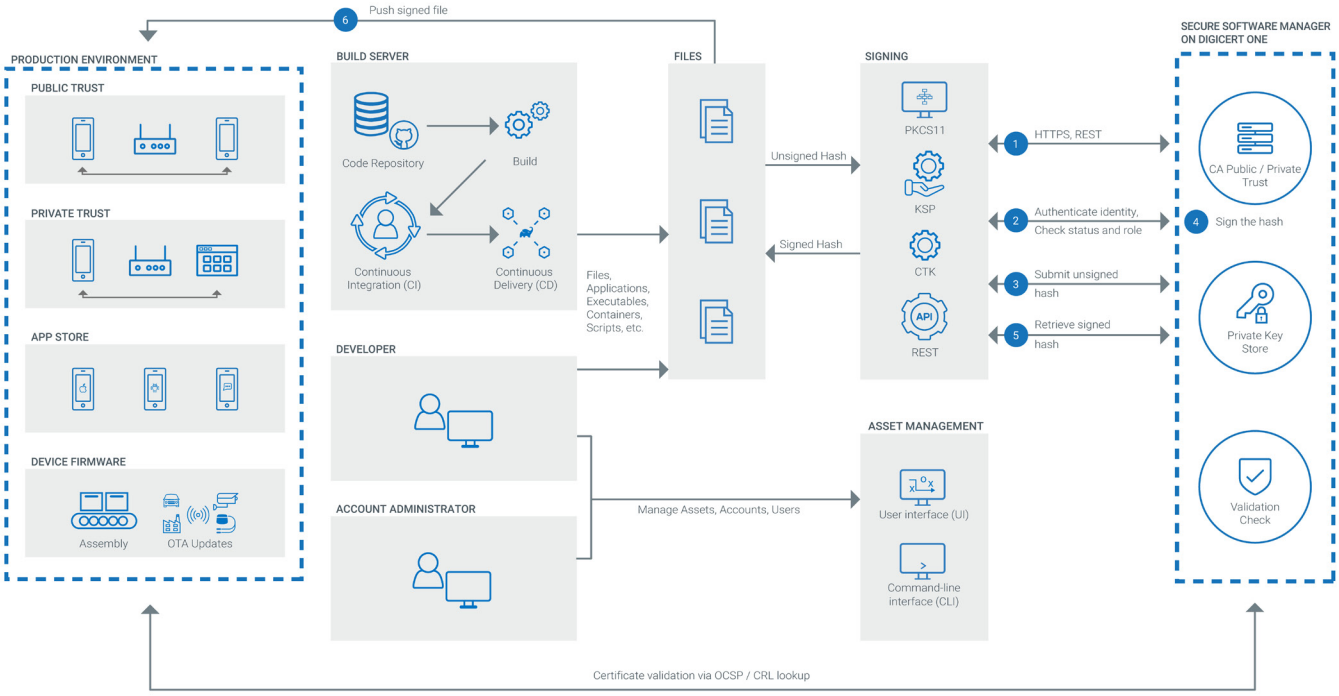
DigiCert Secure Software Manager is built on DigiCert ONE, a modern, container-based platform, with flexible deployment options. Deploy Secure Software Manager on-premises, in the Cloud (DigiCert PKI Cloud or your own), or as a hybrid model. Whatever your unique use case, we meet you where you want to be.



Roots of trust
Build public and private root hierarchies for signing with your external release, internal development, or both. For industry groups, create dedicated and shared private roots so you can have trusted distribution of code and files within your ecosystem. Exercise the option of using a key-based signature that does not require a self-signed or rooted certificate, enabling protected private key signatures that are verified and distributed via public keys.

Development process
Automate signing with your CI/CD platform using the built-in API integration. Leverage the support for major Key Storage Providers (KSPs) and client-side libraries with keypair and certificate management as well as with the signing of applications. Sign hashes, instead of files, for higher security and speed.

Secure Software Manager Signing Workflow



Summary of benefits and features

Know Who Sign What and When

- Tracking for key usages and associated signatures so you can prevent unauthorized usage
- Full reporting and auditing capabilities
- Offline mode for keypairs that require additional approvals for continued use

Sign Apps Faster, Easier and on More Platforms

- Hash signing for expediency and security
- Library-based approach with support for all major file types
- Easy certificate revocation with backdating for quick remedial action
- Workflows support for key imports and exports for ease of use
- Support for test signing with short-lived certificates and time limited test keypairs

Sign with Secure Keys, and Maintain Compliance

- Permission-based access to safeguard signing keys and to control signing usage
- Support for enforcement of internal policies from organization level to product development, including policies on signing algorithms, certificate validity period, and different Extended Key Usage (EKU) for private trust deployment
- Strict adherence to code signing industry requirements, including enforcement of multi-factor access and Hardware Secure Module (HSM) for key storage with public trust deployment

Grow with a Highly Flexible and Scalable Platform

- Built on the most flexible solution in the industry, Secure Software Manager can be deployed on-premises, in-country, or in the Cloud (DigiCert PKI Cloud or yours)
- Automated orchestration technology drives a consistent level of performance with resources that are optimized and shared automatically
- Proven infrastructure to support high volumes of certificates (millions) that can be deployed quickly

Technical specifications

Supported Code Binaries, including

- Android
- Apple
- Authenticode
- ClickOnce
- Debian
- Docker
- GPG
- Java
- Nuget
- OpenSSL
- RPM
- XML

Supported Cryptographic libraries, including

- Apple CryptoTokenKit
- Microsoft CNG/KSP
- PKCS#11

Supported Continuous Integration/Continuous Delivery (CI/CD) Platforms, including

- Apache Ant
- Apache Maven
- Azure Pipelines
- Gradle
- Jenkins

HSM Support, including

- Thales Luna Network HSM and Luna USB HSM
- Thales Luna Cloud HSM

Services support

- Multi-factor Authentication

Find out more

DigiCert provides enterprise-class SSL, PKI and IoT security solutions for some of the world's biggest organizations—providing peace of mind and secured data at all times. Talk to our experts about your needs.

For more information, call 1.801.770.1736, email pki_info@digicert.com, or visit digicert.com/secure-software-manager