# Secure Software with Code Signing Workflow Automation

DigiCert® Secure Software Manager automates code signing workflows, improving software security and integrating seamlessly with DevOps processes.

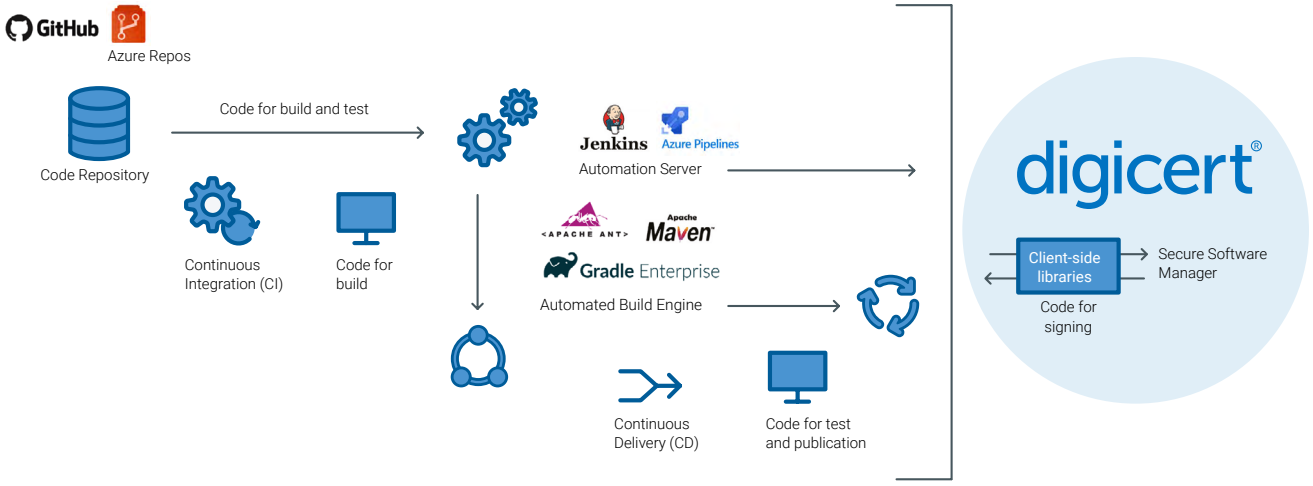
## Reducing software security vulnerabilities

Code signing is broadly recognized as a critical step in conveying trust to software users and protecting companies from harm caused by malicious actors in software supply chain or other types of cybersecurity attacks. Code signing indicates that a software author or publisher is who they say they are and that the code has not been tampered with.

However, manual code signing processes can still leave software and applications vulnerable to attack. The National Institute of Technology (NIST) has identified the infiltration of code signing processes as one of the techniques used by malicious actors.

Key theft, shared or misused keys, unauthorized access, or server breaches can allow code with malware to be signed and distributed as trusted software.

Automation of code signing workflows reduces the attack surface in the software development lifecycle (SDLC), eliminating points of vulnerability by centralizing management and workflows and improving end-to-end security from user access to software release. Integration with DevOps processes ensures that this improved security posture is achieved without slowing down release cycles.




**Integration and automation of code signing workflows within a CI/CD process using DigiCert® Secure Software Manager improves software security and enforces policy compliance.**

# DigiCert® Secure Software Manager Overview

DigiCert Secure Software Manager improves software security with code signing workflow automation that reduces points of vulnerability and delivers end-to-end company-wide security and control in the code signing process. Key capabilities and feature highlights include:

## **Secures Keys** preventing unauthorized access or misuse

- Integration with on-premises or cloud-based Hardware Security Modules (HSM)
- Granular, role-based access supporting dual-user confirmation and separation of duties
- Off-line and on-demand scheduling modes to define authorized scheduling windows and facilitate remediation
- Key access profiles supporting open or restricted access policies
- Key type profiles supporting production and test usage cases
- Static, dynamic, and roaming key usage models

## **Enforces Policy** ensuring consistency of compliance with security policies and practices

- Account management controls for configuration of features, user structures, roles, and permissions
- User access and management controls that prevent unauthorized access and use
- Key and certificate security controls that map key usage to use case needs
- Certificate profile templates and workflows to increase efficiency and reduce error
- Centralized controls delivering crypto-agility in responding to changing industry compliance requirements
- Dedicated private CA options for securing specific environments

## **Centralizes Management** delivering full tracking for fast remediation and audit/compliance

- Centralized logging and reporting of who signed what when, facilitating threat detection and analysis
- Offline key modes to support investigation of suspicious activity
- Centralized, fine-grained account, user, key and certificate controls for consistency of code signing practices
- Supports import of other CA and self-signed certificates

## **Integrates with CI/CD Pipelines** delivering security while supporting DevOps agility

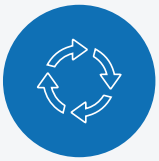
- Native support for various CI/CD platforms and client-side libraries for maximum flexibility
- Supports integration via scripts that can be automatically called from within CI/CD pipeline
- Supports signing of hash files, reducing footprint of transferred files for higher security and speed
- Supports reproducible build checks to screen for insertion of code during the build process

digicert®

# Common Use Cases

**Published Applications**

**In-house applications**



**Testing**

**Containers**

**IoT Firmware**

**Images**

# Key Differentiators

## End-to-end security

Secure Software Manager delivers the benefit of code signing trust while reducing the points of vulnerability in the software development life cycle (SDLC), with fine-grained controls for account management, user access and management, key and certificate handling, integration and automation, and centralized logging and reporting.

## Enterprise configuration

Secure Software Manager is highly flexible and configurable, meeting the unique needs of a company's organizational structure and security process, with the ability to support the diverse requirements of different engineering groups or business units.

## Release process controls

Secure Software Manager includes the ability to verify that the code being signed during the release process matches a baseline build. This step helps prevent the insertion of malware into a code signing workflow.

## Experts in PKI and compliance

DigiCert's deep expertise in PKI and leadership in security standards and consortiums ensures that customers benefit from both best-in-class software and insights into industry developments in cryptography standards.

# Deployment Options

DigiCert® Secure Software Manager is built on a containerized architecture with automated orchestration technology, delivering a consistent level of performance with resources that scale with your needs.

- On-premises and cloud (customer or vendor-managed) deployment options
- Supports high volume use cases
- Rapid deployment with fast time to value

# Supported Technologies

## Code Binaries

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

## Cryptographic libraries

Apple CryptoTokenKit, Microsoft CNG/KSP, PKCS#11

## Continuous Integration Continuous Delivery (CI/CD) Platforms

Apache Ant, Apache Maven, Azure Pipelines, Gradle, Jenkins

## Hardware Security Modules (HSMs)

Thales Luna Network HSM and Luna USB HSM, Thales Luna Cloud HSM

## Services

Multi-factor Authentication (MFA)

# 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

© 2021 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.