END-TO-END CODE SIGNING SECURITY CONTROLS

The recent rise in software supply chain attacks requires organizations to review the security of the entire software development lifecycle (SDLC). Manual code signing practices can create process inconsistencies and points of vulnerability that can be targeted by malicious actors. DigiCert® Secure Software Manager improves security posture, maps key and certificate usage to business needs, and delivers seamless and consistent strong security in code signing.

The Security Features of DigiCert® Secure Software Manager

- Account Management Controls
- User Access & Management Controls
- Key & Certificate Security Controls
- Software Release Security Controls
- Tracking & Reporting
- Automation

Account Management Controls

Account management controls enable organizations to enforce corporate security policies, separate roles and duties, and standardize key security practices that prevent theft and misuse.

Key Features	Benefits
Central account configuration	Flexibility in configuring account features, controls, and user structures to meet the security needs of the organization.
Granular access controls	Prevents unauthorized users from creating keys or certificates that are not associated with their work.
Account-level controls	Enforces policy compliance with controls on algorithms, key size or curve strengths for keypair generation at the account level.
Import of other keys	Provides visibility and control through consolidation and management of the full signing key and certificate landscape.

User Access and Management Controls

User access and management controls ensure that only authorized users have access to designated system functions, minimizing both unintentional or malicious actions and supporting compliance with policy.

Key Features	Benefits
Granular user roles and permissions	Defines system access by user roles, supporting separation of duties and enabling rapid enablement, suspension, removal, or short-term access.
Quorum permissions	Eliminates single point of vulnerability for critical functions, requiring dual user confirmation for specified activities.
Group-level profiles	Improves efficiency, with assigning and revoking of keypair and certificate profiles governing access and generation rights to groups of users.
Multi-factor Authentication (MFA)	Enforces zero-trust policy for account access.

Key & Certificate Security Controls

Sophisticated key and certificate security controls reduce theft and misuse with improved key handling security.

Key Features	Benefits
Key access profiles	Supports multiple security use cases, with "open" settings for access by all authorized signers, and "restricted" settings for tighter security controls.
Key storage options	Provides key storage options for public and private trust use cases, including storage in Hardware Security Modules (HSMs) for public trust.
Production and test signing key types	Defines separate production and test key types. Production keys are evergreen and used to sign public or private binaries and to generate new certificates. Test keys expire within 30 days and are used on-demand for internal release validation.

Static, dynamic, and rotating key usage models	Maps key usage models to the security requirements of major software platforms: • Android: Static keys using the same key/certificate for each application release. • Java & IoT: Dynamic keys with a 1:1 key-to-signature relationship. • Microsoft Smartscreen Filter: Rotating keys cycling through a certificate pool.
On-line and off-line signing key modes	Allows tighter security control for sensitive projects or threat investigation. Online mode allows key use at any time by authorized users. Offline mode prevents key use until keys are brought back online or a scheduled release window created.
Certificate profile templates and certificate generation workflows	Improves compliance, saves time, and reduces errors. Pre-defined attributes can be stored as certificate profile templates and used in certificate generation workflows with a single click in the UI or as part of a command or script.
Granular keypair profile controls	Centralizes management of keypair profiles, improving cryptographic agility and reducing the use of keys with weak or non-compliant cryptographic elements. Keypair profile controls can be set for algorithms, key size, and curves.

Software Release Security Controls

Software release security controls provide tighter security during the release process, thwarting software supply chain attacks targeting internal development.

Key Features	Benefits
Release window	Reduces opportunities for malicious activity during the release process. Predefines release attributes: authorized users, key types (e.g. online, offline, or test), the number of binaries, start and end date/time, pre-authorized signing windows, and release metadata. Setup and approval supports policies requiring separation of duties.
Release comparison	Provides confirmation that malware has not been injected during the release process. Defines a baseline build that acts as a control for what can be signed in the production release, fulfilling the principle of reproduceable builds and providing a verifiable path from source code to product binaries.

End-to-End Tracking & Reporting

Centralized, end-to-end tracking and reporting facilitates threat analysis and detection, supports fast remediation of malicious actions or errors, and supports industry standards certification and audit.

Key Features	Benefits
Centralized logging and reporting, supporting auditing and tracking activity	Delivers full visibility and control of code signing activity, with detailed logging of activity related to accounts, keypairs, certificate operations, and signatures. Both successful and failed events are captured to provide insights for future corrective actions. Reports can be filtered and exported as raw or formatted data or via APIs.

Automation

Automation prevents manual errors, improves efficiency, and drives consistency in signing practices.

Key Features	Benefits
Integration with Continuous Integration/Continuous Delivery (CI/CD) processes	Automates signing processes, providing security without slowing down agile development. Integrates directly with major CI/CD platforms. DigiCert client-side libraries can be called automatically via scripts.
Centralized and preconfigured access and privileges for developers and build servers	Increases security compliance and user convenience, with pre-configured controls that enable signing to occur without direct intervention. Controls can be set from a central panel and timebound to specified intervals. Build servers can be configured as an API user for automatic processing of signing requests.
Hash signing	Reduces the risk of source code interception, as source binaries do not leave the development environment. Hash files are uploaded for signing, reducing the footprint of transferred files and latency associated with transfer of full binaries.

For more information or to request a free trial, call 1.801.770.1736, email pki_info@digicert.com, or visit digicert.com/secure-software-manager.