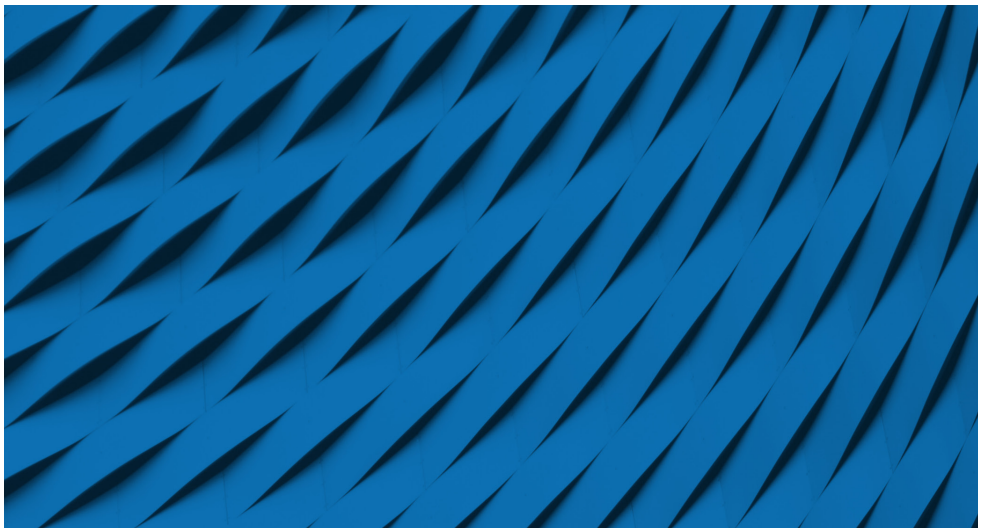
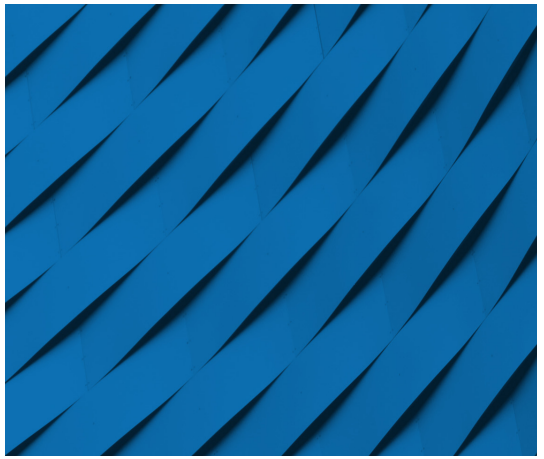
KAUFLEITFADEN

BEWERTUNG VON SIGNIERSOFTWARE UND EINFÜHRUNG EINER CODE-SIGNING-RICHTLINIE



Best Practices, die im Veröffentlichungsprozess für Software größere Sicherheit herstellen ohne die CI/CD-Pipeline zu bremsen



digicert®

EINFÜHRUNG

Angriffe auf die Softwarelieferkette und andere Formen der Malwareverbreitung können das Kundenvertrauen erschüttern und ihre Behebung kann viel Zeit und Geld kosten. Solche viel beachteten Angriffe können zu Datenpreisgabe sowie Lösegeldforderungen führen und das gesamte System lahmlegen.

Gleichzeitig haben sich die Schwachstellen in der Softwaresicherheit ausgebreitet. Durch die agile Entwicklung hat sich die Taktung der Programmierzyklen erhöht. Bereitstellung in der Cloud und Orchestrierung haben den Ort der Softwarebereitstellung verschoben. Nicht zuletzt macht die Verbreitung vernetzter Geräte sichere Firmware-Updates und Kommunikation notwendig.

Für Unternehmen heißt das, dass sie nun mehr als je zuvor den Sicherheitsstatus ihrer Softwareentwicklungszyklen verbessern müssen. Code-Signing-Software zentralisiert die Verwaltung von Code-Signing-Aktivitäten und führt dadurch zur Standardisierung und Durchsetzung der Code-Signing-Richtlinien und -Praktiken, die Schwachstellen in Software reduzieren.

Lassen Sie sich bei der Bewertung und Einsetzung von Code-Signing-Softwarelösungen von den folgenden Kriterien leiten:

1. flexible Konfigurationsmöglichkeiten
2. umfassende Verfahren für die Schlüsselspeicherung und -handhabung
3. Integration und Automatisierung von Workflows
4. zentralisierte und flexible Berichterstellung
5. Steuerungen des Veröffentlichungsprozesses
6. flexible und skalierbare Bereitstellung

Dieser Kaufleitfaden wendet sich an Kunden, die größere Sicherheit bei der Softwareveröffentlichung anstreben. Sie erhalten folgende Hilfestellungen:

- Kriterien zur Bewertung von Code-Signing-Plattformen
- Erfahrungen von Kunden zur erfolgreichen Einführung von Code-Signing-Richtlinien und -Praktiken

FLEXIBLE KONFIGURATIONSMÖGLICHKEITEN

Die feinkörnige Konfigurierbarkeit von Kontostrukturen, Benutzerrollen und Berechtigungen ermöglicht es Unternehmen, Systemfunktionen ihren speziellen organisatorischen Anforderungen anzupassen.

Ziele

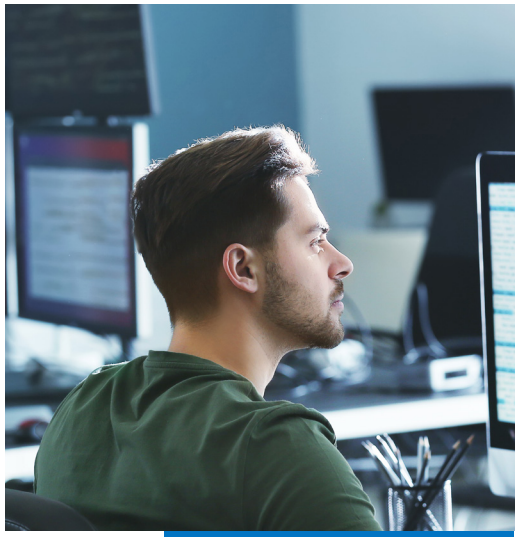
- Zentralisierung der Verwaltung von Signierschlüsseln und Zertifikaten des gesamten Unternehmens
- Anpassung der Kontostrukturen und -funktionen an die Sicherheitsanforderungen
- Beschränkung des Systemzugriffs auf bestimmte Nutzer
- Beseitigung einzelner Schwachstellen, die allein einen erfolgreichen Angriff ermöglichen, für wichtige Funktionen
- Durchsetzung des Zero-Trust-Prinzips für den Kontozugriff
- Verbesserung der Effizienz bei der Zuweisung und Zurücknahme von Systemprivilegien

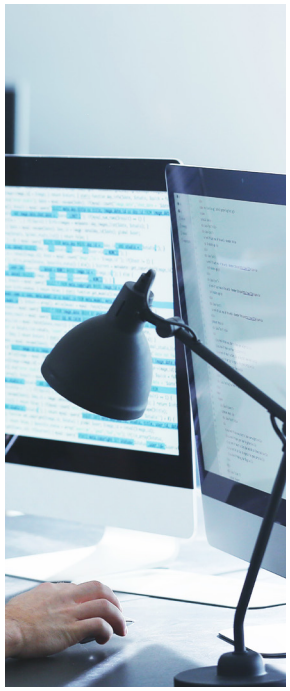
Erforderliche Merkmale

- Import von Schlüsseln und Zertifikaten zur Konsolidierung sämtlicher Schlüssel und Zertifikate
- zentrale Verwaltung von Kontokonfiguration und Nutzerstrukturen, einschließlich Einrichtung von ICAs und ICA-Attributen
- granulare Definition von Nutzerrollen und Berechtigungen mit Steuerungen gemäß der Zugriffsrichtlinie
- Quorumberechtigungen für Funktionen, die eine Genehmigung von zwei Seiten erfordern
- Unterstützung von Multifaktor-Authentifizierung
- Profile auf Gruppenebene

Code-Signing-Richtlinie und -Praxis – Tipp 1

Kunden berichteten von unterschiedlichen Vorgehensweisen zur Paarung ihrer Code-Signing-Richtlinie mit der Nutzung von Code-Signing-Software. Manche gaben an, ein formelles Richtliniendokument erstellt zu haben. Andere setzten auf Leitlinien und Schulungen als Anleitung zu Code-Signing-Praktiken und wieder andere auf den Einsatz von Software zur zentralen Durchsetzung der Richtlinie.





Code-Signing-Richtlinie und -Praxis – Tipp 2

Kunden nannten die folgenden Punkte als die drei wichtigsten Fragen beim Umgang mit Schlüsseln: Wer verwaltet die Schlüssel, welche Schlüssel werden gespeichert und wie werden Signierberechtigungen definiert und durchgesetzt?

UMFASSENDE VERFAHREN FÜR DIE SCHLÜSSELSPEICHERUNG UND -HANDHABUNG

Mit feinkörnigen Steuerungen für die Schlüsselspeicherung und -handhabung können Unternehmen Inkonsistenzen beim Umgang mit Schlüsseln innerhalb des Unternehmens beseitigen und dem Zugriff und der Nutzung durch Unbefugte oder aus Versehen vorbeugen.

Ziele

- Auswahl eines Verfahrens zur Schlüsselspeicherung, das den Sicherheitsanforderungen am besten entspricht (z. B. öffentliche oder private Vertrauenslösung)
- Implementierung strengerer Steuerungen für sensible Projekte
- Zugriffsbeschränkung während der Untersuchung möglicher Bedrohungen
- getrennte Praktiken der Schlüsselnutzung für Produktions- und Testumgebungen
- Anwendung des für die Anforderungen der Zielsoftware geeigneten Schlüsselnutzungsmodells
- Reduzierung der Nutzung von Schlüsseln mit veralteten, schwachen oder nicht vorschriftsgemäßen Verschlüsselungselementen
- Steigerung der Effizienz und Vermeidung menschlicher Fehler

Erforderliche Merkmale

- Optionen für die Schlüsselspeicherung in Hardware-Sicherheitsmodulen (HSM) oder verschlüsselten Speichern
- Schlüsselzugriffsprofile, die regeln, wer wann auf welche Schlüssel zugreifen darf
- Online- und Offline-Signiermodi, die eine schnelle Reaktion ermöglichen
- verschiedene Schlüsselarten für Produktion und Test
- Schlüsselrotation, statische und dynamische Schlüsselnutzungsmodelle
- granulare Steuerungen für Schlüsselpaarprofile
- Vorlagen für Zertifikatsprofile und Workflows für die Erzeugung mit einem Klick

INTEGRATION UND AUTOMATISIERUNG VON WORKFLOWS

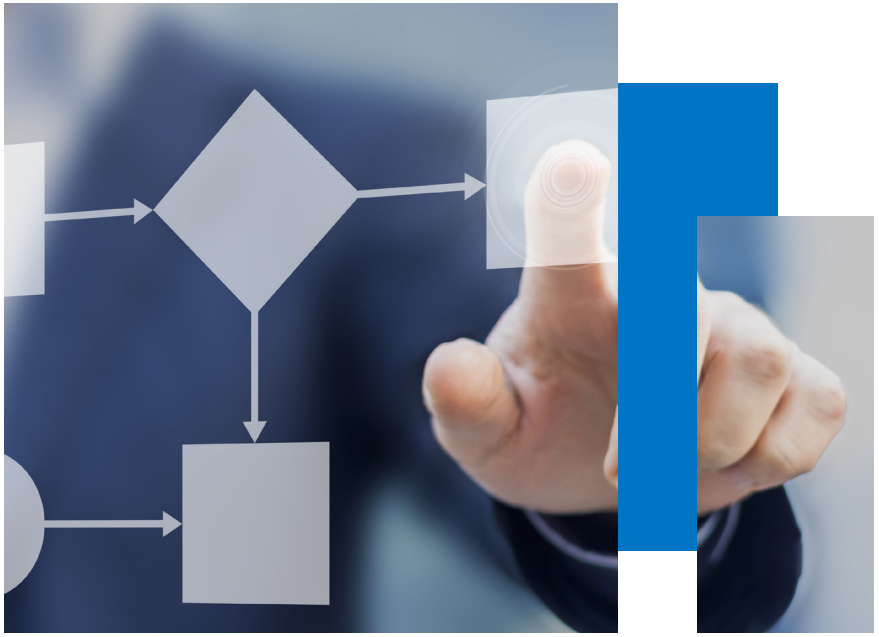
Integration und Automatisierung verhindern manuelle Fehler, verbessern die Effizienz, fördern eine konsistente Signierpraxis und unterstützen die Markteinführungsziele der agilen Entwicklung.

Ziele

- Sicherheit, ohne den Entwicklungsprozess zu bremsen
- ein höheres Niveau der Unternehmenssicherheit und Compliance durch Verbesserung der Benutzerfreundlichkeit im Vergleich mit manuellen Signierprozessen
- Minimierung des Risikos, dass Quellcode während des Signierprozesses abgefangen wird

Erforderliche Merkmale

- Verknüpfung mit CI/CD-Pipelines, optional mit Befehlszeile, Konsole oder API
- Unterstützung mehrerer CI/CD-Plattformen
- Zentralisierung und Vorkonfigurierung von Zugriff und Privilegien für Entwickler und Build-Server
- vorkonfigurierte Zertifikatsvorlagen und Zertifikatserzeugung
- Hash-Signing zur Beseitigung der Notwendigkeit, Quellcode zu übermitteln



Code-Signing-Richtlinie und -Praxis – Tipp 3

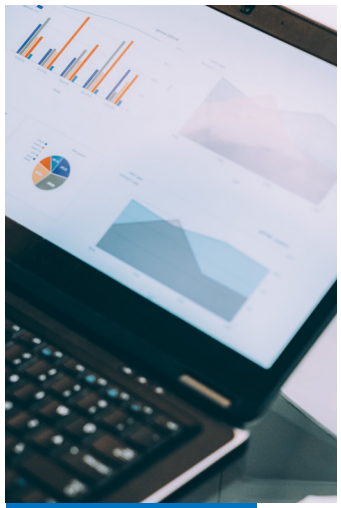
Kunden gaben an, dass geschäftliche bzw. gesetzliche Compliance sowie Anforderungen von Kunden und Plattformen die Hauptantriebsfaktoren für die Entwicklung einer Code-Signing-Richtlinie und -Praxis waren.

Code-Signing-Richtlinie und -Praxis – Tipp 4

Kunden berichteten, dass ihre Code-Signing-Richtlinie, durchgesetzt durch eine Code-Signing-Software und unter Leitung einer festgelegten Sicherheits- oder IT-Abteilung, sehr effektiv ist.

Code-Signing-Richtlinie und -Praxis – Tipp 5

Kunden stellten fest, dass sowohl Sicherheits- als auch IT-Teams bei der Erstellung der Code-Signing-Richtlinie eine wichtige Rolle spielten. Zu den Beteiligten zählten der CISO, das Compliance- und Risikomanagement, DevOps, SecOps, Produktmanagement sowie die Teams für Cybersicherheit und IT.



STEUERUNGEN DES VERÖFFENTLICHUNGSPROZESSES

Steuerungen des Veröffentlichungsprozesses stellen zusätzliche Prüfungen bereit, die dazu beitragen können, der Einschleusung von Malware während des eigentlichen Schreibens vorzubeugen.

Ziele

- Reduzierung der Möglichkeiten schädlicher Aktivitäten während des Veröffentlichungsprozesses

Erforderliche Merkmale

- Attribute und Steuerungen für das Release-Zeitfenster zur Definition des Nutzerzugriffs, vorgegebener Zeitfenster und anderer Kriterien zur Beschränkung des Zugriffs befugter Benutzer
- Funktionen für den Release-Vergleich, die auf der Basis des Prinzips reproduzierbarer Builds einen „Goldstandard“ definieren, der dann als Vergleichsgröße für spätere Builds herangezogen wird

ZENTRALISIERTE UND FLEXIBLE BERICHTERSTELLUNG

Zentralisierte Berichterstellung trägt dazu bei, Probleme schneller zu beheben, Audit-Anforderungen zu erfüllen und mögliche Probleme oder Bedrohungen zu identifizieren.

Ziele

- vollständiger Überblick und Kontrolle der Code-Signing-Aktivitäten
- Kenntnis, wer wann was signiert hat, zur schnelleren Problembehebung
- Compliance und Audit-Fähigkeit

Erforderliche Merkmale

- zentralisierte Protokolle und Berichte zur Unterstützung von Audits und Nachverfolgung
- Berichtsfilter mit Export in rohe und formatierte Dateitypen

Code-Signing-Richtlinie und -Praxis – Tipp 6

Kunden identifizierten zwei wichtige Maßnahmen: die Standardisierung des Code-Signing-Prozesses, wodurch dieser dokumentiert, nachvollziehbar, verfolgbar und sicher wird, und die Gewährleistung der Quelle und Integrität der Softwarepakete des Unternehmens gegenüber dessen Kunden und Benutzern.

FLEXIBLE UND SKALIERBARE BEREITSTELLUNG

Unternehmen sollten auf Auswahlmöglichkeiten beim Bereitstellungsmodell achten, damit sie innerhalb des Unternehmens verschiedene Bereitstellungsanforderungen erfüllen können, und die Skalierbarkeit von Lösungen im Hinblick auf ihre voraussichtlichen Signieranforderungen prüfen.

Ziele

- Möglichkeit der Bereitstellung auf die gewünschte Weise
- Unterstützung eines großen Volumens und Durchsatzes von Signieraktivitäten
- effiziente Einrichtung und Skalierbarkeit im Bedarfsfall

Erforderliche Merkmale

- On-Premises-, Cloud- und Hybridoptionen zur Unterstützung umfassender Bereitstellungsanforderungen im gesamten Unternehmen
- schnelle und effiziente Einrichtung von ICAs für Abteilungen mit besonderen Anforderungen an die Sicherheitskonfiguration
- containerbasierte Architektur mit Orchestrierung zur schnellen und effizienten Skalierung

ZUSAMMENFASSUNG

Code-Signing-Software kann die Schwachstellen in Veröffentlichungsprozessen für Software signifikant reduzieren. Lösungen der Enterprise-Klasse, die flexibel konfigurierbar sind und umfassende Funktionen bieten, sind am besten geeignet, um die Ziele, die ein Unternehmen mit seiner Code-Signing-Richtlinie und -Praxis verfolgt, zu erreichen. Diese Lösungen bieten Folgendes:

Schutz

- Beseitigung von Schwachstellen, die den Diebstahl oder Missbrauch von Schlüsseln begünstigen
- Verhinderung der Einschleusung von Malware während des Veröffentlichungsprozesses

Verwaltung

- Förderung von Konsistenz des Sicherheitsstatus und der Compliance über Programmierteams hinweg
- zentralisierte Übersicht und Kontrolle über Code-Signing-Aktivitäten

Produktivität

- Verbesserung der Effizienz und Vermeidung menschlicher Fehler
- Erlangung von Flexibilität bei Änderungen der Verschlüsselung und Compliance

KLINGT GUT?

Als vertrauenswürdiger Sicherheitspartner bietet DigiCert weltweit eine breite Palette an SSL-, PKI- und IoT-Sicherheitslösungen der Enterprise-Klasse zum Schutz der geschäftskritischen Daten vieler führender Unternehmen. Sprechen Sie mit unseren Experten über Ihre Anforderungen.

Weitere Informationen erhalten Sie unter +1 801 770 1736, pki_info@digicert.com oder digicert.com/de/secure-software-manager