digicert®

DEVOPS-LEITFADEN FÜR REIBUNGSLOSES, SICHERES CODE-SIGNING

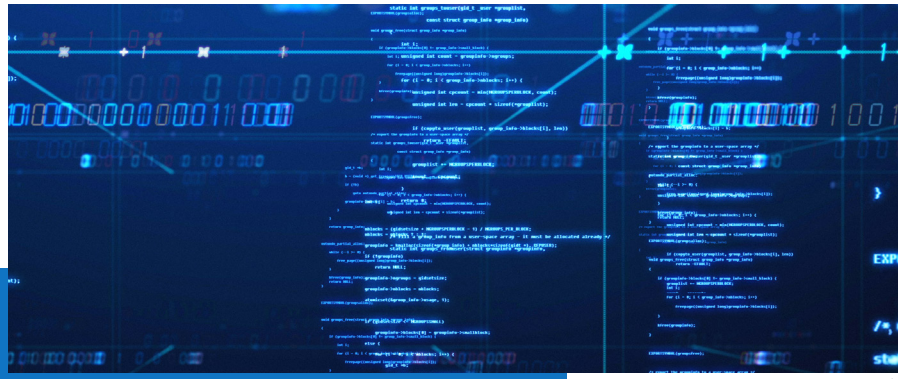
Sicheres Signieren war einmal eine Hürde für DevOps. Aber das ist nun vorbei. Hier erklären wir, warum das neue Verfahren der reibungslose und beste Schutz für die Software ist, die Sie entwickeln und veröffentlichen.

FRÜHER	HEUTE
• manuelles Signieren • gemeinsame Nutzung von Schlüsseln • inkonsistente Prozesse • unzureichende Transparenz • schwierige Problembehebung	• automatisierte Signatur-Workflows • Speicherung von Schlüsseln in HSM • Zugriffskontrollen • zentralisierte Nachverfolgung • schnelle Problembehebung

Was spricht gegen die alte Methode?

Früher war das Signieren von Software nicht nur mühselig und schwierig zu verwalten, sondern ließ im Veröffentlichungsprozess für Software auch Sicherheitslücken offen. Manuelle Signiermethoden waren mit zusätzlichem Aufwand verbunden, wodurch das Signieren zu einer lästigen Aufgabe wurde, die die Softwareentwicklung bremste und viele dazu verleitete, diesen wichtigen Schritt ganz auszulassen. Skriptloses Kodieren bedeutete, dass dem Ingenieur die Aufgabe zufiel, mühsam die Entwicklungsschritte hinsichtlich der richtigen Signierphase zu überwachen.

Bezüglich der eigentlichen Sicherheit war das alte Verfahren nicht nur langsam und aufwendig, sondern erfüllte auch nicht den Zweck, robuste Sicherheit zu schaffen. Lokal gespeicherte Zertifikate können verloren gehen, gestohlen oder missbraucht werden. Private Schlüssel können nicht verfolgt und kontrolliert werden, wodurch Mitarbeiter signieren können, wenn sie nicht sollten, Schlüssel unbeaufsichtigt weitergegeben werden können und Audits und Problembehebung erschwert, wenn nicht unmöglich gemacht werden.



Heute ist Signieren einfacher und sicherer

Heute kann Signieren in CI/CD-Pipelines integriert werden, wodurch es praktisch mühelos wird. Wir nennen das „kontinuierliches Signieren“. Automatisierte Prozesse sorgen dafür, dass im richtigen Moment signiert wird, ohne dass eine manuelle Überwachung erforderlich ist. Und mit skriptbasierten Tools können sich die Ingenieure auf Entwicklung, Kodierung und Feedback konzentrieren, während der Signing Manager während des gesamten Builds Signaturprozesse ausführt.

Diese neue Art des Signierens bietet auch das höchste Sicherheitsniveau und schützt dabei Ingenieure, Teams und Unternehmen vor Fehlern und Missbrauch. Schlüssel werden in Sicherheitsmodulen (HSM) oder Softwarelösungen zum Signieren gespeichert, wo sie vor Verlust, Diebstahl sowie unbefugter Weitergabe und Nutzung sicher sind. Abteilungs- und Teamleiter können diese Zertifikate und die Nutzung von DevOps-Schlüsseln mühelos überwachen und prüfen und Probleme im Bedarfsfall beheben.

Die reibungslose Nachverfolgung ist jetzt die sichere Nachverfolgung

Wenn das Signieren reibungslos und sicher erfolgt, können sich die Ingenieure stattdessen besser auf die erfolgreiche Programmierung der Software konzentrieren. Das ist wichtig, da Angriffe auf die Softwarelieferkette auf dem Vormarsch sind und das Signieren von Software somit ein entscheidender Faktor der kontinuierlichen Bereitstellung ist. Mit Continuous Signing von DigiCert schützen Ingenieure ihren Code ununterbrochen.

Sie möchten gerne mehr über die Automatisierung des Signierens Ihrer Software erfahren?
Weitere Informationen erhalten Sie unter digicert.com/de/signing/secure-software-manager