digicert®

A DEVOPS GUIDE TO FRICTIONLESS, SECURE CODE SIGNING

Secure signing used to be a barrier to DevOps. But not anymore. Here's why the new way is the best—and frictionless—way to protect the software you build and release.

THEN	NOW
• Manual signing • Shared keys • Process inconsistencies • Poor visibility • Difficult to remediate	• Automated signing workflows • Keys stored in HSM • Access controls • Centralized tracking • Fast remediation

What's wrong with the old way?

In the past, software signing was not only laborious and difficult to manage, it also left security gaps in the software release process. Manual signing methods required extra effort, making signing a chore that slowed the software development process and led many to skip this important step. Unscripted coding meant that the engineer was tasked with tediously monitoring the development steps for the correct signing stage.

In terms of the security itself, the old way wasn't just slow and burdensome, it also failed to provide strong security. Locally stored certificates can be stolen, lost, or misused. Private keys can't be tracked and controlled, meaning individuals can sign when they shouldn't, can share keys without oversight, and auditing and remediation are difficult or impossible.

Signing today is simpler and more secure

Today, signing can be integrated into CI/CD pipelines, so it's virtually effortless. We call this Continuous Signing. Automated processes ensure signing occurs at the right stage without the need for manual monitoring. And with scripted tools, engineers can focus on design, coding, and feedback, while DigiCert Software Trust Manager continuously runs signing processes throughout the build.

This new way to sign also delivers the strongest level of security while protecting engineers, teams, and organizations from misuse and mistakes. Keys are stored in HSMs or in signing solution tools, where they're protected from loss, theft, and unauthorized sharing and activity. For managers and team leaders, these certificates and DevOps key usage can be easily monitored, audited, and remediated if an issue arises.

The frictionless track is now the secure track

When signing is frictionless and secure, engineers can focus more on building great software and less on signing—which is important because, with software supply chain attacks on the rise, software signing is a crucial component of Continuous Delivery. With Continuous Signing from DigiCert, engineers protect their code without interruption.

Interested in learning more about automating your software signing?
Visit us at digicert.com/software-trust-manager