digicert®

How a healthcare technology company modernized code signing development with Software Trust Manager

CASE STUDY

Healthcare technology company secures private keys and streamlines compliant code signing with DigiCert Software Trust Manager

Executive Summary

Industry: Technology
Headquarters: North America

Key business requirements:

- Centrally audit and enforce code signing policies across development teams and codebases
- Comply with CA/Browser Forum secure hardware key storage mandate to protect private code signing keys
- Ensure that code signing adheres to evolving global regulations
- Reduce DevOps workload and responsibilities by automating CI/CD processes

Solution:

- DigiCert Software Trust Manager

Key outcomes:

- Company eliminated risk of private key theft by migrating to cloud-based HSM
- Development teams now operated under centralized role-based access controls and team privileges
- Code signing brought into compliance with global regulations and could be audited
- DevOps code signing processes were automated to ensure smooth CI/CD release flow while maintaining security

Requirement

Replace legacy code signing system to ensure global compliance and consistency

A technology company was in a bind. For decades, they had provided Windows-centric solutions for healthcare organizations, and their homegrown code signing system, which supported Microsoft Authenticode, automated code signing for Windows builds. Over the last decade, however, the company expanded software development to provide solutions that worked on other operating systems like macOS, iOS, and Android. But scrum teams working in these codebases couldn't use Authenticode and had to sign code manually, using local tools. As a result, each team handled code signing differently, leading to release delays and other mishaps caused by human error.

This lack of enterprise-wide standards for code signing was not their only concern. More pressing was the company's inability to comply with evolving regulations and standards. Although the company's headquarters was in North America, any solution they sold had to adhere to the regulations of their customers' countries—and many of their customers were in the EU. This meant that in addition to complying with U.S. regulations like HIPAA and HITECH, they needed to satisfy regulatory demands for such strict EU regulations as GDPR, the Cyber Resilience Act (CRA), and the NIS2 Directive, just to name a few. And the penalties for noncompliance were steep. "It could lead to our products being taken off the market and huge fines. We can't let this happen," explained the company's Senior Director of Product Security.

Moreover, the company couldn't comply with the 2023 CA/B Forum code signing mandate for private keys. Instead of housing private keys in a FIPS 140-2 or CC EAL4+ certified HSM, the system allowed developers to download certificates and private keys to local servers—or even client machines. "This scope of what we needed to correct was daunting, and we needed a solution that could handle all these issues," the senior director said.

Solution

DigiCert Software Trust Manager centralized code signing while automating regulatory compliance

After investigating cloud provider solutions like AWS CloudHSM, the company chose DigiCert Software Trust Manager as their code signing solution. Unlike CloudHSM, which requires extensive custom development, Software Trust Manager is a SaaS solution, providing centralized code signing management across all development teams and environments. It also provided the company important out-of-the-box features, including the ability to set role-based access controls (RBAC) and integrate with multiple toolchains and workflows, as well as a cross-platform command-line interface (CLI) tool called Signing Manager Controller (SMCTL) that would facilitate secure code signing and private key management.

Software Trust Manager could also solve the company's pressing concerns about adhering to all the standards and regulations that their legacy system could not. "Regulatory governance is baked in, and we no longer have to worry about whether we're storing our keys properly," said the senior director. "We can trust it to maintain compliance, even as we continue to grow, without any maintenance or custom development on our end."

Eliminating risk of private key theft

First, Software Trust Manager helped the company secure all their private code signing keys by migrating all of them to cloud-based, DigiCert-managed HSMs. All authorized developers, no matter where they were located, could use these keys to sign code, but they no longer had direct access to key material or the responsibility of managing them. "Instead of having to manage the keys themselves, they only need to send file hashes for signing," the senior director said. "They no longer can copy keys or store them in random places. As a result, the risk of these keys getting stolen or abused is down to about zero."

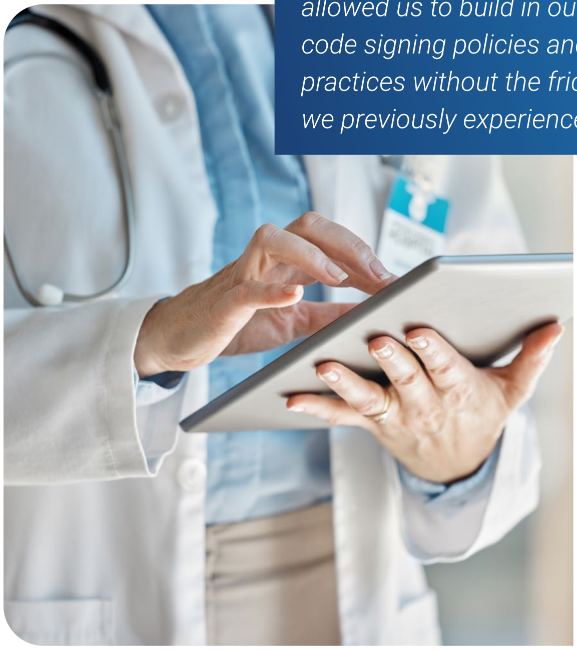
Moreover, the company no longer had to worry about maintaining compliance with the 2023 CA/B Forum mandate surrounding private key storage. Software Trust Manager kept detailed logs to simplify audits, as well as reduce compliance overhead across jurisdictions. "This is something that we simply no longer could handle by ourselves. It would have been a huge drain on our resources and too great a risk internally and for the security of our customers," the senior director said.

Standardizing code signing across globally distributed development teams

Using Software Trust Manager, the company was able to set up a centralized and standardized system across all company divisions. Now the company could enforce governance worldwide while reducing administrative overhead. This centralization extended to setting up both role- and team-based access controls, embedding policies into workflows, and simplifying oversight using a departmental administrator model.

"Software Trust Manager allowed us to build in our code signing policies and practices without the friction we previously experienced," said the senior director. "Within six months we were able to onboard all our development teams to the new system. And it didn't matter whether they were in the U.S., Romania, or the moon—things just worked. And they continue to work as we continue to grow."

> *"Software Trust Manager allowed us to build in our code signing policies and practices without the friction we previously experienced."*



Reducing developer workload through automation and CI/CD integration

In addition, developers no longer were forced to set up their own credentials or individually upload and update libraries to sign code. They just needed to call the SMCTL tool and make simple signing requests through its CLI. Software Trust Manager did the rest. And by integrating Software Trust Manager into Jenkins, the company could automate their CI/CD pipeline, helping developers move faster without sacrificing security or compliance. Software Trust Manager even provided an "Unsigned" feature that ensured that Software Trust Manager signed only unsigned files while ignoring ones that already have been signed.

Because Software Trust Manager works across all development environments, all the company's developers had access to automated, policy-driven workflows that accelerated release cycles. And it didn't require them to learn any new tooling because Software Trust Manager comes with APIs that integrate with Java, Python, iOS, macOS, and other programming languages, as well as Windows. Said the senior director: "When we purchased Software Trust Manager, we were mostly concerned with compliance across our development environments. What we didn't anticipate was the way it has removed most of the security concerns our developers previously had to contend with. Now they can focus almost entirely on building the best software possible for our customers. That's about the best business case I could've hoped for."

Discover how DigiCert helps global enterprises strengthen software supply chain security.

Detects malware
Highlights vulnerabilities
Identifies legacy software
Supports confident releases
digicert ONE

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2025 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.