digicert®

Trust Lifecycle Manager Helps Insurance Company Lock Down Environments without Locking Out Developers

CASE STUDY

Trust Lifecycle Manager Helps Insurance Company Lock Down Environments without Locking Out Developers

Executive Summary

Industry: Insurance
Headquarters: EMEA

Key business requirements:

- Merge multiple, siloed instances of PKI into a single, centrally managed internal PKI
- Centralize inventory and governance of all certificates being used by development teams
- Automate enforcement of company security and regulatory compliance policies
- Make certificate issuance seamless for development teams

Solution:

- DigiCert® Trust Lifecycle Manager

Key benefits:

- DigiCert seamlessly migrated multiple PKIs to a unified centralized internal PKI
- Security team gained single pane of glass visibility into entire certificate population used by developers
- Company could automate all parts of the certificate lifecycle, lessening IT burden
- Automation capabilities enabled enforcement of company security policies on all certificates being used by developers, including ephemeral certificates used in apps
- Developers were relieved of additional security and operational burdens, which enabled them to iterate apps at faster speeds

Requirement

Secure complex, containerized apps without slowing the pace of DevOps

An EU-based insurance provider faced a problem common to many enterprises: Their security team had no visibility into the security practices of their application development teams.

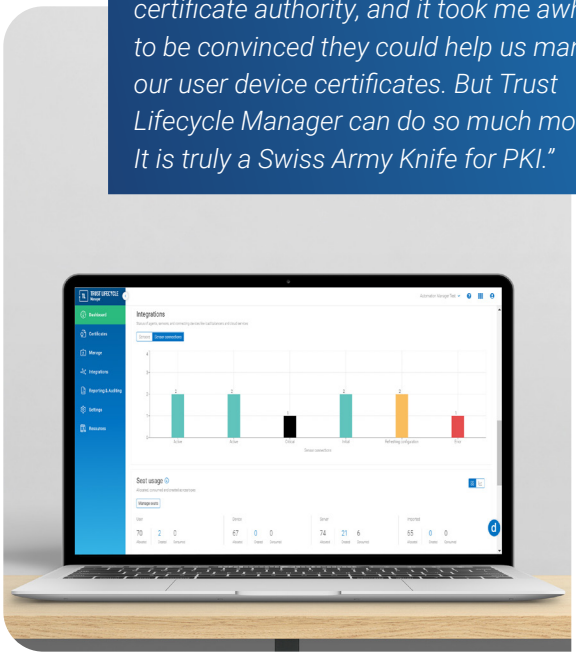
Concerned about this problem, the security team performed an audit. What they learned highlighted the problems caused by siloed teams and a lack of centralized oversight and management:

- Each application had its own internal PKI
- There was no consistency in how digital certificates were being issued and managed
- Enterprise security policies and controls couldn't be enforced
- Weak management of private keys left the company vulnerable to attack and compliance gaps
- Company's microservices-based apps were not in compliance with strict industry and EU regulations

The company's vice president of security acknowledged that his team and the development teams had conflicting objectives. Developers were tasked to build and quickly iterate apps to grow the business, and security was perceived as a hindrance to getting the work done. Most development teams used the ACME protocol to automate certificate deployment. However, ACME lacked visibility features, preventing security teams from tracking the total number of certificates in use, their metadata, or their specific applications.

"We needed to find a solution that would enable us to keep our company secure and also facilitate developers' ability to work fast. Ideally, we needed something that would remove most of the security responsibilities from the developers because they don't have the expertise or the time for that burden," said the vice president. "Then we realized we already had our solution."

"For so long I only saw DigiCert as a certificate authority, and it took me awhile to be convinced they could help us manage our user device certificates. But Trust Lifecycle Manager can do so much more. It is truly a Swiss Army Knife for PKI."



Solution

DigiCert Trust Lifecycle Manager provides unified certificate lifecycle management and managed internal PKI

The company was a longtime DigiCert CertCentral customer and had recently purchased DigiCert Trust Lifecycle Manager to discover and automate user and device certificates to access Wi-Fi and VPN. In discussions with DigiCert, the vice president was reminded that Trust Lifecycle Manager also includes integration with leading cloud and DevOps platforms, including configuration management tool Ansible and container orchestration platform Kubernetes. Also, Trust Lifecycle Manager now provides secrets management through DigiCert's new partnership with HashiCorp.

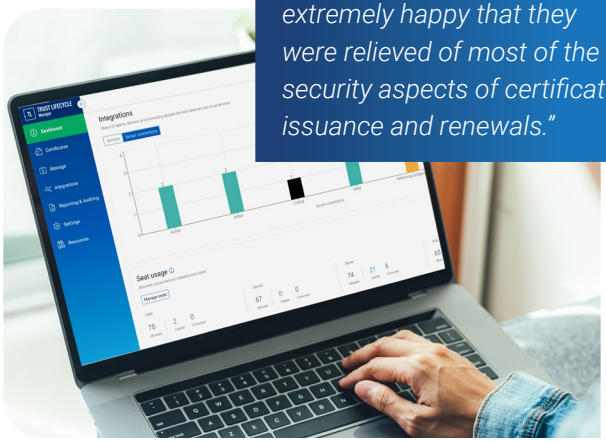
"For so long I only saw DigiCert as a certificate authority, and it took me awhile to be convinced they could help us manage our user device certificates. But Trust Lifecycle Manager can do so much more. It is truly a Swiss Army Knife for PKI," said the vice president.

Migrating multiple internal PKIs into a centralized, unified system

The company first used Trust Lifecycle Manager to identify all of the internal PKIs being used by their development teams. In addition to the ones that were already identified in the audit, Trust Lifecycle Manager found several that had been stood up for apps that had since been deprecated. Trust Lifecycle Manager also discovered the private portion of public/private key pairs, alerting the security team to insecure key management practices.

DigiCert outlined a migration plan that would relocate and merge the active internal PKI into DigiCert's managed PKI-as-a-service, while eliminating the orphaned ones. The new managed PKI would include exporting all private keys into FIPS 140-2 level 3 compliant hardware (HSM), properly configured root certificate authorities and intermediate certificate authorities. Moreover, its architecture would establish a robust security framework that would enhance infrastructure operations by ensuring end-to-end encryption, automated certificate lifecycle management, and seamless integration with enterprise security policies.

Even better, it would not impede developers' work during the transition. "It was done surprisingly quickly, and because of all the integrations, it was a seamless transition. DigiCert's level of expertise in this area is rare, and we're so glad to have it at our disposal," said the vice president. "Finally, we have a line of sight into how our development teams are using their certificates."



"Our development teams were extremely happy that they were relieved of most of the security aspects of certificate issuance and renewals."

Discovering and managing all internal certificates

Just as it provided the company with single pane of glass visibility into their user and device certificates, Trust Lifecycle Manager discovered and made a real-time inventory of all the certificates being used by the development teams. The ability to centralize certificate lifecycle management felt transformational for the security team, which could finally monitor each certificate's lifespan, location, owner, and security algorithms.

But it wasn't enough to have this knowledge without the tools to act on them. Trust Lifecycle Manager automated strict governance for certificate issuance and usage. If a certificate didn't fall within corporate security parameters, it was immediately revoked and replaced. This greatly reduced the risk of certificate mismanagement, shrinking error occurrences and saving time for everyone.

Also, Trust Lifecycle Manager automated all aspects of the certificate lifecycle. Its ability to automate issuance, procurement and renewals, even for those being used by developers within containerized workloads that were previously invisible to the security team, meant that they now had a continuously updated inventory of all certificates used in the company's apps, streamlining operations.

Enable development teams to work even faster

In addition to lessening the burden of certificate management on the security team, Trust Lifecycle Manager also made procuring and using certificates easier and more secure for developers. Trust Lifecycle Manager offers native integration with the ACME protocol, so developers didn't have to learn any new way to obtain certificates. Finally, because Trust Lifecycle Manager's private PKI services automatically store private keys safely in an HSM, it enabled the teams to comply with enterprise security policy and regulatory requirements for secure key storage.

"Our development teams were extremely happy that they were relieved of most of the security aspects of certificate issuance and renewals," the vice president said. "It's an amazing feeling to actually be in sync with the same group we were traditionally at odds with. And Trust Lifecycle Manager can handle as many certificates as we need no matter how many we need. It's amazing that we are at once more secure and in compliance while making life easier for our developers."

Discover how Trust Lifecycle Manager empowers your PKI modernization journey.