

TRUST LIFECYCLE MANAGER IMPROVES EMPLOYEE ACCESS WHILE ENFORCING ASSET SECURITY

Executive Summary

Company name: DigiCert

Industry: Technology

Headquarters: Lehi, UT

Key business requirements:

- Provide a global, hybrid workforce with continuous access to corporate apps and data
- Automate levels of access throughout the employee lifecycle, from onboarding to termination
- Reduce IT helpdesk calls, freeing up IT to work on projects that grow the business

Solution:

- DigiCert Trust Lifecycle Manager with SCEP MDM integration
- DigiCert ONE CA Manager

Key benefits:

- Templates let service desk team easily create certificates that adhere to corporate security policies
- SCEP integrations enable direct certificate autoenrollment through company's MDM solutions
- Automation streamlines management of certificates, reducing complexity and likelihood of certificate-related outages
- Proactive management of certificate lifecycles helps to end service disruptions, cutting helpdesk calls

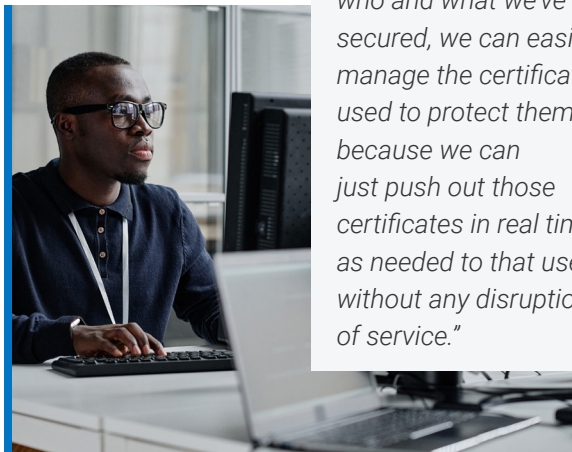
Requirement

Ensure DigiCert employees across the world have continuous access to corporate network

DigiCert's service desk team consists of 15 people who are responsible for more than 1,600 global employees. They ensure these employees can continuously connect to the company's network, apps and data to do their jobs—whether the employee is in an office or working remotely. At the same time, they make certain that ingress is limited only to authenticated users and devices because remote access is such a common attack vector.

The team faced multiple challenges balancing ironclad IT security with uninterrupted access for employees and their devices. For one thing, provisioning user accounts to manage role-based access took time. Moreover, doing so required that user endpoints and company resources could easily connect with one another while seamlessly integrating with Intune (Windows) and Kandji (macOS and iOS) MDM solutions. Finally, the team needed to manage the lifecycles of all the digital certificates required to authenticate the users and devices.





"Not only do we know who and what we've secured, we can easily manage the certificates used to protect them because we can just push out those certificates in real time as needed to that user without any disruption of service."

Too often, they didn't know a client certificate had expired until the affected employee contacted the helpdesk team, unable to figure out why they could no longer access the corporate network. "Each of these helpdesk calls takes a minimum of 10 minutes to diagnose the issue because you have to go through a checklist of best practices to troubleshoot," said Rob Carnesecca, director of IT at DigiCert. "This was especially frustrating when more often than not, an expired certificate was the cause."

Solution

DigiCert Trust Lifecycle Manager provided automated CLM that integrated with MDM platforms

Fortunately, Carnesecca's team had access to DigiCert Trust Lifecycle Manager (TLM), a robust enterprise PKI and certificate lifecycle management (CLM) platform. Unlike competing solutions, Trust Lifecycle Manager could generate and manage the client certificates that authenticate users and devices, as well as provide out-of-the-box integrations with MDM solutions.

Trust Lifecycle Manager could automate all aspects of the certificate lifecycle, from issuance to renewal and revocation.

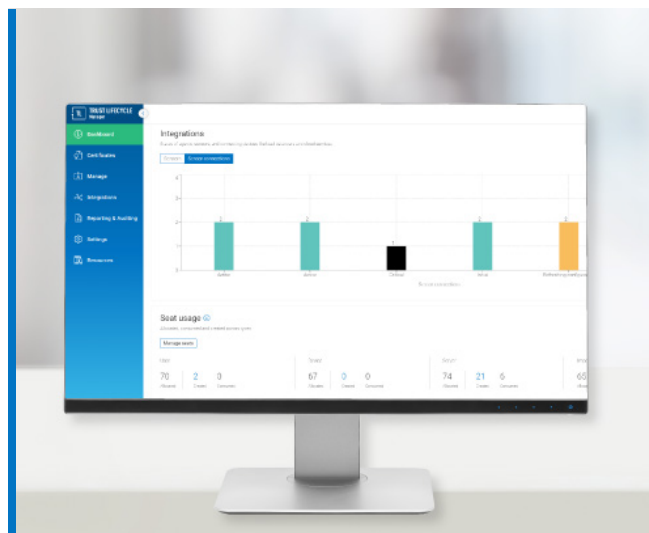
"Trust Lifecycle Manager lets us know what certificates are expiring, and it can automatically renew these certificates as long as the user is active in our system," said Carnesecca. "Not only do we know who and what we've secured, we can easily manage the certificates used to protect them because we can just push out those certificates in real time as needed to that user without any disruption of service."

Leveraging integrations and profiles to streamline CLM

In order to properly install the certificates that authenticate devices, the service desk team needed processes to run through the company's MDM solutions. Trust Lifecycle Manager's SCEP integration enables autoenrollment of certificates, so that a certificate issued from DigiCert ONE Private CA Manager could be handled via Kandji or Intune without having to manually configure or manage the many processes that needed to happen along the way.

In addition, Trust Lifecycle Manager provided a host of profiles that the service desk could set up using easy-to-follow templates to streamline integration. "Because of my limited expertise with certificates, I would have been pretty lost. But TLM provides a template that you can use to set up SCEP bindings," explained DigiCert systems administrator Jordan Wilcox. "Literally, you just choose the SCEP for Intune template, answer a series of questions, and TLM sets up the profile!"

Trust Lifecycle Manager also came with template-based profiles to automate additional integrations with network resources and levels of role-based access, among other options. Added Wilcox: "There are templates that let you configure how long a certificate is valid and to have it renewed before it expires."



Enabling zero touch management and scalability

The ability to automate so many aspects of certificate management meant that Carnesecca's team could now, with minimal overhead, truly leverage PKI to handle all aspects of user and device security quickly. "TLM is so robust. We can lay down one certificate that blesses a device and lets us know it's from DigiCert. Then we can lay down another certificate that talks to our network infrastructure and validates whether the device has access to a specific resource. We can secure applications through a certificate," Carnesecca said. "And we know we have the tools in place where we can rely on TLM's automation to manage that for us."

As Carnesecca pointed out, DigiCert is a geographically dispersed organization, and it would have been hard for his staff to continue to meet all the company's needs without a platform like Trust Lifecycle Manager. "It's important to note that TLM is a global solution that works across the world for us, especially when our resources don't always line up perfectly with our time zones," Carnesecca said. "Because we can automate so many of these tasks, we not only know our users are safe, but we also know our company resources are protected and that we can easily scale up to handle more resources and users without placing additional overhead on my team."

"Because we can automate so many of these tasks, we not only know our users are safe, but we also know our company resources are protected."



"It's a relief knowing that TLM auto-renews certificates so there's no disruption in service. I can set it and forget it because when you need things to be up 24/7, it's one less thing to juggle."



Improving security and accessibility while dramatically reducing overhead

Trust Lifecycle Manager has eliminated the dual challenges of securing DigiCert resources with high availability and ease of use for DigiCert employees. Even better, it has dramatically reduced IT overhead so that team members who often spent large portions of their day responding to helpdesk calls can now focus on projects that maximize business opportunity.

"It's a relief knowing that TLM auto-renews certificates so there's no disruption in service. I can set it and forget it because when you need things to be up 24/7, it's one less thing to juggle," said Wilcox.

Get started today with DigiCert® Trust Lifecycle Manager by contacting us [here](#).