Accelerating Secure Cloud Transformation: Zscaler & DigiCert® ONE

Zscaler Modernizes PKI to Drive Digital Trust and Scale Secure Service-to-Service Communications with DigiCert ONE

Executive Summary

Company name: Zscaler
Industry: Technology
Headquarters: San Jose, CA

Key business requirements:

- Replace multiple, disparate home-grown PKIs with a unified, standards-based PKI
- Ensure secure service-to-service communications across complex, distributed cloud environments
- Use API-based automation to both simplify and improve reliability of certificate lifecycle operations
- Establish a centrally governed digital trust foundation that can scale across all Zscaler product lines

Solution:

- DigiCert Trust Lifecycle Manager
- DigiCert PKI Services

Key outcomes:

- Policy-driven internal PKI aligns with WebTrust standards and governance requirements
- Secure mutual TLS (mTLS) authentication has been implemented across distributed microservices to enable service-to-service trust
- Certificate issuance, renewal, and revocation have been automated through integrated API workflows
- Standards-based trust foundation establishes a repeatable model to power future Zscaler services

Requirement

Replace homegrown internal PKI with a standards-based, scalable foundation for growth

Zscaler, a global leader in cloud security, delivers zero trust protection to enterprises worldwide—safeguarding users, workloads, and devices, regardless of location. Zscaler Internet Access (ZIA), the company's secure gateway for internet traffic, provides customers with a cloud native solution that inspects all traffic for threats, while enforcing cybersecurity and data protection policies. To underpin ZIA as well as other Zscaler solutions, the company had relied on their homegrown internal PKI. However, it was becoming increasingly clear that they needed to modernize in order to keep up with customer requirements and industry best practices—and it made little sense for them to dedicate resources for this continual need to keep pace when PKI expertise was not part of their core skillset.

"Our internal PKI had served us well over the years, but once our cloud infrastructure got to a certain scale for supporting 50 million users on the [ZIA] platform—processing 500+ billion transactions per day, across more than 160 data centers across the globe—it was no longer viable," said Director of Product Management, Lidor Pergament. "PKI is so standards-based. You've got WebTrust standards and cryptographic standards. It's not an area where you should try to reinvent the wheel."

To meet rising customer expectations and stay aligned with industry best practices, Zscaler needed a scalable, standards-based PKI infrastructure that could deliver strong security without constant internal upkeep. And it needed to be a solution that they could deploy quickly, without impacting their customers as part of the migration process.

"Everyone is a DigiCert customer. If you get scrutinized by a federal customer or a bank, the DigiCert brand has so much equity, which in itself gives them comfort."

— Lidor Pergament, Zscaler

Solution

DigiCert® PKI Services and Trust Lifecycle Manager replaced legacy PKI with a scalable cloud trust foundation

After evaluating several solutions including those offered by public cloud vendors, Zscaler chose the DigiCert ONE platform. Only DigiCert ONE could provide a foundational modern PKI infrastructure for the Zero Trust Exchange and ensure comprehensive digital trust to safeguard service-to-service communications at scale.

"We determined that DigiCert PKI Services and Trust Lifecycle Manager would best serve our needs to not only get to market quickly, because we could offload all the hard stuff that's involved in managing internal PKI to DigiCert, but also provide us the most enterprise-grade solution in the industry," said Pergament.

DigiCert's reputation as a leader in the PKI space also played a role in Zscaler's decision. "Everyone is a DigiCert customer. If you get scrutinized by a federal customer or a bank, the DigiCert brand has so much equity, which in itself gives them comfort," Pergament continued. "At the end of the day, it's about trust, and DigiCert supports our ability to ensure trust when we process our customers' sensitive traffic."

Replacing home-grown systems with a standards-based, secure internal PKI

With DigiCert PKI Services, Zscaler modernized their home-grown systems in alignment with WebTrust standards. DigiCert took on the deployment and management of the company's root and intermediate certificate authorities (CAs). The root CA keys were securely hosted on dedicated, offline HSMs (Hardware Security Modules) compliant with FIPS 140-2 standards and housed in DigiCert facilities—an assurance the typical cloud provider solutions simply couldn't offer. "There's no such concept of an offline HSM in the case of a cloud vendor's private CA," said Pergament.
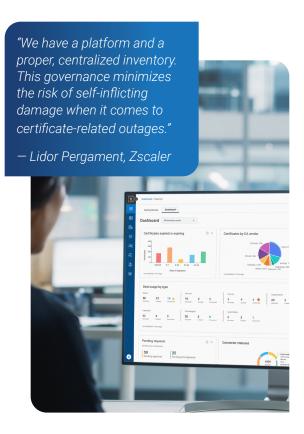
Intermediate CAs now operated from online HSMs, enabling high-volume issuance of short-lived certificates while preserving root key isolation—a best practice for balancing scalability with security. This layered approach helped Zscaler keep pace with evolving regulatory demands and improve operational efficiency. DigiCert PKI Services' flexible architecture also made it easier for Zscaler to adapt quickly to future security and compliance requirements without needing to overhaul their entire system.

Orchestrating secure service-to-service communication at scale

Supported by a secure internal PKI foundation, Zscaler now had the ability to strengthen their Mutual TLS (mTLS) based communication at scale across their highly distributed microservices-based architecture. When a new service was deployed, Zscaler's internal enrollment system attested the identity of the enrolling entity and triggered certificate issuance through a wrapper built on top of DigiCert APIs. That certificate then served as the credential for authenticating secure traffic over mTLS. "After it passes that first-time identity validation," Pergament explained, "you can issue an identity certificate for that client for authenticating and authorizing all its actions with the other services across the cloud."

Using Trust Lifecycle Manager, Zscaler orchestrated every stage of the certificate lifecycle—issuance, renewal, rotation, and revocation—through APIs. This API-first model enabled Zscaler to establish consistent, policy-driven workflows across an infrastructure that scaled dynamically. "Now everything is API-driven and properly audited with industry-standard governance capabilities that simplify cloud operations," Pergament said. "We have a platform and a proper, centralized inventory. This governance minimizes the risk of self-inflicting damage when it comes to certificate-related outages."

> *"We have a platform and a proper, centralized inventory. This governance minimizes the risk of self-inflicting damage when it comes to certificate-related outages."*
>
> *— Lidor Pergament, Zscaler*

> *"That niche-level expertise was absolutely critical for making this a success. We now have a partner who's an expert in this space, which can help us help our customers."*
>
> *— Lidor Pergament, Zscaler*

Laying the foundation for long-term growth and trust

When Zscaler began their PKI modernization journey, they kept it within the boundaries of ZIA, which Pergament acknowledged is Zscaler's biggest platform. But it quickly became apparent that all of the company's solutions needed to standardize on a modern PKI solution. "Again, we don't need to reinvent the wheel, and so our next step is to build a common PKI platform on top of DigiCert to serve all Zscaler product lines. And thanks to DigiCert ONE and the expertise in our partnership, we have a shareable, reusable infrastructure we can use across all product lines," Pergament said.

The strength of the partnership also stood out during implementation. "We got tremendous support from DigiCert's Professional Services team," Pergament noted. "That niche-level expertise was absolutely critical for making this a success. We now have a partner who's an expert in this space, which can help us help our customers." For Pergament, the outcome of the initiative exceeded expectations. What started as a strategic effort to modernize PKI evolved into a transformative foundation for scaling trust across Zscaler's products, deepening customer confidence and meeting the demands of increasingly regulated markets. "We're going to be 10 times better than where we were," he said.

Discover how DigiCert ONE can accelerate your PKI modernization journey.