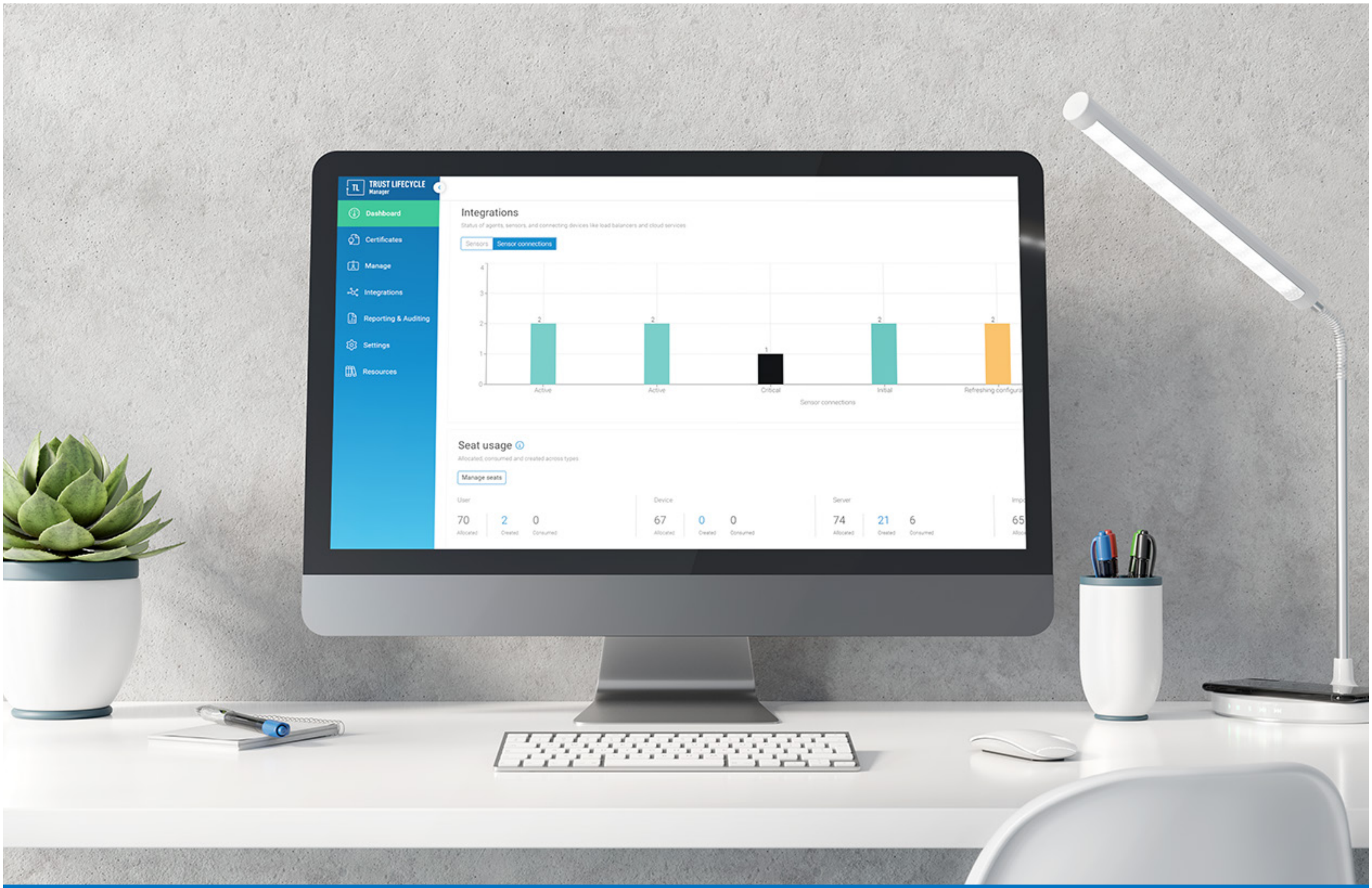


TRUST LIFECYCLE MANAGER: A TECHNICAL PAPER

The use of discovery, management and automation in the management of cryptographic assets/keys and certificates

digicert®

Introduction

Large organizations face increasing complexity in the management of their cryptographic assets. The number of active digital certificates has risen at a rapid pace, as PKI use cases expand due to zero trust adoption, IoT innovation, software supply chain security and digital innovation investments. And internal PKIs also proliferate, making it challenging to apply centralized policy or governance over these many anchors of trust.

At the same time, we are on the threshold of seismic events in cybersecurity that are introducing new pressures on operations and governance. Artificial intelligence, while it offers promising ways to accelerate business, can also accelerate cyberattacks using automation and adaptive malware. And with the National Institute of Standards and Technology (NIST) finalizing quantum-safe algorithms in 2024, organizations need to begin transitions of all of their cryptography to protect against "harvest now, decrypt later" strategies by bad actors, and to ensure that they have sufficient time to update their cryptography before quantum computers arrive on the scene. Alongside this, public trust certificate validity periods, which have dropped over the last decade from five years in 2012 to just over one year in 2020, are again under discussion, with some suggesting a maximum of 90 days.

With the convergence of these trends, it is a great time for organizations to invest in crypto agility — the centralized management of cryptographic assets using discovery, management and automation tools. This paper explores four primary use cases for DigiCert Trust Lifecycle Manager that enable companies to embark on this effort and build in this capability.

Discovery

The first step, for companies seeking to centralize management of their cryptographic assets, is to build a centralized inventory. This inventory should aggregate the certificates, protocols, algorithms, key lengths and other information into a central repository that can then be acted on. The key to success with this step is to make sure that the tools being used can find all of the essential data.

DigiCert® Trust Lifecycle Manager uses multiple mechanisms to identify these keys and certificates. These include:

Integrations with Certificate Authorities (CAs)

- Integrates with DigiCert CertCentral, for ingesting the public certificates issued by DigiCert, and with DigiCert ONE CA Manager, for ingesting the private certificates issued through DigiCert ONE. This integration tightly couples issuance and management into a frictionless experience that can't be offered by most CA-agnostic certificate lifecycle management products.
- Integrates with Microsoft Active Directory Certificate Services (AD CS), also commonly known as Microsoft CA, as well as with AWS Private CA. These certificates are synchronized with the "Central Book of Record" and can be tagged to allow for application of policy or management strategies to groups or classes of certificates. Certificates are discoverable regardless of whether they are issued directly from the issuing CA or from Trust Lifecycle Manager.
- Integrates with Let's Encrypt (planned, 1Q24). This integration enables Trust Lifecycle Manager to centralize and manage the Let's Encrypt certificates that are issued from the system. This capability is particularly useful for establishing visibility into the use of certificates in DevOps environments.

Integrations with Vulnerability Management Tools

Many large organizations have invested in vulnerability management tools that inspect networked assets — physical and virtual servers, routers and switches, cloud instances, containers and even IoT devices like multifunction printers. These organizations may wish to leverage this already deployed scanning infrastructure. Trust Lifecycle Manager has native integration with Qualys and Tenable, enabling organizations to import the certificates and assets found by these tools into Trust Lifecycle Manager's Central Book of Record.

Port-Based Scanning

Port-based scanning is the most basic way to discover certificates in an IT environment. In Trust Lifecycle Manager, organizations can specify the ports they need to scan or a range of IPs — both on premise and in the cloud — and identify assets, including active services and certificates associated with an [IPV4 address](). This scanning ensures that these certificates are secure, properly managed and comply with industry standards. It also ensures their integrity is maintained within an organization's network infrastructure.

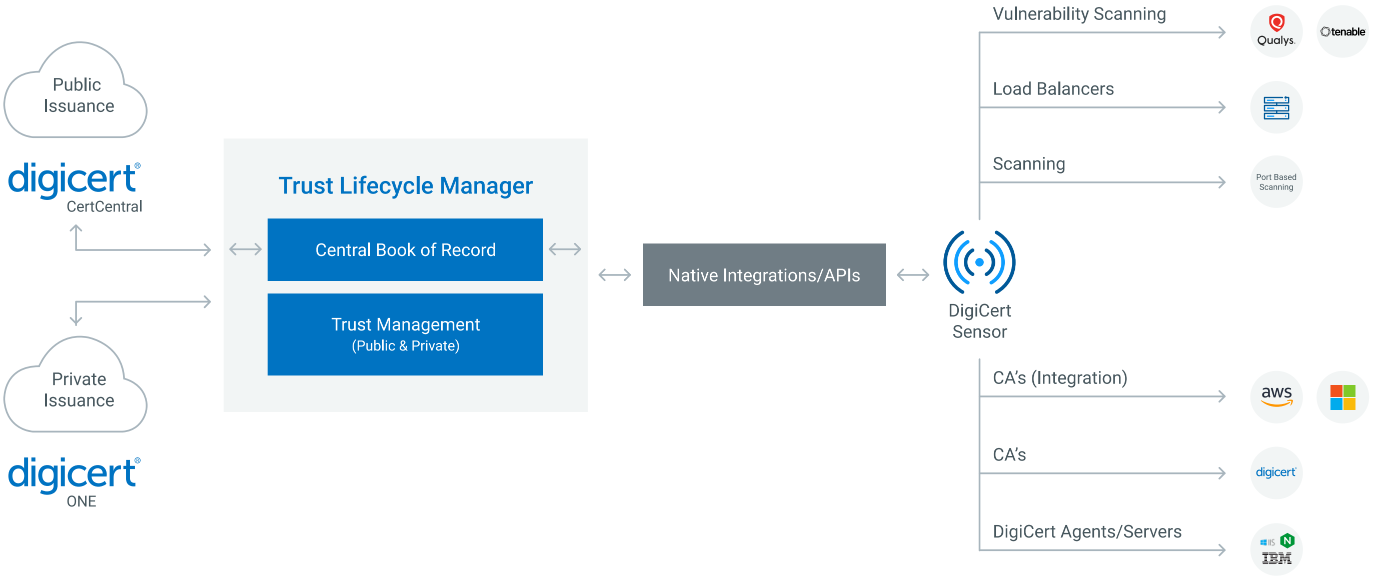
Load Balancer/Server Discovery

These methods enable Trust Lifecycle Manager to find and inventory certificates associated with load balancers (and other network appliances) as well as web servers.

Port-based scanning can identify open ports and services that are running on a load balancer. But it can't identify the TLS certificates themselves because load balancers terminate TLS connections and then route traffic to backend servers. Trust Lifecycle Manager can leverage sensors placed in the network environment to identify the certificates governed by load balancers, which ensures that these are added to the Central Book of Record.

Similarly, certificates installed on web servers such as Microsoft IIS or Apache also are not discoverable using port-based scanning. They require agents to be installed directly on these servers designed to gather the necessary information about these certificates and relay it to the Central Book of Record.

Discovery Mechanisms



Management & Automation: Servers & Infrastructure

Servers and Network Appliances

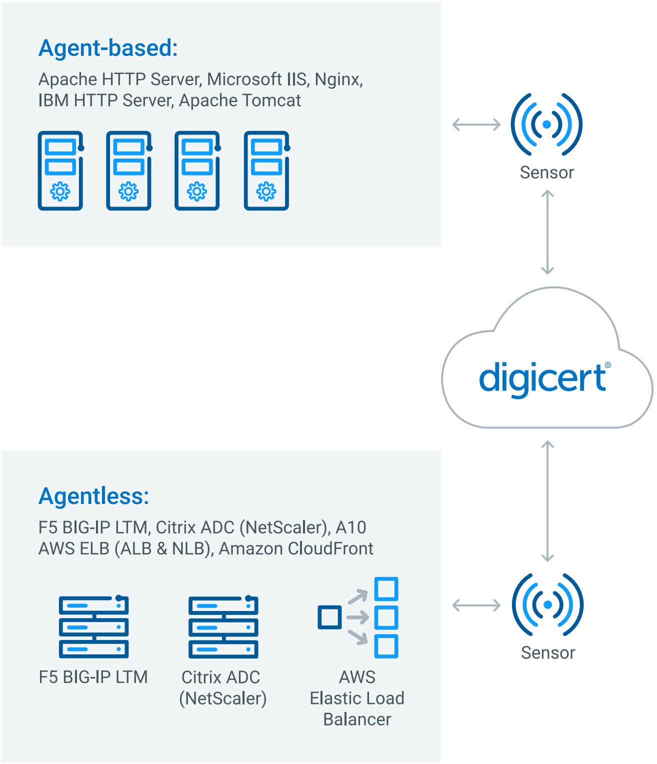
Corporate IT infrastructures depend on machines like web servers and load balancers to ensure availability of internal and external resources. In order to deliver continuous uptime and availability, organizations must ensure that the public certificates on these machines are managed throughout their lifecycles, from enrollment to renewal and revocation.

With the number of these systems numbering in the hundreds or thousands, administrators can benefit from automation to reduce the operational complexity of renewal and to mitigate the risk of an unplanned certificate expiration. Trust Lifecycle Manager provides enterprises with the architecture to automate enrollment, provisioning and renewal on load balancers and servers using sensors, similar to those used during Discovery.

Trust Lifecycle Manager integrates with web servers and load balancers across diverse targets and workflows. Trust Lifecycle Manager sensors connect with the management interface of these machines, allowing installed certificates to be provisioned or renewed via automation. Profiles in Trust Lifecycle Manager can be defined to adhere to corporate policy, directing which certificates may be auto issued, which need to be approved through an ITSM system such as ServiceNow and which can only be renewed through a manual approval process.

Further, if discovered certificates are found to contain vulnerabilities or misconfigurations, administrators can trigger workflows to revoke and replace them. This ability to manage certificates at speed and at scale improves security while freeing administrators to work on other projects that benefit the enterprise. This is particularly important as companies begin their journey transitioning to quantum-safe algorithms.

DigiCert Trust Lifecycle Manager Automation Architecture


Agent-based:
Apache HTTP Server, Microsoft IIS, Nginx,
IBM HTTP Server, Apache Tomcat
Sensor
digicert
Agentless:
F5 BIG-IP LTM, Citrix ADC (NetScaler), A10
AWS ELB (ALB & NLB), Amazon CloudFront
F5 BIG-IP LTM
Citrix ADC (NetScaler)
AWS Elastic Load Balancer
Sensor

Infrastructure

Enterprises employ distributed hybrid IT infrastructures that combine on-premises data centers with cloud instances across multiple, often globally dispersed, locations. These dynamic environments leverage containerized architectures to build and iterate apps, each of which is built on hundreds of microservices using disparate development frameworks. Every single one of these microservices require digital certificates that act as machine identities to authenticate these connections at the speed of light.

The digital certificates that are used across CI/CD pipelines are not only high in volume but also ephemeral, lasting anywhere from a few minutes to a few days.

Securing these machine identities requires automation so that the authentication processes of these thousands of ephemeral machine identities does not impede developer velocity or productivity.

The Profiles feature in Trust Lifecycle Manager enables DevSecOps teams to define reusable templates that describe the enrollment methods and certificate policies for classes of certificates. These templates can be configured for Trust Lifecycle Manager's ACME service, to enable developers to auto-enroll certificates through ACME agents like the popular cert-manager via API calls.

Management & Automation: User and Device Authentication

Trust Lifecycle Manager is differentiated from other certificate management solutions by its ability to support use cases involving user and device authentication.

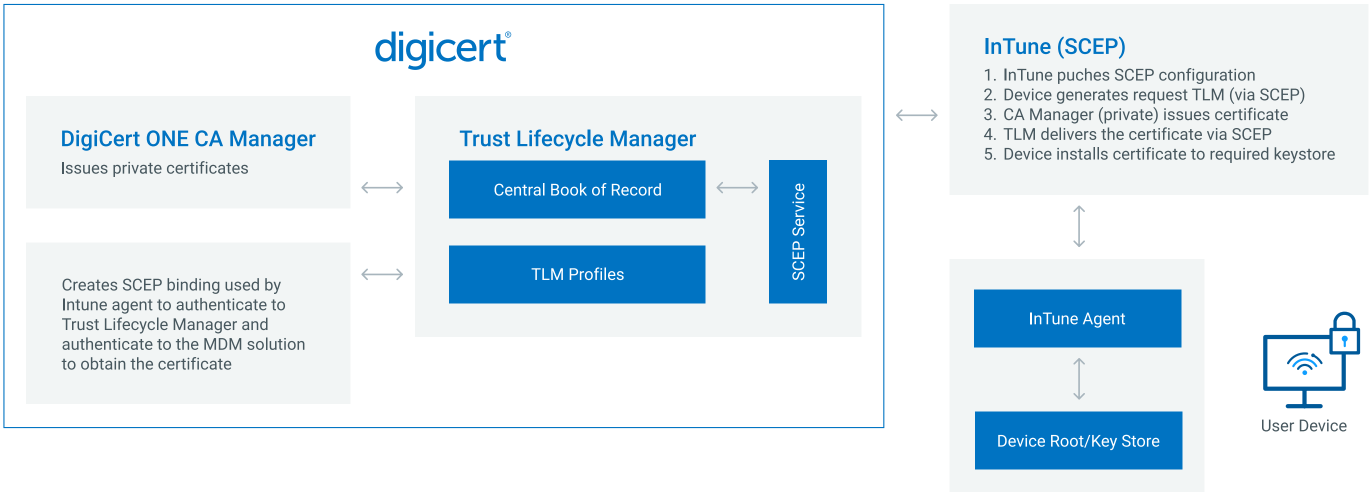
VPN/Wi-Fi Authentication

Trust Lifecycle Manager is often used for automating the authentication of users to corporate services such as VPN and Wi-Fi. Its integrations (e.g., Intune) and supporting tools (DigiCert Trust Assistant, Autoenrollment Server) enable seamless interaction with UEM/MDM systems and support automated last-mile installation of certificates to endpoints such as devices, laptops and workstations. Its Autoenrollment Server and integration to Active Directory (or other directory services) enable all certificate steps to occur automatically without end user intervention.

Due to the impact of the pandemic, the remote office is here to stay, increasing complexity around the methods and types of devices that are used to access the corporate network for IT services such as VPN and Wi-Fi. By automating certificate installation, IT teams improve user experience, reduce the support burden on IT teams, and close access gaps in the employee lifecycle, such as may occur with provisioning during onboarding, privileges changes in role changes and deprovisioning with termination.

> IBM, which has more than 300,000 employees, uses DigiCert to provide this magical combination of secure authentication and seamless access. Weibo "Weber" Yuan, chief architect and strategy lead at IBM, said that it helped them turn "public key infrastructure to public key invisible."

Auto Enrollment Server and InTune Integration



digicert

DigiCert ONE CA Manager
Issues private certificates

Creates SCEP binding used by Intune agent to authenticate to Trust Lifecycle Manager and authenticate to the MDM solution to obtain the certificate

Trust Lifecycle Manager

Central Book of Record

TLM Profiles

SCEP Service

InTune (SCEP)

1. InTune puches SCEP configuration
2. Device generates request TLM (via SCEP)
3. CA Manager (private) issues certificate
4. TLM delivers the certificate via SCEP
5. Device installs certificate to required keystore

InTune Agent

Device Root/Key Store

User Device

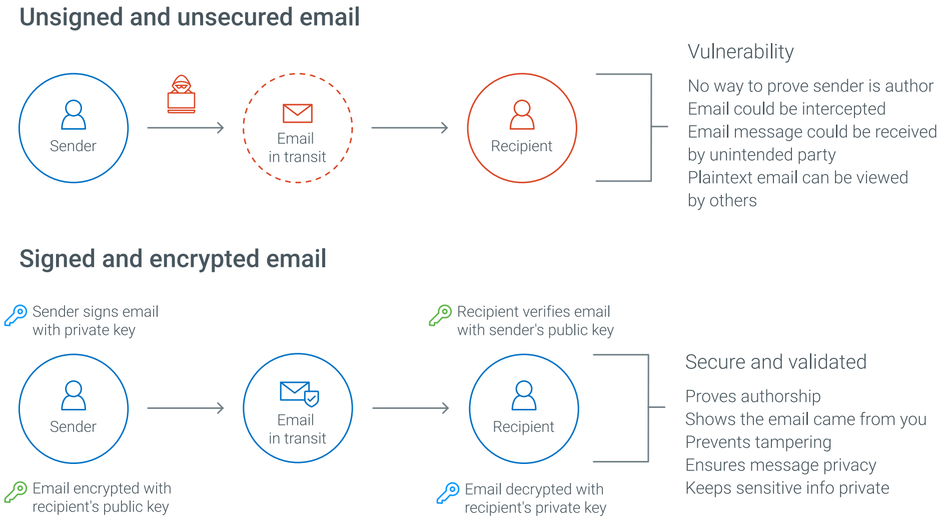
Secure Email

Trust Lifecycle Manager can also be used to manage the provisioning of S/MIME certificates for securing email. By securing email with a DigiCert S/MIME certificate, organizations can easily encrypt and digitally sign every message to protect against phishing, spoofing and man-in-the-middle attacks. But managing S/MIME certificates, like TLS certificates, can be difficult without a solution tailor-made to handle them. Trust Lifecycle Manager provides that ability to deploy S/MIME certificates at scale to authenticate senders and encrypt and decrypt email messages. This is something most legacy CLM providers don't offer.

At-scale secure email through Trust Lifecycle Manager provides organizations with:

- Central administration: manage and deploy all certificates from a single console
- Centralized recovery: cloud-based, two-part recovery or on-premises key escrow
- Rapid deployment: leveraging expert-designed certificate profiles
- Flexible enrollment: PKI client, self-support portal, OS/browser enrollment or MDM
- Seamless provisioning: automation with Active Directory authentication

How Email Certificates Work



Unsigned and unsecured email

Sender
Email in transit
Recipient

Vulnerability

No way to prove sender is author
Email could be intercepted
Email message could be received by unintended party
Plaintext email can be viewed by others

Signed and encrypted email

Sender signs email with private key
Recipient verifies email with sender's public key
Sender
Email in transit
Recipient
Email encrypted with recipient's public key
Email decrypted with recipient's private key

Secure and validated

Proves authorship
Shows the email came from you
Prevents tampering
Ensures message privacy
Keeps sensitive info private

PKI Modernization and Private Trust

When embarking on the path of crypto agility, many organizations also take the opportunity to modernize their trust architectures. Trust Lifecycle Manager includes the ability to stand up private CAs within the organization, managed with the same rigor or Certificate Policy Statement and practices applied to public Web Trust environments. Organizations that lack the necessary PKI expertise for complex PKI environments or that need to migrate a PKI off of unsupported servers may benefit from working with DigiCert to modernize their underlying infrastructure. Our PKI services team uses our proprietary automation tooling for signing ceremonies and key generation activities, developed over more than two decades of experience.

DigiCert conducts more than 3,000 key signings every year and operates seven global key ceremony facilities around the world, important to customers who require local key residency. Our teams are recognized as establishing the foundational principles behind key ceremony processes, which have been adopted by organizations such as ICANN and Verisign. In addition, DigiCert has developed proprietary automation tooling for signing ceremonies and key generation activities, developed over more than two decades of experience. This tooling delivers fast time to value and reduces human error when standing up private roots.

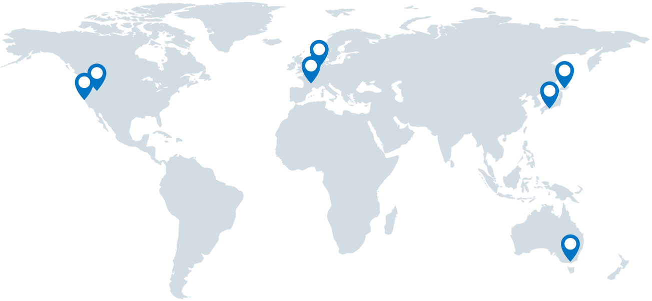
3,100+
key signings per year

2,600+
active public and private roots

5,700+
active public and private ICAs

7
golbal key ceremony facilities

Key ceremony facilities



Conclusion

Companies need to invest now in preparing their trust infrastructure for the coming impact of artificial intelligence and quantum cryptography transitions. By investing in crypto agility with DigiCert Trust Lifecycle Manager, companies can achieve these goals alongside the myriad benefits of centralizing, managing and automating their digital trust operations.

Get started today with DigiCert® Trust Lifecycle Manager, by contacting sales@digicert.com.