# DIGICERT® ONE

All servers. All signings. All users. All devices. All managed in one platform.

DigiCert ONE is the modern, holistic approach to PKI management. Built on an advanced, container-based design, DigiCert ONE allows you to rapidly deploy PKI services or identity verification in any environment. Roll out new services in a fraction of the time with end-to-end user and device management at any scale. It's PKI reimagined.

07
Pending

88
Available seats of
200
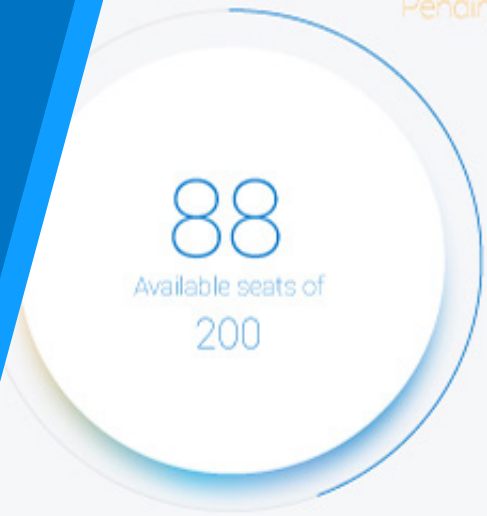
Add new seat   Add more seats

digicert®

digicert®

The entire PKI family under one roof

For nearly three decades, PKI technology has been the proven building block of public trust for the Internet. PKI is also proven in private trust for users, access, endpoints, devices, documents and code. PKI has even bridged the public/private gap with IoT devices. But while time-tested, PKI was frequently deployment-challenged and often managed in disparate silos without standards, governance or visibility across the organization. DigiCert ONE is a new approach to PKI—one built with the flexibility and power to manage any deployment or workflow.

- DigiCert® Trust Lifecycle Manager
- DigiCert® IoT Trust Manager
- DigiCert® Software Trust Manager

The fast and flexible solution

DigiCert ONE is the platform that meets you where you are. With configuration options for DigiCert-hosted cloud, on-premises, hybrid, air-gapped and more, DigiCert ONE is flexible enough to fit any need. And thanks to modern, container-based architecture, not only is DigiCert ONE highly scalable, it's also extremely quick to set up. Stand-up times clock at minutes or hours instead of weeks, regardless of the size or configuration of your current environment. This lightning-fast deployment ensures you're issuing—as many as tens of thousands nearly simultaneously—and managing certificates without the complications and cost of consultants and standard integration processes.
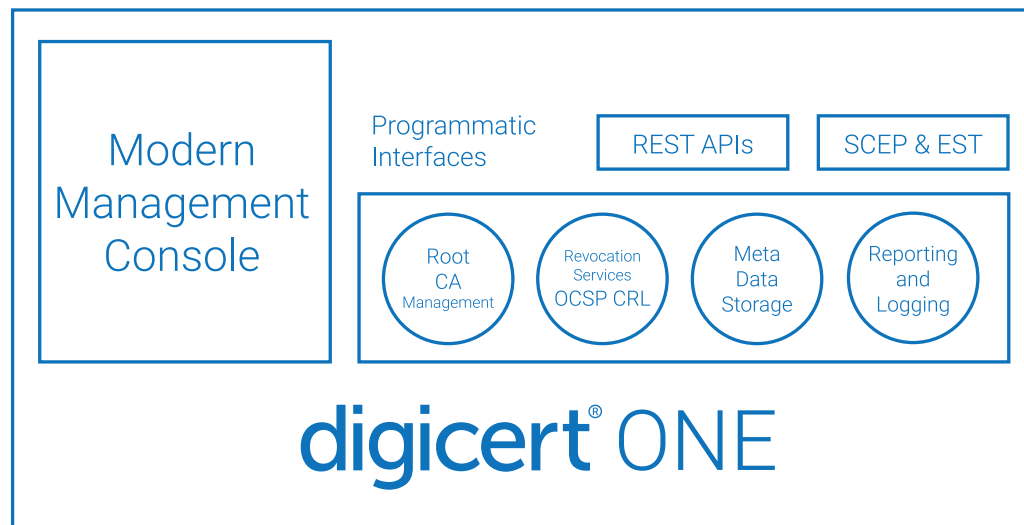
digicert®

DigiCert® Trust Lifecycle Manager

Manage your workflows in one place

With Trust Lifecycle Manager, you can securely designate and delegate issuing and management privileges, monitor system activities and resource consumption, and manage every certificate in your enterprise.

Because it's built on the DigiCert ONE platform, you can issue exceptionally high volumes of certificates in moments, while taking advantage of dynamic, nearly instantaneous CA creation.

Automatic orchestration and continuous updates ensure your data and systems remain secure while staying compliant with the latest PKI industry standards and audit requirements.

Trust Lifecycle Manager workflows

Secure Email

Wi-Fi Device Authentication

Secure Remote Access with VPN

Unified Endpoint Management/MDM

Server Authentication

SSL Inspection

Smart Card Login

Web Authentication

Network Access Control

Other Use Cases

Trust Lifecycle Manager allows IT teams to:

- Build identity verification systems for e-government and in-country programs
- Adapt to fit your needs, with flexible deployment models supporting customer configurations in private or public cloud, air-gapped environments, or completely managed by DigiCert
- Integrate with third-party applications for your business process needs
- Manage out-of-the-box or create custom private CA hierarchies
- Customize certificate profiles and tailor deployments to your infrastructure and needs
- Serve extremely high volumes of certificates quickly using robust and highly scalable infrastructure
- Deploy automated secure access to large user populations with little to no end-user interaction
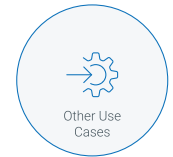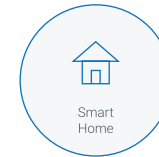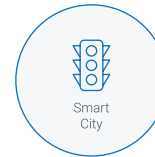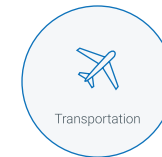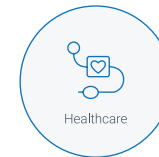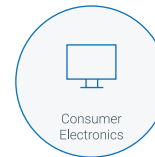
DigiCert® IoT Trust Manager

Full lifecycle management for IoT

Billions of connected devices. Each unique in its manufacture and use. You need a security solution that allows you to control your devices no matter where they are in the lifecycle.

IoT Trust Manager makes it easy to identify, secure and manage any device at any point. From silicon injection to deployment in the field, IoT Trust Manager allows you to insert and monitor digital certificate security at any stage. And for manufacturers, security can be incorporated into your devices without any need for changes to your manufacturing process.

IoT Trust Manager Use Cases

Consumer Electronics

Healthcare

Transportation

Industrial Controls

Smart City

Smart Home

Supply Chain

Other Use Cases

Benefits

- Deploy in a fraction of the time it takes to get other platforms up and running
- Configure to fit your needs with options for on-premises, cloud or hybrid
- Automatic updates and orchestration
- Avoid third-party license fees
- Manage easily and at scale with container-based architecture
- Get access to award-winning support, available 24 hours a day, 365 days a year

Features

- Issue, manage, revoke and renew certificates from one platform
- User provisioning workflows
- Device provisioning workflows
- IoT provisioning workflows
- Custom certificate profiles
- Customizable enrollment
- Customizable authentication

digicert®

DigiCert® Software Trust Manager

## Secured and validated with compliance

Just like email and web, code, apps and containers are vulnerable to in-transit tampering.

With DigiCert Software Trust Manager, you can ensure code signing key protection while delegating cryptographic operations, signing activities and management of the service to your developer teams in a controlled and auditable way.

This solution not only protects the integrity of the code and your end-users, it also speeds your time to market by embedding trust that prevents operating systems and browsers from flagging your code as suspicious. DigiCert Software Trust Manager adds speed and efficiency

to your security. All this, plus compliance, means management of your code integrity is now complete and simple.

Software Trust Manager Use Cases

App Signing

Device Integrity

CI/CD Workflows
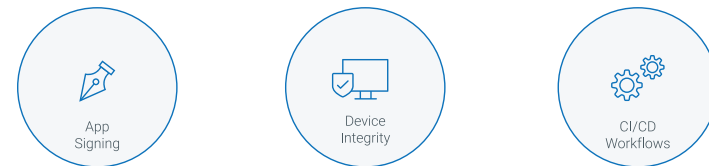
Benefits

Signing Visibility
- Secure your keys with industry-leading encryption and identity
- View and control who can sign applications
- Control who accesses keys and guard against unauthorized key sharing

Agility with control
- Sign faster, with more control, thanks to the use of hashing
- Integrate client tools with your CI/CD tools for automated codesigning
- Quickly remediate if a certificate needs to be revoked

Signing security
- Preserve the life and integrity of your applications
- Ensure adherence to compliance standards
- Enjoy support for RSA with a range of key sizes and curves with ECDSA

Features

- Secure private keys on the cloud for cryptography functions requiring a digital signature
- Generate and manage certificates using public and private hierarchies
- Make use of implementation and support for cryptographic library standards, including PKCS#11 and Microsoft CNG/KSP
- Deploy various types of code signing for binaries, including OpenSSL, Java, Authenticode, Android, GPG, RPM and Debian
- Manage keys and certificates from command line client
- View and manage keys and certificates through a browser user interface
- Report on activities and deploy client-side tools
- Customize and configure with REST APIs

The trusted leader in PKI

The better way can't become common practice until someone finds it.

At DigiCert, building a better way to secure the internet is the single-minded pursuit that goes all the way back to our roots. That's why our TLS/SSL certificates are trusted everywhere, millions of times every day by 89% of the Fortune 500, 97 of the 100 top global banks, and for 81% of global e-commerce. It's why our customers consistently award us the most five-star service and support reviews in the industry. It's why we're modernizing PKI by building the DigiCert ONE platform and management tools to help enterprises and governments secure identities, access, servers, networks, email, code, signatures, documents and IoT devices. In SSL, IoT, PKI and beyond—DigiCert is the uncommon denominator.

See how DigiCert ONE can help simplify and strengthen your security. For more information go to www.digicert.com or contact pki_info@digicert.com.

digicert®