IoT Security Made Easy

DigiCert simplifies the process of provisioning and deploying the critical and often complex security solutions needed to secure the Internet of Things.

DigiCert IoT Capabilities

DigiCert works with all industries to issue certificates using multiple signature algorithms, public key types, and cryptographic properties to meet specific needs. DigiCert adopts cryptographic technology as needed and works with key contacts within organizations to ensure they can reap the full benefits of the vast PKI experience DigiCert has to offer.

CERTIFICATE MANAGEMENT SERVICES

DigiCert certificate management services are designed to help manage hundreds, thousands, or even millions of IoT device certificates. The DigiCert PKI service is customizable to fit the needs of all certificate deployment approaches, making it one of the most flexible IoT security deployment solutions.

SCALABILITY

The DigiCert PKI management platform can scale to accommodate changes for thousands to millions of certificates. The infrastructure and servers needed to handle mass issuance, reissuance, and/or revocation are a large investment but are critical to ensure continuous integrity of PKI systems.

DEVICE IDENTITY

The DigiCert authentication solution does not require tokens or passwords. Certificates are installed (embedded) on connected devices and used to securely identify and authenticate one device to another, ensuring that only trusted devices are allowed to connect to a nearby server, and enabling trusted communications between devices to take place.

PROVISIONING AND CERTIFICATE DEPLOYMENT

There is no IoT deployment too large or small to fit the DigiCert solution. Certificate requests can be automated through our REST API, SCEP, EST, or using DigiCert CertCentral® to streamline certificate management.

The Leading Provider of IoT Encryption and Authentication

DigiCert specializes in IoT security solutions, delivering the critical trust that is needed in IoT device management, system and device authentication, encrypted data communications, and secure software.

As a pure security player, DigiCert focuses on creating simplified approaches to integrating highly scalable, available, and customizable security into IoT management platforms.

HOSTED AND ON-PREM SOLUTIONS

Hosted CA Infrastructure: The PKI framework is hosted and managed by a publicly trusted CA. On-Premise CA Infrastructure: The entire PKI framework is hosted and managed by the IoT provider.

Hosted HSM: Key management is hosted and managed by a publicly trusted CA. On-Premise HSM: Key Management is hosted and managed by the IoT provider/organization.

digicert®

PUBLIC/PRIVATE TRUSTED MODELS

While private PKI may seem like an ideal use-case, an internal CA cannot be trusted automatically by external services or relying devices. Using publicly trusted certificates is not only valuable but also crucial to IoT deployments.

SECURITY DESIGN AND CONSULTING

As a global certificate authority, DigiCert's main IoT objectives are to provide digital certificates, provide access to partners who provide other IoT services, and consult with organizations about IoT security.

DigiCert security experts can assist in readiness assessment, design and deployment, architecture and PKI security review, and IoT security solution implementation.

HIGH AVAILABILITY

DigiCert boasts 99.99% server uptime and has the systems in place to accommodate global issuance. High availability is important when dealing with global certificate provisioning, verification, and revocation. Deploying an infrastructure specifically for these needs is not logistically nor economically feasible for many organizations.communications between devices to take place.

For more information, contact an IoT expert by phone at 1.855.800.3444 or email iot@digicert.com.

digicert®