DigiCert Partner Solution Brief

Business Needs

In an exponentially connected world, Internet of Things (IoT) providers need a scalable security solution for devices—regardless of computing power—that addresses encryption, authentication, and data integrity.

Business Challenges

When organizations are developing large-scale IoT environments, finding a robust yet simple solution for deploying, delivering, and managing device identity can be challenging. Public key infrastructure (PKI) presents a proven, scalable model for trusted identity. Maintaining certificate security, staying on top of management, and establishing the right processes are all aspects that need to be considered, especially when many IoT projects affect millions of devices and users.

Technical Challenges

- Developing policy-driven processes for billions of devices
- Managing and provisioning bulk certificates before product rollout
- Automating the renewal, rotation, and revocation of certificates in a time-efficient manner
- A need for an issuance platform for high-volume certificate deployments
- Device certificate provisioning for low-computing devices

Partner Solution

Device Authority and DigiCert partnered to expand the range of IoT devices that can be secured and to provide enhanced device provisioning and credential management for the IoT.

ENCRYPTION

Our solution provides certificate provisioning and management through policy-driven device registration and authentication controls. Digital certificates are used to encrypt communications between devices and servers. Certificates can be generated, signed, encrypted, and delivered to devices as part of their initial registration process with management servers. Organizations may also choose

DEVICE AUTHORITY
IoT Security Simplified

deviceauthority.com

Industry: Internet of Things

Region: Global

Partner Profile: Device Authority provides simple, innovative solutions to address the challenges of securing the Internet of Things (IoT). DA helps its customers simplify the process of establishing a robust, end-to-end IoT security architecture, including device provisioning, credential management, and secure updates.

digicert®

to have certificates pre-generated and signed ahead of device rollout to help expedite bulk device deployments.

AUTHENTICATION

A patented device-derived key generation process was designed so device certificates are cryptographically bound to the device identity in a way that ensures only an authenticated and authorized device may utilize a given certificate. Binding the certificate to the device identity prevents certificates from being stolen and helps prevent device cloning.

CREDENTIAL MANAGEMENT

Our PKI management platform can support billions of devices through a services-oriented, horizontally-scalable, high-availability architecture, and it leverages on-demand certificate management options.

It further streamlines certificate management through certificate rotation policies that initiate and control the renewal and rotation of device certificates. Revocation policies keep certificate validity in line with device authorization status, and the system can automatically revoke associated certificates in the event a device becomes unauthorized.

The integrated DigiCert and Device Authority solution is addressing the need to secure the IoT—from the largest deployments to smallest devices—with encryption, authentication, and credential management.

Device Authority and DigiCert partnered to expand the range of IoT devices that can be secured and to provide enhanced device provisioning and credential management for the IoT.

digicert®