Hosted vs. On-Premise CA for IoT Implementations

DigiCert Managed IoT PKI vs. Internally Managed Software

Deploying, managing, and maintaining an enterprise-level PKI security solution can be a complicated task. Organizations who seek to implement and maintain an on-premise or in-house PKI security solution face hidden costs and other complications.

As a publicly trusted Certificate Authority, DigiCert already understands the complexities associated with managing a PKI solution. Our years of experience as a leading CA allow us to provide a Managed PKI solution for IoT that is not only cost-effective, but also simplifies the implementation process while delivering dependable and trusted authentication, encryption, and integrity vital for connected devices.

PKI is more than implementing an on-premise PKI software. Managing a PKI requires adherence to PKI standards, developing storage, data backup, and certificate management policies, training personnel, and creating a data center with backup system.

Acquiring the necessary hardware, training, and resources needed to implement, run, and maintain an on-premise PKI solution bring substantial costs beyond the initial software acquisition in order to ensure device integrity throughout the lifecycle.

Hidden Costs of Internally Managed PKI Systems:

- Software acquisition and maintenance
- Hardware and networking infrastructure
- Secure facilities
- Creation and auditing of policies and procedures
- End-user support
- Management of the certificate lifecycle
- IT training
- Backup and disaster recovery
- Certificate Revocation List (CRL) and Certificate Status Protocol (OCSP) infrastructure
- Scalability to support user and application growth
- Highly available validation

Comparing On-Prem vs. Hosted PKI Implementations

HYBRID (ON-PREM RA INTEGRATED WITH PKI SAAS)

Pros

- Improved disaster recovery
- Increased reliability
- Increased global accessibility
- Off-loading PKI expertise
- Cost Efficient
- Resilient
- Scalable
- Automatic and continuous updates
- Limited to no hardware expense
- Additional features with less Dev time
- Security audits and process control
- Public trust for subCAs
- Highest level of security controls over Root CAs
- 24/7 Support
- Unified portal for managing Private/Public PKI

Cons

- Delegation of some aspects of data security and access controls
- Root CA not physically accessible
- No access to directly change functionality
- Dev time to integrate with API
- Most UX requires internet connectivity and causes downtime
- Vendor lock-in

ON-PREM CA AND RA

Pros

- Full control of issuance process
- No internet dependency
- Configuration/Dev changes done on your schedule

Cons

- Divided portal for managing Public vs. Private SSL
- No availability of public trust without costly, repeated audits
- Maintenance and acquisition of software
- Creation of CSP and related procedures
- End user support of certificate users
- Deployment of globally available CRLs and distributed OCSP responses
- Expertise in PKI and constant awareness of industry standards, changes in servers, browsers, libraries, forums, and working groups
- Staffing costs to securely manage CA
- Hardware costs for HSMs
- Hardware costs for issuing/management servers
- Inefficencies in CA and related services

Why Choose a Hosted IoT PKI Solution

PUBLIC TRUST

An internal CA will never be able to be used in a way that is trusted automatically by external services or relying parties. While private PKI may be a primary use case, having the flexibility to also issue publicly trusted certificates is valuable.

PKI EXPERTISE

Understanding PKI is complex and typically isn't an IoT provider's full-time job. As a CA, DigiCert understands FIPS 140-2 level 2, ECDHE cipher suites, PKCS #11 cryptographic interfaces, root ubiquity compliance, and X.509 OIDs.

SCALABILITY

Certificates are used to secure sensitive and valuable information. Investing in servers and infrastructure to handle mass issuance, reissuance, and/or revocation events is necessary to ensure integrity of the PKI systems. Those events are rare, but the costs associated with these investments are high, especially when dealing with thousands or millions of certificates.

HIGH AVAILABILITY

All core DigiCert services offer exceptional uptime and availability. When dealing with globally disparate certificate provisioning, verification, and revocation, deploying a brand new infrastructure to support the many needs of such systems is not logistically feasible for most organizations, and is almost never economically feasible when compared to using systems already in place.

SECURITY

The security requirements of running a CA are substantial. Your Root CA needs to be secured to the absolute highest level, which requires investment in hardware, CA software, infrastructure, PKI architects, consulting services, and training.

PRICING

DigiCert offers competitive pricing that scales with certificate issuance. This way your investment starts at a financially viable point and gets more cost effective as certificate issuance increases.

CRYPTOGRAPHIC AGILITY

Cryptography is constantly changing. Certificates require quick turnaround when standards shift or cryptographic properties change. As a publicly trusted CA, DigiCert can anticipate these changes to curves, algorithms, and hashes years before they become mainstream. When vulnerabilities are found or deprecation occurs, we can immediately switch to a secure alternative.

LIABILITY

If an internal CA is compromised and enables access to privileged data, the damage to a company's reputation is often detrimental, not to mention the resulting monetary loss can be significant. Separating management of some parts of an organization's security solution can not only increase the overall security of that solution, but also help to minimize damages in worst-case scenarios.

To learn more about the DigiCert IoT solution, call 1.855.800.3444 or email iot@digicert.com

© 2017 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.