

4 Trends every security leader should be watching

Public certificate lifespans are shortening

As Web PKI certificate lifetimes shrink, organizations are investing in automation.



Post-quantum cryptography is becoming a business priority

Crypto-agility and modern PKI architectures are essential for long-term resilience.



AI is increasing demand for trusted machine identities

PKI provides cryptographically-based identity for AI governance at enterprise scale.



New regulations are raising the bar for governance and compliance

Organizations are under increasing pressure to demonstrate audit readiness.



What does Modern Internal PKI look like?

A modern internal PKI is more than a collection of certificate authorities. It provides the centralized governance, automation, and flexibility needed to secure identities across the enterprise while reducing operational complexity. The capabilities below represent the core building blocks of a modern PKI strategy that meets enterprise-ready internal PKI needs.



Deployment and integration

Centralize certificate governance across the enterprise

Deploy flexibly with cloud-ready support while supporting hybrid environments



Certificate issuance

Support users, devices, workloads, and applications from a common trust platform

Automate certificate lifecycle management with support for modern standards like ACME



Security and compliance

Enable crypto-agility for future algorithms

Strengthen auditability with role-based administration and policy controls

A practical framework for modernizing Internal PKI

Modernizing your internal PKI doesn't have to be an all-or-nothing project. Organizations that successfully modernize typically follow a phased approach that minimizes risk while building a more scalable, secure PKI foundation.

Before you can modernize your PKI, you need to know what you have.

Discovery capabilities, like those in DigiCert Trust Lifecycle Manager, can perform cloud, network, and system scans to identify certificates and other digital trust assets across your organization, helping you build a comprehensive cryptographic inventory.



Step 1: Assess your current PKI

Build a complete inventory of your PKI environment before making any changes.

- Inventory certificate authorities
- Discover certificates across users, devices, workloads, and applications
- Identify certificate dependencies and trust relationships



Step 2: Design your future PKI

Define the architecture and governance model that will support your organization's future needs.

- Simplify your CA hierarchy to build for crypto-agility and future growth
- Centralize governance and policy
- Determine cloud, hybrid, or on-premises deployment requirements



Step 3: Validate with a pilot

Start small to reduce risk and validate your approach.

- Select a low-risk use case
- Test integrations and automation
- Validate certificate policies and workflows



Step 4: Migrate in phases

Move certificates incrementally while maintaining business continuity.

- Run legacy and new PKI environments in parallel
- Minimize user and operational disruption
- Retire legacy CAs as dependencies are removed



Step 5: Optimize and scale

Once migration is complete, focus on improving efficiency and governance.

- Expand certificate lifecycle automation
- Increase visibility across your PKI estate
- Strengthen governance and role-based administration
- Prepare for future cryptographic requirements



Why organizations choose DigiCert

Modernizing internal PKI requires more than replacing legacy infrastructure. It requires a trusted partner with the expertise, proven operations, and scalable platform to help you reduce operational complexity while preparing for the future.

For more than 25 years, DigiCert has helped the world's largest enterprises build and operate trusted PKI at a global scale. DigiCert Private CA provides a cloud-ready foundation for modern internal PKI with centralized governance, flexible deployment options, automated certificate lifecycle management, and enterprise-grade security and compliance.

8B+

Proven scalability

Customers rely on DigiCert Private CA for over 8 billion certificates worldwide

20x

Faster issuance

Experience certificate issuance up to 20 times faster, improving user experiences and increasing scale

5700+

Global presence

DigiCert operates over 5700 Intermediate Certificate Authorities across 7 global facilities

Ready to modernize your internal PKI?

Whether you're evaluating solutions outside Microsoft CA or planning your next-generation PKI architecture, DigiCert can help you assess your current environment and develop a modernization strategy that aligns with your business and security goals.

Learn more about [DigiCert Private CA](#) to explore in-depth capabilities and technical specifications or [talk to an expert](#) if you'd like to discuss your internal PKI modernization strategy today.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com