



Practical Lessons for PKI Modernization



When DigiCert began our own PKI modernization journey, we assumed that we knew our certificate environment well enough. Then discovery told a different story. What we thought was a PKI infrastructure of 6,000 certificates turned out to be more than 18,000. In this executive brief, we share the practical lessons of how to structure PKI modernization, assign accountability, and build visibility and control across distributed teams and systems.

Customer Zero is DigiCert's in-house PKI modernization program. We have done the work in a real production environment, with real constraints: segmented systems, distributed ownership, exception paths, automation gaps, and teams that still need to move fast. We have also realized real benefits and improvements: centralized governance, fewer outages, and reduced administrative costs.

Centralize Governance. Distribute Execution.

PKI is too distributed to centralize everything. It lives in cloud platforms, third-party SaaS, legacy systems, appliances, software pipelines, managed services, and secure network enclaves.

Our central team maintains the inventory of all existing certificates, where they are used, who owns them, and when they renew. This team is responsible for applying policies and responding to deviations and exceptions. The policies are set with input from the teams that operate the systems. The central team helps with compliance, overall and it monitors for gaps in automation or ownership that need leadership attention. The central team also acts as in-house consultants, advising internal teams and vendors on best practices.

The business and system owners help deploy and manage the technologies needed to discover certificates and automate lifecycles. They are responsible for adding metadata to their certificate inventory, along with the day-to-day operations of PKI inside the environments they control and vendors they use.

This approach makes PKI visible, governed, and accountable without slowing down the teams that rely on it.

Lessons Learned



Inventory is only useful when it creates accountability

Discovery should produce owners, service context, renewal paths, and business priorities, not just a longer list of certificates. The central team should remove friction. Its job is to set policy, maintain the system of record, monitor progress, and help teams move faster. It should not become a bottleneck for every certificate.



Automation needs tiers

Some systems natively support industry standard automation interfaces. Others need integrations, vendor engagement, or a replacement plan. Because of the move to 47-day certificates, most vendors support, or will soon support, automation.



Metadata quality matters

Bad ownership, duplicate records, and missing tags create noise. Treat certificate inventory hygiene like configuration management database (CMDB) hygiene.



Automation still needs monitoring

API connectors, protocol servers, and automation agents are operational dependencies. If they fail quietly, teams can mistake silence for assurance.

Outcomes of Customer Zero

3x

more certificates
discovered than expected

1500+

hours per year of manual
work eliminated

<6 months

reduction in certificate-
related outages

PKI modernization is achievable when the operating model reflects the way the enterprise runs: central governance, distributed execution, and clear roles and responsibilities. Start with one important business application environment, prove the model there, then expand the pattern.

Ready to start your PKI modernization journey?
Get the playbook

digicert® ONE

DigiCert ONE unifies certificate lifecycle management, PKI, and DNS under a single governance and automation layer. It empowers organizations to replace fragmented tools and siloed PKI environments with one scalable platform.

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.

© 2026 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.