digicert®

# PKI Modernization Playbook for Decision-Makers

## PKI under pressure

Digital certificates are the mechanism by which every system, service, and identity in your organization proves it is what it claims to be. They secure web traffic, authenticate users and devices, protect internal APIs, and authorize AI agents to act on behalf of your organization. The infrastructure that manages them has not kept pace with how much depends on it.

Three forces are converging to make this a leadership-level problem.

### Certificate lifespans are shrinking

Industry standards are reducing the maximum validity of public TLS certificates from 398 days to 47 days. In practice, this means an organization managing 1,000 public certificates will do at least 8,000 renewal-and-deployment cycles per year. At a 99% success rate, that still means 80 failures annually. Manual or haphazard processes cannot absorb this.

### Machine identities have overtaken human identities

Servers, containers, APIs, and IoT devices each require a certificate. In most enterprises, machine identities already outnumber human identities by orders of magnitude. Without full inventory, consistent governance, and systemic management, the “debt” grows with each new service your organization deploys.

### AI adoption is creating a new identity surface

AI agents need cryptographic identity for the same reason your servers do: so that the systems they interact with can verify who they are and what they are authorized to do. Organizations moving quickly to deploy AI without a governed identity infrastructure are extending trust to systems they cannot verify, audit, or revoke. The attack surface is real and growing.

These are not separate problems. They share a root cause: most organizations lack a complete, governed, and automated approach to PKI management. The three pillars that follow are the framework for building one.

# Pillar 1: Inventory

## You cannot govern what you cannot see.

The goal is a complete, continuously maintained inventory of every certificate in your environment. Having an inventory means you know who issued it, where it is deployed, and who is accountable for it. Most organizations discover through this process that they have significantly more certificates than they thought, issued through more channels than they knew, with ownership gaps that make automated renewal or incident response impossible to reliably execute.

Start with important business systems. Then expand and iterate.

## Leadership Goals

### No unknown certificates

Every certificate in your environment is mapped to a service, an owner, and a deployment location. This is the prerequisite for automation.

### Mis-issuance detection

Any certificate issued for your domains — by any CA, through any channel — is detected and reconciled within a defined window. Certificate Transparency logs make unauthorized issuance visible in near real time. If you are not monitoring them, you are not monitoring your perimeter.

### Cryptographic hygiene

You know what percentage of your certificates do not meet your cryptographic standards. Weak key sizes and deprecated algorithms are proactively tracked and prioritized rather than appearing as audit findings.

## Metrics for your dashboard

| Metric | Direction | What it signals |
|---|---|---|
| Certificates with unknown owner | Down toward zero | Accountability gaps are closing |
| Critical services covered by 2+ discovery methods | Up toward 100% | Inventory confidence |
| Certificates missing mandatory tags | Down toward zero | Governance discipline |
| Mis-issuance reconciled within SLA | Up toward 100% | Detection & response |
| % of inventory failing crypto policy | Down | Hygiene progress |

The right owner for this program is the PKI or identity team, with application and service owners accountable for confirming ownership of certificates within their domains. Without cross-functional accountability, inventory efforts produce data without governance.

# Pillar 2: Policy

## CA hierarchy decisions are long-lived. Most organizations have never made them deliberately.

Every certificate derives its trust from a chain that terminates at a root certificate authority. How that chain is designed — how many roots, how use cases are separated, where keys are stored, what cryptographic standards apply — shapes your security posture and your operational complexity for years. The most common CA hierarchy problems in enterprise environments are not cryptographic failures. They are architectural and operational ones: roots overloaded across too many use cases, intermediates that cannot be revoked without widespread disruption, key material managed without adequate controls, and hierarchies that were never formally documented.

## Leadership decisions:

### 1 Design your hierarchy deliberately

Before any CA infrastructure is provisioned, document the answers to four questions:

- How many roots do you need and why?
- How will you separate use cases (e.g., TLS, user identity, code signing, machine identity) structurally versus through policy controls?
- Where will CA keys be stored, and who controls them?
- What is your cryptographic baseline, and who is accountable for maintaining it?

These decisions do not require a CIO to configure an HSM. They require a CIO to ensure the decisions have been made explicitly, signed off, and documented. The cost of redesigning a CA hierarchy after certificates have been issued is significant.

### 2 Build a CA rationalization roadmap

Most enterprises have accumulated multiple CAs across their environment: one for the enterprise domain, another for workloads in one cloud, yet another for workloads in a different cloud, and perhaps others inherited through acquisitions. Each represents a separate skills investment, a separate governance model, and a separate visibility gap. The certificates issued by each CA are often not visible in a unified inventory, which means they are not consistently governed.

The strategic objective is not to eliminate every CA immediately. It is to bring all existing issuance infrastructure under a common management and governance layer as a first step, then rationalize the CAs over time toward a standardized set. This reduces operational complexity, eliminates skills fragmentation, and produces a PKI that can actually be governed uniformly, regardless of which underlying CA issued each certificate. An organization running three cloud platforms does not need three separate PKI programs. It needs one governance model applied consistently across all three.

### 3 Document your cryptographic baseline and PQC posture

NIST finalized the first post-quantum cryptography standards in 2024. The migration timeline to quantum readiness is long and the inventory requirement is immediate: you cannot plan a cryptographic migration without knowing what you have.

The correct action now is to establish a documented cryptographic baseline across your organization, identify long-lived certificates and CA keys that carry the most exposure, assess whether your HSM infrastructure supports PQC algorithms, and assign ownership of the migration roadmap. Organizations that defer this until the threat (or compliance mandate) is immediate will execute the migration under pressure, without the inventory or the automation infrastructure needed to complete this effectively.

# Pillar 3: Automation

The volume of renewal-and-deployment cycles required at 47-day validity exceeds what any manual process can reliably sustain at enterprise scale. Shorter certificate lifespans also apply to ephemeral workloads and AI agents. Organizations understand the urgency to automate, but many get two things wrong.

## Inverted systems priorities

The instinct is to pilot automation on low-criticality services where failure is inconsequential. The problem is that you then scale a model validated on assets nobody would notice if they broke onto the services your business cannot function without. Start with Tier 0 and Tier 1 services: customer-facing, revenue-impacting, identity-critical. They force you to build the program correctly with deterministic deployment paths, tested rollback procedures, and closed-loop validation. A routine built for your most critical services is what every other service in your estate should also have.



## The undeployed metric of success

Measuring issuance success is the wrong metric. An automation pipeline that reports a successful renewal has not confirmed that the certificate was deployed, that the service reloaded, or that the service is healthy. This is the “renewed-but-not-deployed” condition that is a common failure of partially implemented automation programs. Ultimately, the only metric that matters is whether the service is presenting the expected certificate at the live endpoint. Build that confirmation into every automation workflow.



You may not be able to automate 100% of your certificates. Most of your systems will be automation-ready through support for standard protocols. Manage the remaining systems as a temporary exception with compensating controls and a defined retirement path. An exception register that grows without shrinking is not a sign of a complex environment. It is a sign that the program is not working or not being enforced.

## Leadership owns:

- Approving the criticality tier model that determines the rigor of controls applied to every certificate
- Mandating that inventory is sufficiently mature before any certificate moves into production automation
- Setting the exception policy and review cadence; the rate at which exceptions accumulate or are retired is the most reliable leading indicator of program health
- Requiring that runbooks are tested, not just documented, and that break-glass procedures for critical services are rehearsed on a defined schedule

# Questions to identify strengths and gaps

- Can you produce a complete and current inventory of every certificate in your environment?
- Does every certificate have a named owner with a tested escalation path?
- Are you monitoring Certificate Transparency logs for your domains, with a defined SLA for reconciling unexpected issuance?
- Has your CA hierarchy been formally documented and approved, including key custodians, use-case separation rationale, and cryptographic standards?
- Do you have a CA rationalization roadmap? Does it identify all PKI environments you are currently operating, and document the plan for bringing them under unified governance?
- Has a named owner been assigned to your post-quantum cryptography migration?
- Are you starting automation efforts with your most critical services? Are you measuring deployment success, not just issuance success?
- Is the exception register static, being actively retired or growing?

## Accountability model

| Responsibility | Central PKI team | Platform & app teams | CIO / CISO |
|---|---|---|---|
| Certificate inventory standards and tagging | Own | Confirm ownership within their domains | Demand evidence of completeness |
| CA hierarchy design and key custody | Own | Implement within approved model | Approve architecture and custody decisions |
| CA rationalization roadmap | Own | Migrate on defined schedule | Hold accountable to timeline |
| Cryptographic baseline and PQC roadmap | Own | Implement per standard | Assign named owner; set timeline |
| Certificate profile governance | Own | Use approved profiles; escalate exceptions | Set policy on exception authority |
| Exception register and review cadence | Own | Submit exceptions with retirement plans | Set cadence; review aging exceptions |
| Incident response playbooks | Own and test | Execute per playbook | Require evidence of testing and review |

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. Whether you're mapping your first inventory or untangling PKIs that grew without a plan, we can help you find the right starting point.

Ready to design a PKI modernization roadmap for your organization?

Start the conversation

## 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.