digicert®

Certificate Lifecycle Maturity Assessment Guide

Your Path to Reducing Costs and Eliminating Outages with an Agile Public Key Infrastructure (PKI)

GUIDE

Introduction

The Connected World Requires Modern Certificate Management

PKI certificates provide the foundation of digital trust for the connected world. Modern networks operate on increasingly complex infrastructures that continuously scale and evolve alongside enterprise needs. These networks don't exist in isolation. Modern systems interact with many other networks, internal and external. Providing trust for this level of complexity requires certificate management that is equally scalable and adaptable.

Methodology

What is Certificate Lifecycle Management (CLM) Maturity?

CLM maturity is a journey from manual, reactive practices to automated, policy-driven operations. As maturity increases, associated costs and risks are significantly reduced. The implementation of stronger management tools, policies, and integrated automation are all important elements in your organization's journey to cryptographic agility.

Crypto-agility is the ability to quickly update or replace cryptographic algorithms, keys, and protocols in an automated fashion with minimal disruption to operations. While CLM is a significant component of crypto-agility, it's important to understand that the full scope also includes other cryptographic assets, such as encryption keys for databases, computer hard drives, multi-factor authentication (MFA) keys, and more.

The PKI Renaissance

PKI is undergoing a mandatory rebirth. This renaissance is driven by a series of events that require action in order to address security threats, regulations, scalability, and lifecycle management challenges. The good news is that this transformation will lead to a new generation of PKI that is more secure, resilient, and agile.

Factors Driving the PKI Renaissance

- **Shortened certificate validity**
  By 2029, organizations will need to operate certificates with 47-day validity periods for all public trust use cases. This decision by the CA/Browser Forum will make manual processes practically impossible to maintain.

- **Explosion of Machine Identities**
  From APIs and IoT devices to containers and multi-cloud environments, machines now represent billions of connections. Soon, there will be three times as many devices as humans—not including the coming wave of AI agents that will also need trusted identities.

- **Operational Scale and Complexity**
  Traditional cloud and hybrid environments blur the lines between external, internal, and federated PKIs. These systems demand large volumes of varying certificate types, which in turn requires a flexible CLM that can seamlessly tie everything together.

- **The Quantum Threat**
  The very foundation of PKI—the cryptographic algorithms that cannot be guessed or brute-forced with today's computing power—is now under threat. Quantum computers will soon be able to break existing crypto algorithms. New, quantum-safe algorithms exist, but they need to be tested and deployed everywhere by 2029, according to Gartner and other industry experts.

The CLM Maturity Scale

The scale below outlines three levels of CLM maturity: Ad Hoc, Developing, and Maturing. Each level provides a high-level summary of what your certificate management environment may look like at that stage. In the sections that follow, this scale is applied to six key CLM best practice areas, with tailored maturity descriptions for each level that aligns to each discipline.

- Ad-Hoc
  Management is conducted primarily through reactive, manual processes with very little visibility into the full certificate landscape or existing risks. Processes are difficult to control, and policy is underdeveloped or siloed, making it difficult to enforce. Certificate inventory is often managed in spreadsheets.

- Developing
  Management includes centralized visibility with partial control over risk notification and mitigation. Policy-driven governance is being introduced, and certificate renewals are automated for over 30% of systems, while automated certificate deployment is in place for a small set of critical systems and applications. Outages caused by failures of manual certificate management processes are common.

- Maturing
  Management includes centralized visibility with near-complete control over risk notification and mitigation. Policy-driven governance is now the norm rather than the exception. Certificate renewals are automated for over 50% of systems, and automated deployment is implemented for the most critical systems. Ongoing efforts focus on onboarding and integrating tier 2 and 3 systems as part of a broader crypto-agile strategy.

Applying the model to your organization

Because your needs are unique to your organization, applying crypto-agile tools and processes to your certificate landscape requires an understanding of where you are in the maturity model. This guide helps you assess six key areas of Certificate Lifecycle Management to determine your organization's position as you progress toward crypto-agility.

Assessment

Assess your organization's CLM Maturity

These best practices describe an ideal state for solutions, workflows, and governance surrounding crypto-agile PKI. Use these descriptions to assess your current state and chart a course toward increased maturity.

Category One

Discovery and Inventory

The capability to know where all your certificates are, how they are configured, when they expire, who owns them, and the relevance to the organization. Building this inventory requires data from multiple sources to bring your external, internal, and embedded PKIs into full view.

- **Ad-Hoc:** Manual tracking, typically utilizing spreadsheets. Visibility is fragmented and limited, with little insight into the full certificate landscape and associated risks.

- **Developing:** Scheduled discovery with limited automation. Owners are identified, and basic notifications for renewals and expirations are in place, enhancing visibility and accountability.

- **Maturing:** Real-time, continuous discovery across internal, external, and third-party PKI sources. Centralized ownership is documented and leveraged for proactive alerts, approval workflows, and governance at scale. The system also provides analytics for cost tracking and forecasting.

Critical reason

Discovery drives inventory, which enables policy and, ultimately, automation. When you have discovery and inventory capabilities, you know where all your certificates are, how they are configured, when they expire, who owns them, and the relevance to the business—even if the certificates come from shadow IT.

Category Two

Policy and Governance

The implementation and enforcement of well-defined policies that enable rules-based issuance, renewal, and revocation. These policies prevent misuse, minimize the risk of certificate outages and unauthorized access, and ensure the organization remains in compliance with standards and regulations.

- **Ad-Hoc:** If oversight exists, governance is occasional and typically reactive. There is no effective way to apply or audit policy across the environment, making consistency and accountability nearly impossible.
- **Developing:** While consistent communication and some governance exists, policy enforcement is still largely manual. It remains difficult to apply policies consistently across business units or regions.
- **Maturing:** Governance is embedded into the CLM processes through policy-driven automation. Rules are applied dynamically, ensuring consistent issuance, renewal, and revocation. Teams can quickly report on the status of PKI assets.

Critical reason

Strong policy and governance reduces human error, accelerates remediation, and enforces accountability across teams and environments—transforming certificate management from a reactive burden into a proactive, strategic asset.

Category Three

Integrated CLM Automation

The ability to automate renewal and deployment of certificates with the corresponding certificate authorities, and the deployment of certificates to their specific servers, applications, devices, etc., on a repeatable basis with minimal human intervention. Dependent on a solid, centralized inventory with defined owners and policies, as well as varying integration methods and protocols, subject to the requirements of each system.

Note: While the Automated Certificate Management Environment (ACME) protocol is often used interchangeably with the subject of CLM automation, ACME represents only a small part of CLM automation.

- **Ad-Hoc:** No automated management or renewal. Administrators renew and install certificates manually, prompted by calendar alerts or other reminders. As certificate volumes increase and their validity periods drop, the burden of this work increases, along with the number of outages.
- **Developing:** Individual machines are configured to check certificate status and renew and install certificates automatically, running regularly on a schedule. The automation is distributed with no way to centrally monitor status, respond to errors, or apply policy.
- **Maturing:** Central automation of renewals, replacements, and installation of certificates, based on a central inventory and ownership defined by global policies. This automation helps to facilitate the planned adoption of cryptographic changes, including Post-Quantum Cryptography.

Critical reason

Because ACME must be configured on each endpoint, it doesn't scale easily across complex environments. Even when certificate ownership is distributed across teams or systems, a centralized approach to management is essential. This ensures visibility, consistency, and control—something ACME alone cannot provide. You need other protocols and integrations to centrally manage all tasks across your entire ecosystem.

Category Four

Audit Readiness

The ability to track and proactively log all certificates through automation with the analytics and reporting necessary to quickly produce evidence of compliance. To unify certificate data and related change logs across enterprise systems, including Active Directory, and asset management platforms like SAP EAM and ITSM tools.

- **Ad-hoc:** Virtually no evidence of compliance nor ability to produce it in a timely manner. Without oversight of existing assets, risks, and needs, the organization cannot respond to audit requirements or prevent outages.
- **Developing:** Inventories and evidence of policy compliance are available but not centralized. There is no consistent tracking of policies and procedures across all certificates and applications. Visibility and audits are possible but resource intensive.
- **Maturing:** Full accounting of certificates, policies, and procedures across the majority of applications in your enterprise. This enables the ability to respond quickly to audits to produce evidence of policy enforcement.

Critical reason

To avoid compliance missteps, you need to know where your certificates are and maintain the capability to actively manage them. The key to this is full auditing across all CAs and all systems, with the ability to conduct reporting that meets industry standards.

Category Five

Public, Internal and Federated PKI

Converged visibility and control over all PKI; both public, internal, and federated, regardless of use case. The ability to use the right type of certificate trust model for the right use case.

- **Ad-hoc:** Internal PKIs likely exist within the organization, but the capability to find and centrally manage those private CA certificates does not exist.
- **Developing:** The organization has mapped its siloed PKIs and addressed critical security or compliance issues. However, these PKIs remain isolated and managed separately.
- **Maturing:** The organization has full visibility into, and management of, public, internal, and federated PKIs through a consolidated system. The internal PKIs can be managed through a centralized solution rather than application tools. A capable CLM can seamlessly replace Microsoft CA with the management of Active Directory certificates. It can manage certificates from any public CA, making it easy to move certificates from one to another.

Critical reason

In the real world, the number of certificates in private or internal PKIs dwarfs that of public ones, but the difference should probably be greater. Sysadmins sometimes use public certificates, particularly free ones, when the application would be more secure with internal or federated PKI, but this introduces risk. You should choose the right PKI for the use case and maintain the ability to monitor and control every certificate, regardless of type.

Category Six

Scalability and Extensibility

Crypto-agile solutions and processes allow for growth and change across the organization and over time, with allowances and readiness for Post-Quantum Cryptography integrations.

- **Ad-hoc:** Certificate management is fragmented and unscalable requiring manual intervention at every step. The result is a brittle, reactive system that cannot easily evolve.
- **Developing:** Certificate issuance is partially standardized with a mix of legacy private CAs, cloud services, and public CAs. However, management is still fragmented, along with development and maintenance for integrations.
- **Maturing:** Central control allows enterprise PKI to run on-premises and in one or more clouds. This level of PKI scales with the growth of users and machines, and it integrates with many technologies as the enterprise infrastructure evolves.

Critical reason

Brittle integrations often break, require frequent fixes, and struggle to support new requirements and workflows. Mature CLM processes enable your organization to dynamically respond to business and security needs, supporting automated provisioning, flexible policy enforcement, and seamless integrations across on-premises, cloud, and hybrid environments.

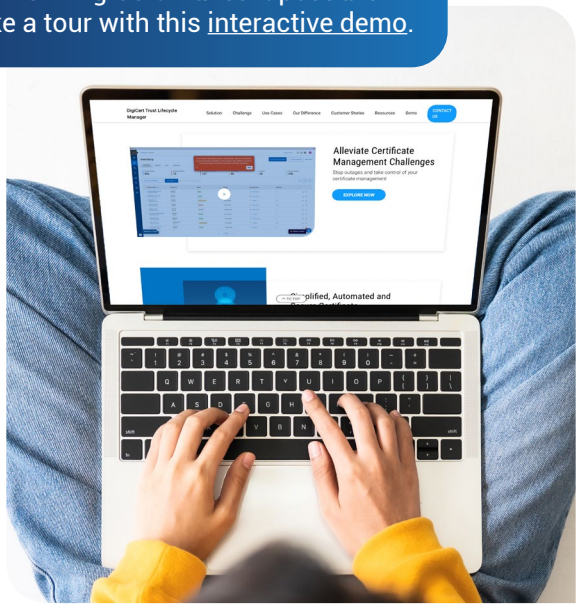
What To Do With This Guide

Taking the Next Steps

Now that you have a sense of your organization's current maturity level, where do you go from here? It's important to keep in mind that automation itself is not the end goal, nor are you trying to reach a final state of maturity. By focusing on crypto-agile solutions, processes, and policies, your organization will continue to adapt as your systems grow, standards evolve, and new threats emerge.

With the right Certificate Lifecycle Management solution, you can future-proof your infrastructure, ensure compliance, and maintain trust in a rapidly changing digital ecosystem.

See how DigiCert makes it possible.
Take a tour with this interactive demo.



About DigiCert

At DigiCert, finding a better way to secure the internet goes all the way back to our roots. That's why our PQC, TLS, PKI, and IoT solutions are trusted everywhere, millions of times a day, by people and companies around the globe. It's why our customers consistently award us the most five-star service and support reviews in the industry. And it's why we'll continue to lead the way toward a quantum-safe future powered by digital trust for the real world.