EBOOK

Certificate Management Maturity Model

A Practical Guide to Scale and Automate Certificate Management

KEYFACTOR

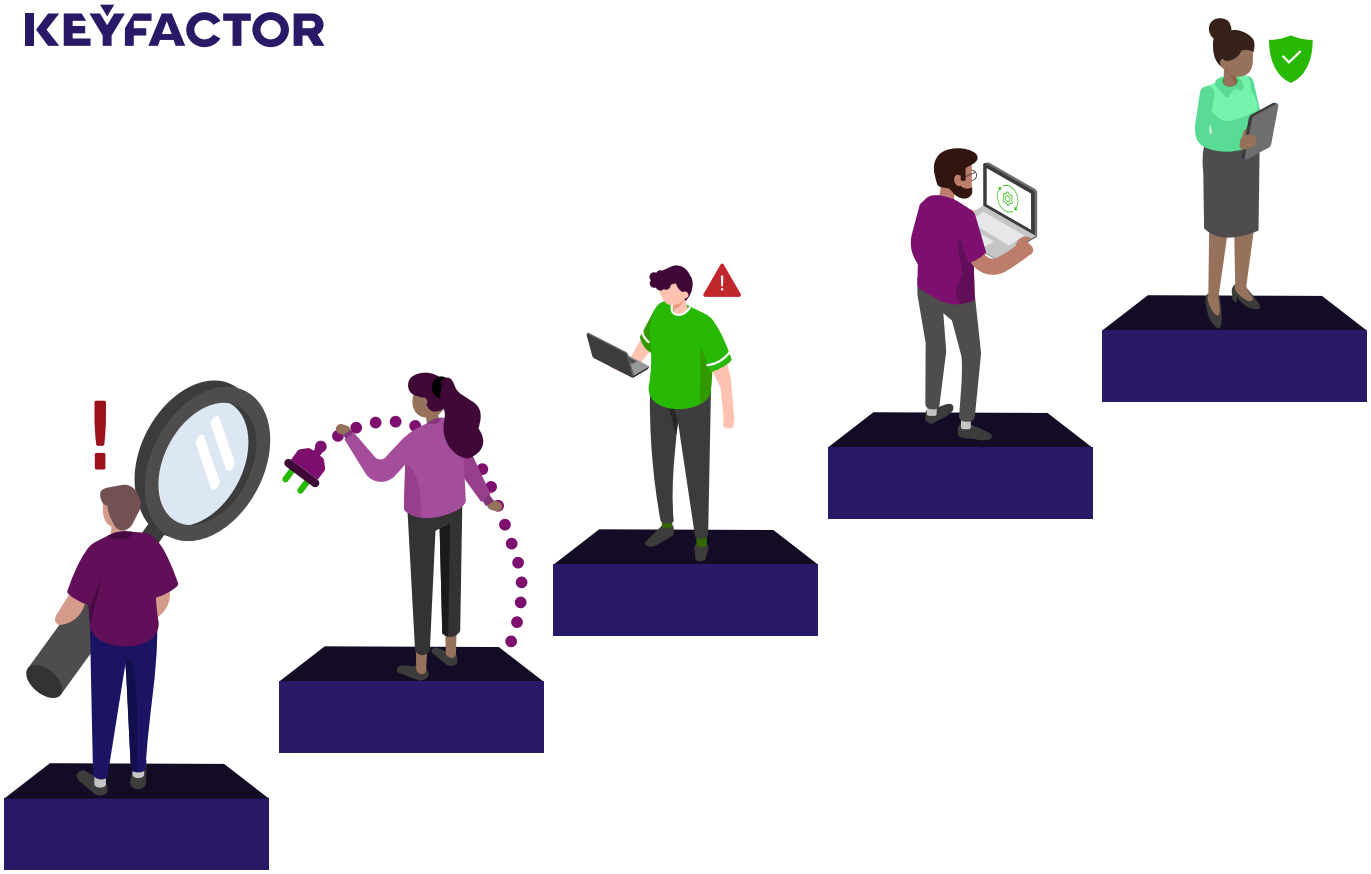


Table of Contents

The Growing Need for Certificate Lifecycle Management

The role that digital certificates and keys play to secure your business has reached critical importance.

The exponential growth in certificate usage has reached unprecedented levels; industry standards for certificate lifespans continue to shrink; and quantum-safe certificates are starting to gain traction.

On average, a typical organization uses 88,750 keys and certificates today to secure data and authenticate systems.

However, over 73% of companies admit that digital certificates have and continue to cause unplanned downtime and outages.

What's more concerning is that over half of these same companies say they have experienced four or more certificate-related outages in the past two years alone.

These are just some recent examples and challenges that plague the minds of IT and security leadership.

Bottom line: **security teams need to get certificate management under control.**

And that's why we've built this model to help.

The broad scope of certificate management makes it hard to know how mature your current practices are today and where they need to be for the future.

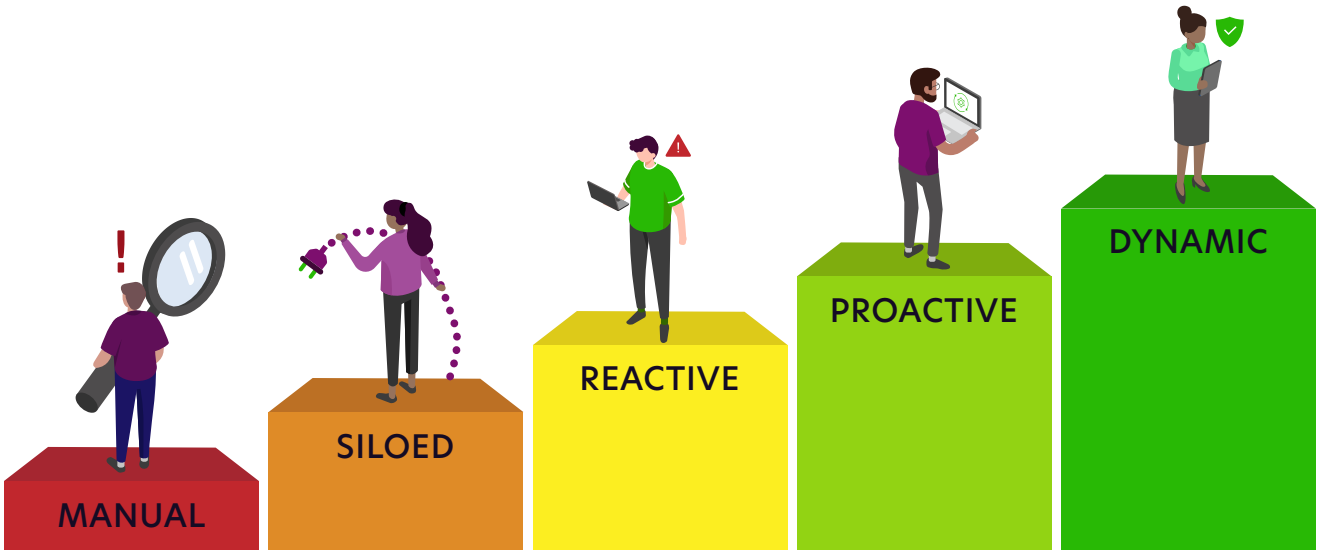
Each level in this model gives you a description of the most common scenarios we hear from the companies we work with every day.

This model outlines practical next steps to move you to the next level, and provides quick insights into your expected achievements.

Ways to use this guide:

- **Self-Assess:** Start by understanding each maturity level and pinpoint where you stand.
- **Identify Gaps:** Define your success criteria and plan practical next steps to address existing gaps.
- **Make a Plan:** Share findings with your team and involve leadership in the process.

Now let's take a closer look at the five levels of certificate management maturity. By doing so, you'll understand how to scale and automate the management of certificates across your organization (and keep your sanity in the process).



LEVEL 1:

Managing at High Risk with Manual Processes (Manual)

Spreadsheets & Manual Process • Time-consuming and error-prone • High risk of outages

At Level 1, you're likely aware of the increasing volume and sprawl of certificates across your organization, yet you're still tackling the problem with highly manual processes. This typically involves using spreadsheet-based tracking to keep tabs on your inventory and using some form of calendar reminders or scripts to notify certificate owners about pending expirations.

The problem with manual processes like spreadsheets is that all certificate information must be kept up-to-date and regularly reviewed to ensure that certificates don't unexpectedly expire. All this repetitive work presumes there will be no error or oversight in the process and relies heavily on administrators to ensure all data is accurate and current.

There are four critical components missing from manual tracking:

Visibility:

Spreadsheets only account for known certificates that you're tracking, but it's the unknown and untracked certificates that cause outages.

Resources:

It's time-consuming to maintain an active record of all certificates and ensure the data you have is correct and accurate.

Error-Prone:

Manual actions lead to higher risks of errors like missing a certificate to a misconfiguration of an endpoint — and these lead to outages, or worse, breaches.

No Automation:

The steps required to request certificates from CAs are slow and manual, not to mention issuance, provisioning, renewal, and revocation.

This DIY solution might be good for a small number of certificates (e.g. less than 100); however, this process quickly starts to take up too much time, and attention to detail immediately suffers. Moreover, since different company departments may purchase certificates from various certificate authorities (CA) or stand up their own CAs, there's a high probability that many of these certificates have not been accounted for.

At the end of the day, you might not have experienced a catastrophic event due to an expired certificate, but you've realized you're not prepared to prevent one.

Level one should highlight the need for better oversight, the need for an established process, and identification of how to remove manual processes.

Next Steps

- Understand which business units and applications rely on certificates
- Audit the number of CAs in use across your environment, how they're used, and where they live
- Identify immediate risks and assign clear ownership for certificate management

Questions to ask

- Do I know how many certificates are in use?
- How many CAs are actively issuing certificates in our environment?
- How much time is spent issuing and updating certificates across all departments?
- Are we confident in our knowledge of potential weaknesses and vulnerabilities? (i.e. SHA-1, MD5, etc.)

LEVEL 2:

Limiting Risk through CA Provided Tools (Siloed)

Doing the Bare Minimum • Fragmented, Siloed Visibility & Reporting • Zero to Minimal Automation

At Level 2, your team should look to introduce more oversight into certificate issuance and usage. For example, you may introduce tools provided by your SSL/TLS vendor. These tools offer better reporting on certificates issued from their infrastructure.

While tracking the initial issuance of a certificate from the CA is no longer a problem, it's the unknown and untracked that keeps you up at night. Knowing the existing expirations dates helps with visibility, but now you must find where each certificate resides across your network, and who to contact in order to properly renew. However, this is easier said than done.

The problem is that a certificate can be provisioned to multiple devices. You need network-based discovery and local discovery tools (i.e. agents/orchestrators) to find where those certificates end up on your network, which applications use them, and where the private key is stored.

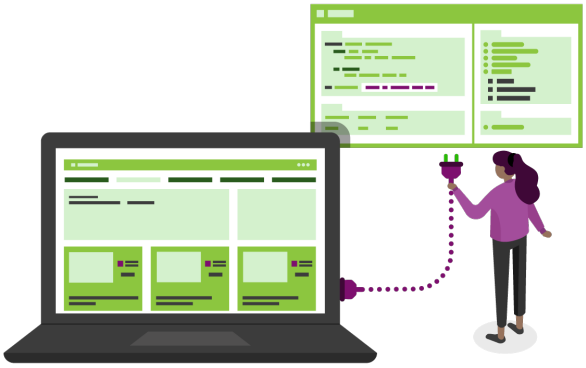
Although you're making progress out of a manual state of being, you're dealing with multiple silos of certificate management spread across disparate toolsets. This siloed management and reporting on upcoming certificate expirations leaves you exposed to critical service interruptions due to expired or misconfigured certificates.

Level 2 also highlights additional challenges in user management and permissions. If one user has access to an issuing CA, they might not have the same access to another CA. This separation of ownership leaves a hole in the overall governance of certificates across your company and creates a single point of failure with no backup for remediation.

You're standing at the crossroads of where you should start to invest to scale your certificate management. Either you need to invest in more resources to handle increasing workloads, or you need to research full certificate lifecycle management tools that can scale across multiple use cases.

Next Steps

- Look for solutions that support network-based discovery of rogue or unknown certificates across your internal and internet-facing infrastructure
- Replace manual certificate requests with automated workflows and lifecycle handling
- Consolidate inventory and management of certificates across internal and external CAs into a single database



Questions to ask

- How many reports does it take to create a holistic view across multiple CAs? Which reports are missing?
- How many CAs do we have and how do we consolidate inventory across all of them?
- If a certificate is near expiration, how do we make sure the owner will renew it in time?
- How do we notify application owners when certificates are near expiration? How do we escalate the issue if the app owner fails to take action?

LEVEL 3:

Full Oversight with a Single Pane of Glass (Reactive)

Centralized Visibility & Control • Advanced Reporting & Alerting • Expiration Reporting

Risk lies in not knowing where certificates are being used: you can't manage the unknown. Prior to Level 3, there was sporadic oversight of the certificate landscape across fragmented disparate tools and data sources.

Now that's all changed.

Level 3 begins a massive turning point in your certificate management maturity. Consolidation of all certificates, across all issuing CAs (public and private), has been brought under a single pane of glass to manage. Teams can now start categorizing certificates and assigning metadata to better understand the breadth of their certificate inventory.

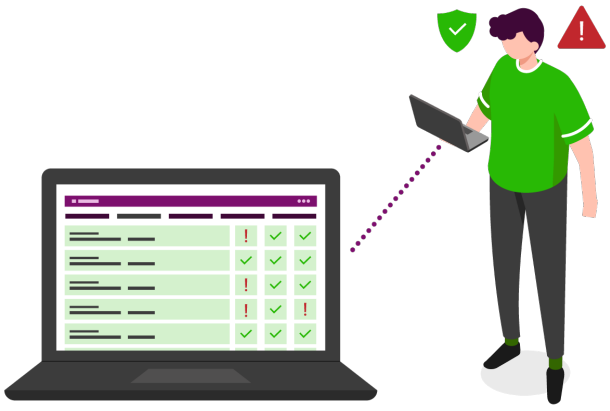
A continuous inventory scanning and monitoring process has been established to always know where each certificate lives, when it needs to be renewed, where it is located, and who issued the certificate. You've expanded your certificate monitoring to detect any weak keys, signing algorithms, or validity periods around the certificate, so you can respond to crypto events in real-time.

Reporting gets a major upgrade as you move from static visibility to proactive prevention, detection, and response. Multi-CA support and simplified dashboards provide an overview of your environment. You're able to pull any report within minutes, rather than days or hours, that instantly gives the health status of your certificates.

Level 3 should provide a peace of mind around having a complete inventory, but more work is ahead. Automation needs to be incorporated to stop the reactive communication around certificate activities across departments.

Next Steps

- Identify high-priority applications for certificate automation (e.g. web servers, load balancers, etc.)
- Define automation and approval workflows for certificate issuance, provisioning, renewal, and revocation
- Shift to a self-service model for application owners to request security-approved certificates from a common portal or API



Questions to ask

- Can we access the reports we need in minutes?
- Which applications are most affected by outages caused by expired certificates?
- How much time do application owners and PKI administrators spend on requesting, issuing and provisioning certificates?
- How quickly can we identify and remediate certificate-caused outages?

LEVEL 4:

Enabling Self-service and Automation (Proactive)

Certificate Lifecyle Automation • Simplified CSRs • Automated Workflows with ITSM

At level 4, automation now starts to take center stage as you move from certificate management into certificate lifecycle automation. This starts with providing users a self-service portal or API to easily request certificates. Then you can automate the lifecycle of those certificates – from provisioning them to end devices to renewing them automatically before expiration.

Beyond sending alerts to users about expirations, which then requires manual actions, you're now able to push certificate updates without any need for human intervention. This allows you to renew certificates with the same information as the previous certificate, and automatically bind that certificate to the necessary application.

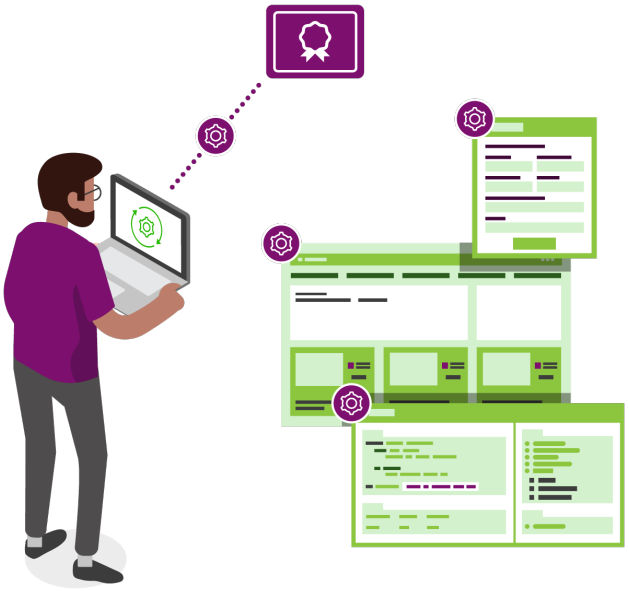
Automated workflows, self-service certificate issuance, and integrations with existing ITSM tools, like ServiceNow and BMC Remedy, become a significant time-saving mechanism for the business.

By allowing network and infrastructure teams to easily obtain certificates on demand, you've reduced the workload on PKI and security teams that would normally be spent fulfilling certificate requests. Not only does this improve productivity and reduce costs, but it also allows you to more easily expand into new use cases.

Level 4 should give encouragement that automation has begun and this motivates you to look for more ways to start extending automation across the business. You've laid the groundwork for certificate lifecycle automation and reduced the workload brought on by growing certificate counts. Now it's time to think about aligning your identity strategy with leading-edge initiatives, like your DevOps workflows and cloud infrastructure.

Next Steps

- Achieve end-to-end automation
- Partnering with engineering and development
- Evaluating current state PKI



Questions to ask

- How much time does it take to process CSRs?
- After a certificate alert is received, where can we add automation to resolve?
- Can certificate owners bypass manually importing certificates onto applications?

LEVEL 5:

Zero-Touch Automation, Achieving Crypto-Agility (Dynamic)

DevOps Integrated • Cloud-First PKI Strategy • CA & Technology-Agnostic

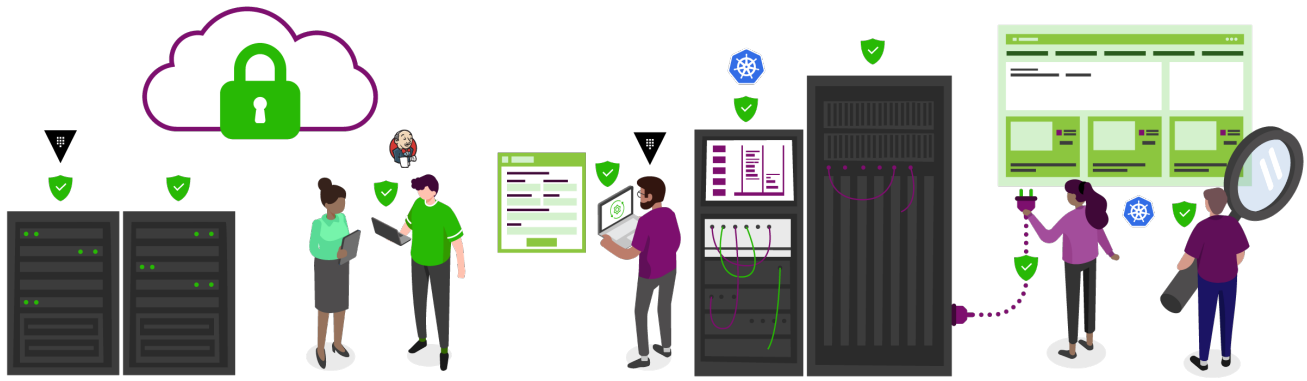
If you have reached Level 5, you've moved into a premier status for certificate lifecycle automation. It still may be unrealistic to expect that every certificate lifecycle is automated; however, you know about every certificate, have a process in place to manage them, and have automated the things that save the most time and reduce the most risk.

You have a complete and continuous inventory for all certificates in the environment irrespective of source or destination — especially when related to DevOps workflows.

Development and engineering will always prioritize speed over security. At Level 5, you're merging automated DevOps workflows and security-approved PKI, without slowing them down. This means automating the deployment of certificates through infrastructure and container orchestration tools like Kubernetes, Docker, and Istio service mesh that's backed by a secure root of trust. InfoSec teams are now a part of the DevSecOps fabric that helps engineers succeed rather than blocks their speed to innovate.

PKI operations, and not just cert management, now achieves critical importance. PKI goes beyond the management of keys and certificates. It's about the people, infrastructure and policy behind your PKI that allow you to respond and make changes in cryptography, such as signing algorithms, key lengths and validity.

Monitoring issuance from your CAs now becomes critically important. For example, seeing a spike in one-year certificate issuance from an issuing CA might not be a problem. However, if the intermediate CA is about to expire, all of those recently issued certificates are now about to expire without notice.



Signs You're in Level 5

- Deployed a Cloud-First PKI Strategy
- Support a multitude of CAs, applications, and devices
- Aligned with DevOps priorities and certificate usage practice
- You've mastered automation of PKI and certificate-related processes

Next Steps

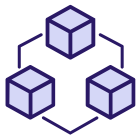
- Make a plan to change your certificate management process
- Expand practices into SSH key management
- Investigate PKI use cases for IoT device identity provisioning
- Sync with developers on how to deploy secure code signing

Getting Started

Now that we've covered the steps to certificate management maturity, it's time to put plans into action. Here are some practical steps you can take to kick off the roadmap to certificate management success.

Bring in the A-TEAM

Chances are that multiple teams across your organization manage digital certificates. Bringing in a stakeholder from each of these teams will ensure that you understand all current and planned use cases. For instance, a team could have stood up their own CA infrastructure for a specific use case, without the necessary knowledge or support of the enterprise PKI or security team. Building a cross-departmental team helps you all align on priorities to enhance certificate management for the future.



Map Out Your PKI

Take your learnings and start mapping it out. Nothing is more powerful for conveying a message than a picture. Take time to map out your entire CA infrastructure and certificate management processes on a whiteboard, connecting workflow diagrams, or simply writing it down on a napkin. Once you get the process out of your head and into a visual, this helps you quickly identify gaps and inefficient processes.

Share Best Practices

Learn more about cross-team challenges by joining department meetings. Join their stand-up calls and digital strategy meetings to better understand how certificate management is being done. Are there best practices that need to be shared across different business units? Or do you see a bigger problem coming to a head?

Propose a Business Plan

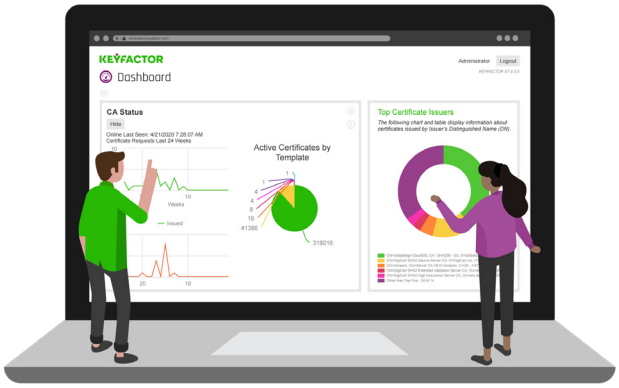
In the end, you might realize that you have certificate management under control, or have major work to do in the days ahead. If additional work is involved, you'll need to build a business plan to either do the work in-house, evaluate tools to help, or keep the status quo. To justify the budget necessary for your project plan, you'll need to convey the business reasons for improving your certificate management maturity. Tie your strategy back to quantifiable metrics such as improved productivity (hours), reduced risk (outages), and cost-savings (uptime).

Conclusion

See how achieving a Dynamic state with certificate lifecycle automation can help keep your certificates and keys more secure with less effort:

Request a demo of Keyfactor Command.

REQUEST A DEMO



KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains. With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook. Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

CONTACT US

- www.keyfactor.com
- +1.216.785.2990