EBOOK

PKI Maturity Model

A Practical Guide to Modernize PKI

Read before you start

Public key infrastructure (PKI) isn't anything new. It's been around for decades. Beginning as the trust engine behind the internet, it is now ubiquitous in every business to authenticate and establish trust in each device, workload, human, and connected thing.

As critical as it is for security, PKI is often disjointed and misunderstood. Someone sets up a Microsoft CA or installs OpenSSL, and they say they're "doing PKI." The problem with this overly simplistic definition is that it creates a disparate approach, where PKI is a "tool" versus a strategic asset – making it extremely difficult to govern and secure.

The reality is that PKI isn't just software. It's critical infrastructure that requires processes, policies, infrastructure, the proper tooling, and people to manage it. To establish trust and better support business initiatives, organizations need a deeper and broader understanding of how PKI is used across different teams and applications, then develop a strategy for how it should be designed, deployed, and managed to match those needs (and future needs).

There's just one problem – well, maybe a few.

For starters, cybersecurity skills aren't exactly a dime a dozen. Many IT and infrastructure groups don't have the headcount or the skillset on their team to handle PKI. Either that or the one person who knew how to run it switches roles or moves on, and suddenly you're left with a PKI "hot potato" to pass onto the next IT admin in line.

Meanwhile, the move to the cloud, containers, and microservices, combined with the need to support remote work and IoT devices, only increases the demand for PKI. A recent report shows that 53% of organizations don't have enough staff to maintain PKI, yet the average company has nine different PKI solutions they need to manage.

The worst part is, in many cases, the team responsible for managing PKI is set up for failure right from the start, tasked with building a modern solution using tools and software from the 2000s (you know, back when we were playing Snake on our retro mobile phones).

Bottom line: it's time for a modern, agile, resilient PKI strategy.

It's not all bad news. PKI has come a long way since its inception. New technologies have emerged, standard protocols and well-documented guidance are now widely available, and PKI practices have evolved to meet modern requirements.

That's why we've built this maturity model. Whether you're new to the space or an experienced practitioner, this guide will help you measure your current maturity level against advancements in PKI practices and help you establish a new foundation for an agile and modern PKI that can scale with your business.

Table of contents

Introduction 4

Understanding and assessing PKI maturity 5

The path to PKI maturity 6

Level 0: Ad Hoc 8

Level 1: Limited 10

Level 2: Foundational 12

Level 3: Transformative 14

Level 4: Resilient 16

How to Get Started 17

Introduction

As the IT and threat landscape evolves, your cybersecurity efforts must follow suit. With PKI serving as the foundation of trust for your business, you must ensure that it can handle anything that comes its way.

Whether your organization's PKI is run by a team of one or two or a 24x7 operation, advancing maturity will help improve overall security posture, drive efficiency, and become fast and agile in response to the changing needs of the business. This guide explores Keyfactor's PKI Maturity Model (PKIMM), which explains how to measure the effectiveness of PKI operations.

In this guide, you will learn:

- How to understand and measure the operational excellence of PKI
- How to evaluate your organization's PKI maturity and where to start
- The five levels of the Keyfactor PKI Maturity Model (PKIMM)
- The potential risks and setbacks of not improving PKI maturity

Author:

Ryan Sanders

Product Manager
Keyfactor

Subject Matter Experts:

Bryan Uhri

PKI Product Manager
Keyfactor

Chris Hickman

Chief Security Officer
Keyfactor

Neal Fuerst

Sr. Director, Federal
Compliance, Keyfactor

Sven Rajala

Sr. PKI Solutions Engineer
Keyfactor

Ted Shorter

Chief Technology Officer
Keyfactor

Tomas Gustavsson

Chief PKI Officer
Keyfactor

Understanding and assessing PKI maturity

Keyfactor's PKI Maturity Model (PKIMM) is based on research and conversations with enterprises across industries and has been validated by practitioners, analysts, and thought leaders. It's a high-level framework for assessing the current state of your organization's PKI capabilities and effectiveness, creating a plan to improve them, and measuring ongoing success and business value at each stage.

The first step to maturity is understanding the critical capabilities required to support a best-in-class PKI. This assessment evaluates six critical categories: reliability, efficiency, security, governance, agility, and strategy.

Reliability

Ability to provide resilient, high-performing, and scalable infrastructure (the "I" in PKI), which includes CA software, servers, revocation, etc.

Efficiency

Ability to efficiently operate PKI, including configuration, installation, maintenance, certificate management, and required staffing and resources.

Security

Ability to define and enforce adequate security controls for PKI and proactively identify and remediate security risks and incidents.

Policy & Governance

Ability to make policy-based decisions, continuously monitor PKI posture and consistently adhere to established policies and procedures.

Agility

Ability to deliver CAs and certificates seamlessly to support new use cases and standards, which requires extensibility, self-service, and CA-agnostic support.

Strategy

Ability to plan and deliver on capabilities that align with the overall strategic initiatives of the business, with a focus on enabling digital transformation.

Mapping the path to PKI maturity

Understanding your PKI landscape and evaluating critical operational and security capabilities enables you to identify where your organization is today and learn how to best focus your efforts and investments. This approach ultimately positions you to better support the business and deliver value.

Trust & Security ↑

Level 0: **Ad Hoc**	Level 1: **Limited**	Level 2: **Foundational**	Level 3: **Transformative**	Level 4: **Resilient**
Disparate, fragmented CAs and PKI tools with no clear ownership	A basic PKI that meets minimum requirements, partial ownership	Well-documented, policy-backed PKI infrastructure with dedicated ownership	Unified, strategic PKI program with a vision and widespread adoption	Highly reliable, extensible, and seamlessly scalable infrastructure
Teams issue and manage their certificates without oversight	Improved security practices, but no policy or documentation	Basic observability and monitoring of PKI and certificate landscape	Integration with other PKI and CA technologies, tailored user guidance	Continuously tested disaster recovery and business continuity plans.
High risk of outages and security incidents	Reliance on legacy PKI software with minimal extensibility and scalability	Partial adoption but limited integration and automation capabilities	Automation and self-service capabilities that drive efficiency	Fast adoption of new cryptographic standards and technologies

Operational Efficiency & Agility →

When mapping your organization's path to PKI maturity, remember:

PKI maturity isn't linear

PKI is one of those things where you have exactly one chance to build it right – at design. Conversely, to build upon a poorly architected PKI is to build a house on a cracked foundation. For this reason, moving from one level of maturity to another often requires a complete rebuild or migration, particularly at the lower levels.

PKI maturity isn't permanent

PKI maturity can be broken just as quickly as it is built. All it takes is one misconfigured template or abuse of PKI privileges to degrade the level of trust and assurance in your organization's PKI, which could require lengthy remediation or an entire rebuild, depending on the severity of the incident.

PKI maturity can vary

These different levels seem clearly delineated, but they're not. In reality, PKI can be messy and fragmented. One group could have a well-architected PKI, while another uses OpenSSL without restraint. Achieving PKI maturity demands an enterprise-wide strategy.

PKI maturity is a lifecycle

There is no finish line. PKI maturity is a continuous process of assessment, investment, and re-assessment. New standards, threats, and technologies will require organizations to evolve their strategy to maintain trust constantly.

LEVEL 0:

“Doing PKI” without PKI

(Ad Hoc)

DIY PKI and CA tools • No clear ownership • High risk of compromise

At level zero, PKI is an afterthought. It’s not well understood, there is no clear ownership or accountability, and at the same time, it’s being used everywhere in the organization. That’s because virtually every team in IT needs digital certificates to do their job. Still, most don’t understand the tools, infrastructure, and policies required to issue and manage them properly (aka PKI).

So, what happens? It’s the Wild West. The Active Directory (AD) team may have a PKI to handle basic use cases like device authentication, but for the most part, every team has its way of “doing PKI.” Some buy certificates from an SSL/TLS vendor, some stand up their own certificate authority (CA), and others use accessible open-source tools and PKI utilities for convenience. It’s not PKI; it’s a hodgepodge of CAs and tools.

At this level, PKI seems deceivingly easy. Just a couple Google searches and a few clicks on the “next” button, and you’re ready to issue certificates. However, when it comes to PKI, you have one chance to get it right – at implementation. Improper policies, weak algorithms, or using the wrong key sizes can create issues down the line. If mistakes are made early on, parameters are more or less set in stone, and a complete rebuild becomes the only way to fix it.

○○○○○

Reliability

High risk of outages and operational downtime.

○○○○○

Efficiency

Inefficient and fragmented tools with no clear ownership.

○○○○○

Security

High risk of security incidents and audit failures.

○○○○○

Policy & Governance

No centralized visibility or operational oversight.

○○○○○

Agility

Ad hoc adoption on a per-application basis.

○○○○○

Strategy

No defined strategy or role within the modern IT stack.

How to recognize if you're at level 0

In level zero, there is no centralized PKI operation. Teams at this level often see PKI as a "necessary evil." No one consults with security or compliance groups before implementation. Instead, application owners stand up a CA to issue certificates, often with little knowledge of how it works. Then, they're on the hook when something goes wrong but don't know how to fix it.

The problem is that every team, from IT and sys admins to infrastructure and application teams, needs PKI, but it's not their primary skillset. The result is that there's no consistency in policy, if any at all, and critical components such as CA architecture, root key material, and templates go ignored or overlooked, creating a high-risk scenario. For example, root key material is left unprotected on a flash drive or local drive, putting the entire PKI at risk.

Moving past level 0:

Establish PKI ownership

There's no path to a higher level if you're at level zero. PKI operates on trust, and if that trust isn't established, or worse, it's compromised, the only way to fix it is to start over. The biggest risk here is having a false sense of trust in PKI and building upon it. It's time to start fresh, and to do that, you'll need to:

- Acknowledge whether you have the expertise in-house to build and maintain PKI, or if you need to consider a new hire, consultant support, or a vendor
- Define ownership over internal PKI, which at this point is typically the AD or infrastructure team (security typically manages publicly-trusted certificates)
- Identify piecemeal tools and start documenting how different IT and application owners implement PKI processes and handle certificate requests
- Invest the time and effort to plan and architect an enterprise PKI that is designed to expand with the business over time (don't skip to CA installation)

Risks of Ad Hoc PKI:

Operational downtime

A system-wide outage could occur if a CA server goes down or a CRL is not published correctly.

Outages

Certificates issued from unknown or rogue CAs expire and cause application outages.

Security incidents

Default configurations and mishandled private keys create a high risk of compromise.

Key consideration

If you're leveraging open-source or freeware, it's essential to consider whether you have all the capabilities and support you'll need to deploy and manage a PKI that can support enterprise-wide requirements and policy.

LEVEL 1:

Doing PKI with the bare minimum

(Status Quo)

Bare minimum PKI • Minimal policy & security • Shadow IT

Welcome to level one. At this stage, PKI is a recognized component in the enterprise security stack, but it’s not yet reached the status of critical infrastructure. One or two individuals – often within the AD or infrastructure group –may be responsible for PKI, among other responsibilities. They aren’t necessarily experts, but the responsibility was assigned to them, or they inherited a PKI that a previous employee built.

At level one, PKI meets the minimum standards for security, including an offline, air-gapped root of trust, use of hardware security modules (HSMs) to protect CA private keys, and a general framework for who is allowed to access the PKI, create CAs, and issue certificates. The problem here isn’t setting the policies; it’s documenting and enforcing them.

Old habits die hard. Multiple teams will still use non-compliant methods to get certificates (aka shadow IT), either out of ignorance or intentionally skirting slow and tedious PKI processes. Either way, there are still unmanaged and unknown CAs out there that create unpredictable risks for the business.

Overall, PKI at this level still feels like a pain for very little gain. There’s no real strategic direction or alignment to business initiatives, it just “exists.” And without well-documented policies and procedures, a simple misconfiguration or shortcut could compromise the PKI and move right back to level zero.

●○○○○

Reliability

PKI is not adequately resourced or well-maintained.

●○○○○

Efficiency

Inefficient and manual processes result in shadow IT.

●●○○○

Security

A centralized PKI is established but not well-adopted.

●○○○○

Policy & Governance

Lack of centralized control and documented policies.

○○○○○

Agility

Not able to quickly identify or support new business initiatives.

○○○○○

Strategy

Partial ownership but no clear strategy or vision.

How to recognize if you're at this level

Most organizations at this level rely heavily on traditional tools, such as Active Directory Certificate Services (AD CS) and auto-enrollment, to handle the day-to-day PKI functions. It works for basic use cases, but it isn't very scalable, and it's rarely well-maintained.

As organizational needs expand, you are left pushing the boundaries of current solutions, often to their breaking point, or procuring expensive ad hoc point solutions that ultimately only solve a specific need.

The biggest challenge at this level is governance. A team builds a well-architected PKI, but the procedure and process behind it sit in their memory rather than well-documented policies. If they leave the organization or move into another role, all of that knowledge leaves with them.

Without proper care and feeding, configurations drift further from the standards set when the PKI was initially built. For example, a common mistake is plugging the root CA into the network, even just for a few minutes, to patch the server or publish a certificate revocation list (CRL). Suddenly, the level of assurance in your organization's PKI has been diminished.

Moving past level 1:

Rebuild or reinforce the foundation

If your organization is at level one, you'll need to assess whether you can build upon your existing PKI or if a rebuild is required. If PKI configurations have drifted from set policies or the underlying CA software is insufficient, it's time to migrate or lay a new foundation. To move to the next level, you'll need to:

- Assess your PKI solution stack – check for vulnerabilities, re-evaluate business requirements, and evaluate alternative solutions.
- Invest in training and documentation, such as a formal certificate policy and certificate practice statement (CP/CPS), to establish and maintain assurance levels.
- Establish visibility and observability of all PKI solutions and certificates across your organization's environment (e.g., network scanning, CA discovery, etc.).
- Rationalize and consolidate PKI tools that stem from different teams procuring point solutions.

Risks of Status Quo PKI:

Configuration drift

Administrators take shortcuts and make ad hoc changes until their PKI is no longer consistent with the organization's requirements.

Policy decay

Undocumented policies and procedures quickly decay, increasing the risk of an audit failure or security incident.

Staffing changes

Without guidance and training, a shift in staff often results in PKI being left shorthanded with little to no direction for its new owner.

Key consideration

At this point, you'll need to consider whether you have the skillset and solution stack to architect and build a proper PKI that can support what the business needs and go the distance.

LEVEL 2:

Establishing a foundation for digital trust

(Foundational)

Dedicated ownership • Well-documented policy • Lack of interoperability

At level two, you've reached the big leagues. Organizations at this stage recognize that PKI isn't just part of the security stack, it's critical infrastructure that supports critical internal IT and revenue-generating services and applications. In many cases, this realization comes after a major incident, such as an outage or security breach, but sometimes it's simply a realization that their current approach has unacceptable shortcomings.

An organization at this level has dedicated resources behind its PKI. There is an individual or team with the knowledge and bandwidth required to properly maintain and operate the infrastructure, whether in-house, SaaS-delivered, or fully managed. At this point, they have moved beyond "check box" security to a well-documented and policy-backed PKI, and they're beginning to see the benefits of a well-oiled machine.

Things aren't perfect here, though. The foundational elements of security and policy are in place, but the biggest challenge here is operational efficiency. As awareness and usage of PKI increases, so does the complexity of managing it and keeping pace with demand. At this stage, processes such as requesting certificates or scaling infrastructure are still manual, which reduces efficiency and slows down other teams.

●●●○○

Reliability

Reliable and well-architected PKI infrastructure.

●●○○○

Efficiency

A well-maintained PKI, but manual processes slow down teams.

●●●●○

Security

Well-established security practices and policies

●●●○○

Policy & Governance

Well-documented policies and visibility of PKI and certificates.

●●○○○

Agility

Better visibility into use cases, but still lacks interoperability.

●●○○○

Strategy

Dedicated ownership, recognized as critical infrastructure.

How to recognize if you're at this level

At level two, organizations have invested in the organizational processes and headcount needed to support a functional PKI. The foundation is set with a formal certificate policy and certificate practice statement (CP/CPS), and you're on your way to consolidating certificate services into a single platform.

However, PKI still lags when it comes to interoperability and automation. Teams at this stage typically rely on a standard protocol like SCEP, ACME, or EST, but it doesn't support all applications and use cases. In addition, manual processes to provision and install certificates create room for error and slow down projects.

Despite policy improvements, teams at this level still run into operational fire drills. Too many people get involved when something goes wrong because nobody knows where the problem is, and the blame game ensues. Most organizations at this level will have some certificate discovery and monitoring capabilities, such as SSL/TLS network scanning, but there are still blind spots.

Shortcomings of Foundational PKI:

Inefficiency

Manual and time-consuming processes to request CAs and certificates slow down teams and cannot scale.

Lack of extensibility

Limited out-of-the-box integrations and protocols prevent the PKI team from truly enabling other business units.

Fire drills

Human errors and troubleshooting pull resources from priorities to remediate issues.

Next step:

Automate, educate, and integrate

Your next focus is easing the administrative burden by automating high-volume, low-complexity processes – an effort made easier with a PKI solution that supports high availability and automation and certificate lifecycle management capabilities beyond basic network discovery. To move to the next level, we recommend that you:

- Actively involve key stakeholders in your PKI program and establish a working group to get buy-in and guidance from end-users, such as developers and IT admins
- Provide tailored guidance to developers, IT, and security teams by defining how different PKI and CA tools should be used and when new instances can be deployed
- Align PKI architecture to enterprise architecture – backed by a mission, strategic vision, and supporting business processes and technology
- Research and adopt tooling and infrastructure that can support automation, high availability, flexible deployment (e.g., cloud, on-premise, hybrid), and extensibility

Key consideration

At this point, you'll need to evaluate your organization's PKI and certificate management stack to ensure it can support critical functions like automation, self-service, and extensibility via APIs and protocols.

LEVEL 3:

Enabling the business with automation and agility

(Transformative)

Delegated ownership • Automation & self-service • High level of adoption

Organizations at this level have fully embraced the power of PKI. It is widely adopted across the organization, and a clear vision and roadmap aligns with strategic business initiatives – from zero-trust architecture and multi-cloud security to remote workforce enablement.

At this stage, multiple teams are now involved in PKI operations. For instance, the PKI team may manage infrastructure and policy, a network operations center (NOC) runs the operations, and security handles incident response. As a result, PKI becomes an enabler – or at least, not a blocker – for developers, product security, and IT teams who can now self-service and leverage APIs and protocol interfaces to integrate with their applications.

Reaching this level takes a high level of automation, including provisioning and maintaining the backend PKI infrastructure (e.g., CA configuration and deployment) and automating certificate-related tasks for end-users (e.g., renewal, provisioning, and installation).

Most importantly, a strategic approach requires tailored guidance and training for teams that may leverage CAs and tools outside the enterprise-sanctioned PKI (e.g., HashiCorp Vault, Let's Encrypt, etc.). These teams should know if and when they can leverage these tools and the process they should follow to properly implement and integrate them.

●●●●○

Reliability

Scalable, highly available, and well-maintained infrastructure.

●●●●○

Efficiency

Self-service and automation accelerate productivity.

●●●●○

Security

Tailored guidance and training on security best practices.

●●●●○

Policy & Governance

Centralized policy and control across decentralized PKI.

●●●●○

Agility

Flexibility to support new use cases quickly and efficiently.

●●●●○

Strategy

A well-defined enterprise-wide PKI strategy.

How to recognize if you're at this level

One of the biggest changes at this level is ownership. PKI is no longer centralized exclusively under the AD or infrastructure team. Instead, a central team can govern and control PKI services, but different business units can set up their own CAs or PKI solutions under the right circumstances.

A cross-functional team, also known as a working group, can provide thought leadership, best practice guidance, and weighted tooling decisions, which eliminates siloes and better supports the needs of the business.*

By this point, PKI isn't just one or two issuing CAs behind the four walls of the data center. It's an enterprise-wide trust fabric built upon an integrated, CA-agnostic set of tools and infrastructure. Control and governance are centralized, but enforcement is decentralized, allowing teams to operate quickly and efficiently within the parameters of policy. PKI becomes a supporting technology to reinforce revenue generation and brand integrity.

Next step:

Continuously test, monitor, and adapt

Security isn't static. New threats will emerge, algorithms will evolve, and organizational changes will be unavoidable. The next steps at this level are about maintaining trust, not making monumental changes. Trust requires ongoing testing, proactive monitoring, and preparations for major changes.

- Identify new opportunities to expand automation and integration within DevOps, IoT, and emerging use cases
- Extend integration capabilities with your enterprise identity fabric to streamline processes and improve detection and response (e.g., SIEM, EPP, ITSM, IGA, etc.)
- Develop and continuously test DR and business continuity plans to ensure resiliency, which includes events like CA compromise and crypto library bugs
- Create and implement a strategic roadmap for post-quantum cryptography (e.g., crypto-asset inventory, compatibility mapping, migration planning, etc.)

Benefits of a Transformative PKI:

Uptime and efficiency

Outages and downtime are avoided with highly available and automated PKI infrastructure and certificate management.

Flexibility

Teams can proactively integrate PKI with modern applications like cloud platforms, microservices, and CI/CD tools.

Scalability

PKI and certificates are available on-demand as the business grows without exploding complexity and risk.

Faster delivery

The PKI team can take on new initiatives and deliver projects faster without slow server provisioning and maintenance.

*(16 March 2022) Managing machine identities, secrets, keys and certificates. Erik Wahlstrom, Gartner

LEVEL 4:

Maintaining a resilient and future-proof PKI

(Resilient)

Proactive planning • Agility and modernization • Minimal risk of compromise

Organizations that reach this stage of PKI maturity are far more transformative, efficient, and secure. However, without continued investment and effort, it takes no more than a simple misconfiguration to compromise the entire operation and fall back to level zero. This is where resiliency comes into play.

The foundation of DevOps, the continuous improvement mindset, applies as much to PKI operations as it does to application development. Teams that continuously monitor, test, and plan for future changes and requirements will avoid the risk of a serious breach or disruption to services and ultimately, deliver more value to the business.

There are three core components to a resilient PKI:

1. Proactive planning and business enablement
2. Continuous monitoring and testing
3. Detection, response, and remediation

Each of these components is equally important to maximize the return on investment (ROI) of PKI and avoid inevitable risks in the future, including, but not limited to, the shift to post-quantum cryptography, future mergers and acquisitions, and emerging software supply chain attacks.

●●●●●

Reliability

Continuous DR and BC testing to maximize resilience.

●●●●●

Efficiency

Expanding automation and integration with new use cases.

●●●●●

Security

Continuous enforcement and re-assessment of policy.

●●●●●

Policy & Governance

Ongoing audits and monitoring of the PKI environment.

●●●●●

Agility

Well-integrated and automated with business processes.

●●●●●

Strategy

A proactive roadmap for crypto-modernization and agility.

Get Started

Now that we've covered the steps to PKI maturity, it's time to evaluate where you stand and implement improvement plans.

Here are some practical steps to kicking off your roadmap to a successful PKI strategy.

Find your A-TEAM

PKI doesn't (or at least shouldn't) operate in a silo. Every team across the organization relies on PKI, so bringing in key stakeholders from each team will ensure you get a clear picture of your current environment. This could include IAM, security, cloud architecture, infrastructure, DevOps, application teams, and other stakeholding business units.

Seek to understand

Once you have an A-team, it's time to map out use cases and requirements, understand how certificates are used and issued, and whiteboard a rough blueprint of your current PKI architecture (fragmented as it may be). This can take days or months, but the important thing is not to rush this step. Learn more by joining weekly team meetings and stand-ups or setting up 1:1 meetings with departmental heads. Remember, this is about seeking to understand gaps, not criticizing flaws.

Assess tools, people, & processes

Identify the people, technology, and processes involved in PKI across the business. If you don't have in-house PKI expertise, it will not be an easy role to fill. Instead, consider a consultant or a PKI vendor that can provide expertise or even offload entire components of PKI operations, whether a turnkey appliance, a SaaS-delivered instance, or a fully managed service. Take time to assess existing policies and tooling and determine the risks and shortcomings of your current approach using this model.

Build the business case

Ultimately, you'll know what needs to be done, but action doesn't come without investment. Unless you've just experienced a major incident that prompts leadership to prioritize PKI, you must justify your project's time and budget. Then, tie your strategy back to quantifiable metrics such as improved productivity (hours), reduced risk (outages and security incidents), and cost savings (reduced infrastructure complexity).

The following questions act as a guide to assess maturity in each of the six categories:

Reliability

Ability to provide reliable, high-performing PKI infrastructure at scale:

- Can you deploy CA infrastructure where needed, whether in the cloud, multi-cloud, on-premises, or hybrid?
- Is your organization's PKI able to handle high demand without interruption to services? (e.g., high availability, clustering, on-demand provisioning, etc.)
- Does your organization have disaster recovery and business continuity procedures for PKI? How often are these procedures tested?
- How often does your business experience PKI-related outages that impact employees or revenue-generating services?

Efficiency

Ability to manage and operate PKI with efficiency:

- Has your organization established service level agreements (SLAs) to approve and fulfill certificate requests? How often are these SLAs met?
- How much time do teams spend managing and maintaining PKI infrastructure? Does your company have adequate staffing and skills to support PKI?
- How many servers, databases, and HSMs are required to run your organization's PKI? What will be needed to support future growth?
- How much time is required to spin up a CA? How much time do application owners spend to obtain and install certificates? (i.e., requests, renewals, provisioning, etc.) Is it possible to automate these processes?

Security

Ability to protect critical infrastructure and enforce security controls:

- Have you implemented adequate security controls to harden and protect critical PKI components? How, are CA private keys generated and protected?
- What is the process to patch and update servers across your organization's PKI footprint? How do you prevent CA configuration drift and privilege escalation?
- Can your organization discover and quickly resolve PKI-related incidents, such as certificate outages or unexpected audit findings?
- Does your team maintain a comprehensive audit log of PKI-related activities?

Policy & Governance

Ability to establish trust and govern your organization's PKI:

- Does your organization continuously monitor critical PKI components' health and security posture to ensure uptime and policy compliance?
- Does your organization have an accurate inventory of certificates? (e.g., certificate owners, locations, expiration dates, and other details)
- Have you documented certificate policies and practices in a formal CP/CPS? How do you enforce adherence to policies?
- How do you prevent shadow IT? Is there a process to identify and approve the use of other PKI solutions and CA services?

Agility

Ability to deliver with agility and support all use cases:

- Can you supply new use cases with the required PKI capabilities quickly? (e.g., deploy a new CA, support a new integration, etc.)
- Can application owners self-serve certificate requests and renewals? Is it possible to delegate certificate management to specific groups or individuals?
- Does the PKI support various interfaces and protocols? (e.g., REST API, ACME, SCEP, CMP, etc.) Or just auto-enrollment?
- Does your organization use multiple PKI solutions or CA services? How do you maintain centralized control and governance?
- Is your organization prepared to migrate to new CAs, algorithms, and standards? For example, are you able to re-issue or rotate certificates at scale?

Strategy

Ability to plan and deliver PKI capabilities to support business strategy:

- Is your organization's PKI strategy aligned and unified across all business units?
- Who owns the CA infrastructure vs. individual certificates? How do you uncover and support new business initiatives that require certificates?
- Do you have a clear, comprehensive vision of how to evolve PKI services to meet emerging needs? (e.g., IoT, DevOps, cloud-native applications, etc.)
- Is PKI adequately funded and supported by leadership?
- Can you measure the return on investment (ROI) of PKI services?

PKI Maturity Model by PKI Consortium

PKI Consortium

PKI Maturity Model ↗

Assessment Tools ↗

Discussions ↗

Charter ↗

The PKI Consortium established the PKI Maturity Model Working Group to build a PKI maturity model for evaluation, planning, and comparison between different PKI implementations. Keyfactor is an active member of the PKI Consortium and an active member of the PKI Maturity Model Working Group.

Maturity models measure the capability and ability of an organization or implementation for the continuous improvement and evolution in a specific area. The PKI Consortium PKI Maturity Model (PKIMM) focuses on the specifics of a Public Key Infrastructure (PKI) implementation and helps identify the maturity and improvements that can be made.

While the Keyfactor PKI Maturity Model serves as a beginner's guide, the PKI Consortium PKIMM is a technologically independent model that evaluates in depth the various aspects related to the PKI (people, process, technology) according to specific categories. The overall maturity level of a PKI is determined based on the maturity of the categories and is independent of the size of the organization and the use case.

The PKI Consortium PKIMM does not target a specific PKI, rather it serves as an industry-wide standard for PKI maturity assessments and helps to identify areas for improvement, unrelated to the scope, and whether the PKI is private, public, shared, bridged, etc.

The PKI maturity model provides the following:

- Quickly understand the current level of capabilities and performance of the PKI
- Support comparison of PKI maturity with similar organizations based on size or industry
- Action plans on how to improve the capabilities of the current PKI
- Improve overall PKI performance

The ultimate benefit of PKI maturity:

Digital Trust

Our world is more digitally connected than ever. Devices, workloads, and digital transactions are foundational to business as IT architectures continue to expand and evolve with digital transformation. In this hyper-connected environment, digital trust is essential. Digital trust enables organizations to confidently and securely engage with customers, employees, and the outside world.

PKI is foundational to making this happen. In a world without perimeters, every device, every workload, every human, and every connected thing must be verified with a trusted identity. PKI delivers the authentication, encryption, and integrity required to verify machines and humans at scale. A robust and scalable PKI makes it possible for organizations to build trust and, consequently, build and grow their business.

Learn more

You've already taken the first step if you've read this guide. Here we've provided additional resources and solutions to help you reach PKI maturity.

Certificate Management Maturity Model

by Keyfactor

Assess your maturity in certificate lifecycle management, a critical component in PKI maturity.

Download now ↗

PKI Maturity Model

by PKI Consortium

Go a level deeper and thoroughly assess your PKI maturity with the PKI Consortium's PKI Maturity Model (PKIMM).*

Learn more ↗

*Keyfactor is a sponsor of the PKI Consortium and an active participant in the PKI Maturity Model Working Group. We recommend using the Keyfactor PKIMM as a starting point for technical and non-technical stakeholders. The PKI Consortium PKIMM is the next step to thoroughly assess and measure PKI maturity against industry standards.

Explore solutions

See how to modernize your PKI and move up the maturity model with flexible, scalable, and agile solutions.

PKI your way

Simplify and scale PKI with the only platform that deploys fast, runs anywhere you need it, and scales on demand without limits.

Learn more ↗

PKI as a service

Offload the cost and complexity of PKI with a fully-managed, cloud-hosted PKI service operated by experts.

Learn more ↗

Certificate lifecycle automation

Gain complete visibility of all certificates, centralize control, and enable automation to reduce downtime and risk.

Learn more ↗

IoT identity management

Centrally manage and automate the lifecycle of identities across your fleet of connected IoT products and devices.

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946
  (North America)
- +46 8 735 61 01
  (Europe)