KEYFACTOR

EBOOK

Why it's time to re-think your PKI

Migrating to the cloud? Here are 5 reasons to modernize your PKI

Table of contents

Introduction

Whether you're securing IT infrastructure, the software supply chain, or embedding identities into connected products, organizations turn to public key infrastructure (PKI) as a proven technology to establish digital trust. However, legacy PKI deployments often leave teams straining to cope with costly infrastructure, certificate sprawl and outages, and piecemeal hardware and software solutions that create more complexity.

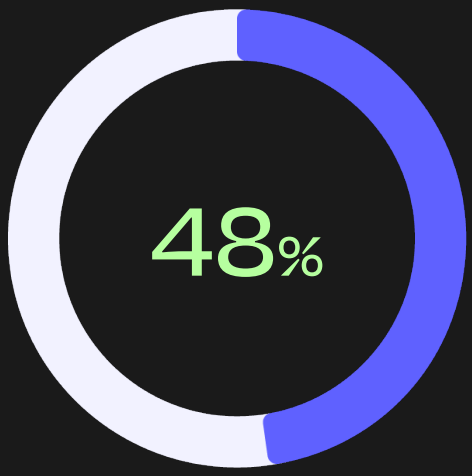
To meet the demands of hybrid and multi-cloud and fast-paced application development teams, organizations have been forced to re-think their PKI and certificate management strategy.

Traditional PKI vs modern IT

Microsoft CA, also known as Active Directory Certificate Services (ADCS), may have been an easy choice for traditional IT environments, but the path to the cloud and the remote workforce introduces several new challenges.

For starters, legacy PKI environments just weren't designed for the high volume and velocity of certificate issuance today. They also typically lack integrations with modern tooling and, due to error and oversight, can be easily misconfigured at any time throughout their long lifespan. Not to mention that many teams just don't have enough expertise or resources on staff to dedicate to their PKI deployment.

For these reasons and more, many organizations have recognized the need to modernize their PKI or move it to the cloud entirely. PKI as a Service (PKIaaS) or SaaS PKI solutions offer all the benefits of a state-of-the-art PKI, without the burden of running and maintaining it in house. Regardless of how or where you deploy it, the importance of getting PKI right cannot be overstated.



of organizations say cloud based services are driving the deployment of PKI, keys, certificates, and other secrets.

2023 State of Machine Identity Management

The Changing Role of PKI

Over the last two decades, the world of PKI has changed dramatically, from being a fringe technology to becoming a ubiquitous piece of infrastructure used by virtually every team in the IT organization today.

While PKI was initially adopted to secure the Internet, it's use has since exploded, now used to secure everything from internal networks and applications to edge devices and smart manufacturing. It's essentially become the foundation of digital trust in an era where trust cannot be assumed, it must be built.

Web Servers

SSL/TLS certificates on external facing web and applications to enable trust.

Internet of Things (IoT)

Mutual authentication, encryption and integrity controls for connected devices.

Multi-Coud

Ephemeral certificates to authenticate containers, microservices, and workloads.

Network Devices

Authentication between routers, firewalls, load balancers, and SSL inspectors.

Secure Email

Digitally sign and encrypt emails across corporate and BYOD devices.

DevOps

Signing containers and software builds, and securing ephemeral workloads.

MFA / SSO

Multi-factor authentication for single sign-on applications such as Windows Hello or Office 365.

WiFi Access

Authentication to Wi-Fi connections to ensure that only trusted users are accessing the network.

VPN Access

Replacing expensive VPN authentication solutions with password-free certificated-based authentication.

Mobile Devices

Trusted access for mobile apps, mobile browsers, Wi-Fi authentication, S/MIME email encryption, and more.

Getting it right: Key Considerations

Designing, deploying, and maintaining the necessary systems to support a modern enterprise PKI can be a complex undertaking without the right approach. That's why it is critically important to evaluate whether your organization has the right solution, expertise, and infrastructure to run a PKI that can support your business as it grows.

Use cases

The number of tools and applications dependent on PKI for identity and authentication has increased dramatically. Certificates are now used for everything from signing software to authentication in microservices deployments. Identifying the different certificate types, templates, protocols, and automation capabilities needed to support these different use cases is critical to a successful deployment.

Expertise

A rare few companies have an in-house expert (or team) dedicated to PKI, but for most, it's more of a "hot potato" that gets passed to any admin willing to take it on. It's important to consider if you have the right expertise and bandwidth on your team to set up and run a robust PKI over its entire 15-20+ year lifespan. If not, you may want to consider a hosted or managed PKI service.

Cloud migration

Every PKI deployment is different. Some organizations are further along in their cloud journey, others are still figuring out what should stay behind their firewall. The good news is that the technology behind PKI has advanced dramatically, and there are far more deployment options today than ever before, including PKI as a Service (PKIaaS).

Scalability and availability

Another key consideration is the expected service level agreements (SLA) for uptime and availability, especially as you scale up with new use cases. High availability (HA), backup and disaster recovery (BU/DR), and the ability to manage certificates issued from your PKI at scale are all important factors for supporting environments with thousands or even millions of certificates.

Security and assurance levels

PKI is more than just CA software and certificates. You'll also need to consider the required safeguards and policies around your PKI infrastructure to meet expected assurance levels and protect the private keys behind your root of trust. Certain industry regulations or internal security policies may dictate specific parameters required for your PKI deployment as well.

Business Challenges

It's clear that PKI is an essential building block to digital trust and security, but there are a number of challenges that can stand in the way of success.

No clear ownership

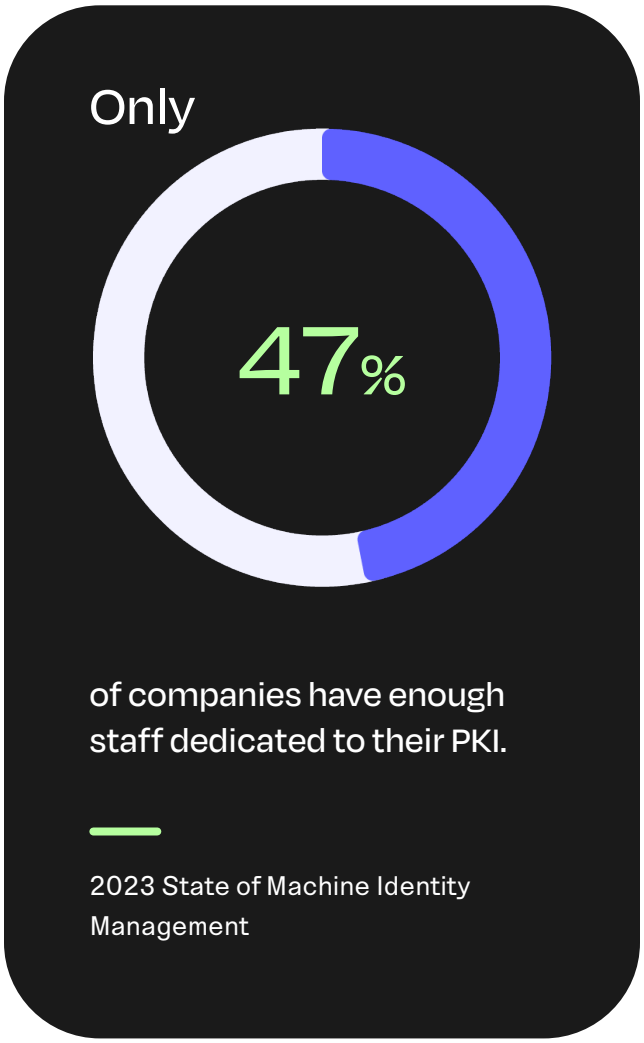
PKI has always been a bit of a technical "hot potato." It's passed between different teams or individuals without any clear ownership, and when an incident such as a certificate outage occurs, it's difficult to respond effectively.

Lack of expertise

PKI just isn't a core skillset of many IT and security teams. Expertise can be difficult to find and retain, so unless you have the skillset and full-time equivalent (FTE) hours available on staff, then you may need to augment your team with a trusted partner.

Disparate tools and processes

Security teams too often rely on an inefficient patchwork of internal PKIs and certificate authorities (CAs), monitoring tools, and management interfaces that fail to provide consistent visibility and control.



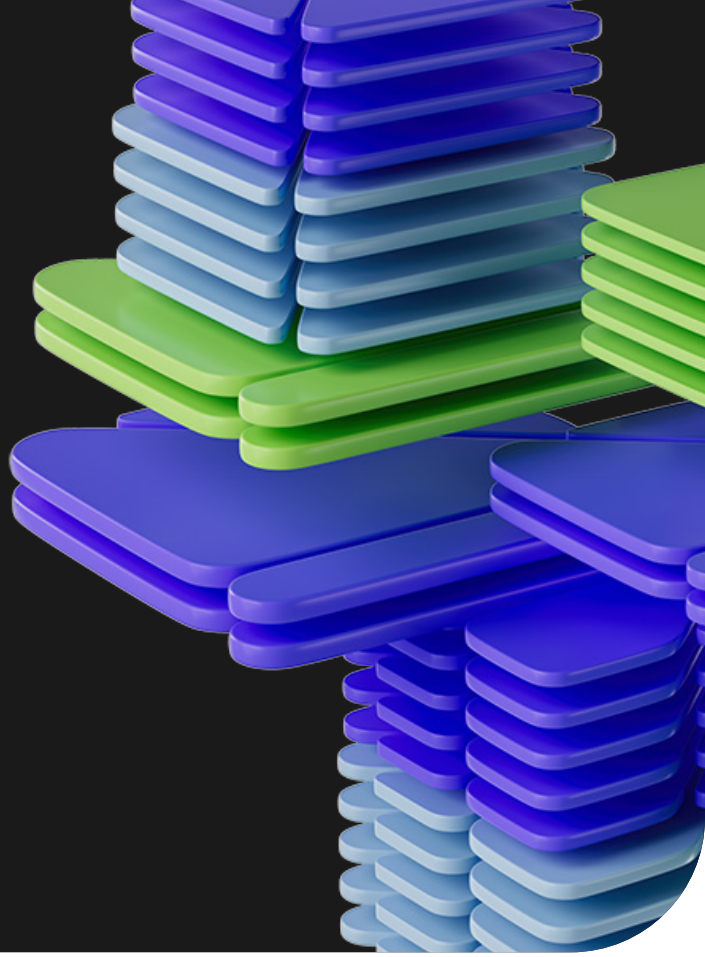
Outdated CA infrastructure

PKI deployments initially built for one or two applications are now stretched to cover more users and devices than ever before. Legacy PKI systems not originally designed for things like cloud computing and IoT devices can become an operational roadblock.

Shadow PKI

Different teams often deploy their own certificate authorities (CAs) for specific use cases without consideration for corporate IT policies. CAs can be misconfigured, and certificates left untracked, which leads to unexpected audit findings and outages.

5 reasons to modernize your PKI



So, why is it time to re-think your PKI?

Here are the top reasons why organizations are migrating from legacy PKI systems to a modern PKI solution.

01

Deploy your way

When it comes to PKI, one size does not fit all. How and where you deploy your PKI is a critical decision, so flexibility is important. For instance, a cloud-based solution, such as Keyfactor EJBCA SaaS or PKI as a Service, offers cloud-native scalability and ease of deployment. On the other hand, an on-premises solution, such as EJBCA hardware or software appliance, may make more sense if you have available resources or strict regulatory requirements to deploy and manage PKI internally.

In either case, legacy PKI deployments typically can't live up to the need for flexibility in hybrid and multi-cloud operations. To account for the unique challenges of your organization, including security, budget, and availability of resources, your team needs deployment options that suit their needs today and allow them to grow flexibly over time, including scenarios like PKI migration, M&A activity, and hybrid PKI.

02

Meet any use case

Just as you need the flexibility to deploy anywhere, you should also be able to integrate easily with your existing tools and applications. Auto-enrolment works well for Microsoft infrastructure, but today's IT landscapes are much more complex, involving multiple operating systems, services, and cloud platforms.

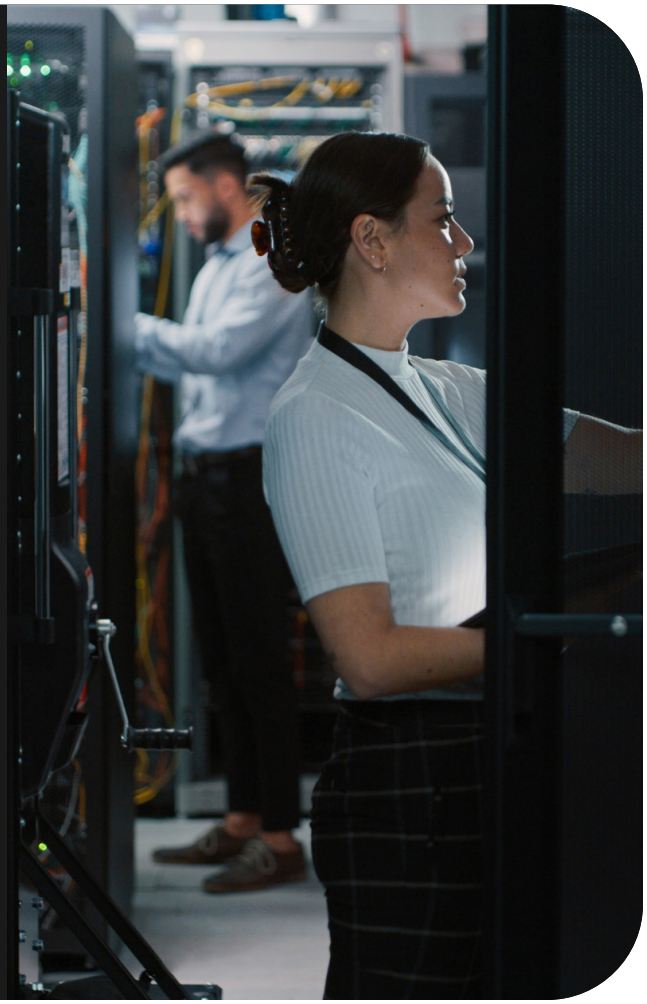
Developers expect certificates to be easily consumable via API. Manufacturers need to embed certificates into products right on the manufacturing floor.

To meet a variety of use cases, PKI must be adaptable and extensible. Modern PKI solutions support thousands of certificate operations per second, and provide built-in support for protocols like SCEP, ACME, EST and CMP, as well as a robust underlying REST API. This level of flexibility is invaluable when you're dealing with different devices, operating systems, and geographies.

What about Microsoft CA?

So, you're looking for a new modern PKI solution to support new use cases like cloud migration and DevOps, but you still have traditional use cases already supported by Microsoft CA. Should you migrate? Or should you keep your existing PKI?

The simple answer is, both are possible. Finding the right PKI solution will allow you to support modern use cases alongside Microsoft-native tools like Auto-enrollment, Intune, and Azure Key Vault. It will also allow you to run in tandem with Microsoft CA or migrate over time to your new PKI with minimal disruption.



03

Scale without limits

Because your PKI supports mission-critical applications, scalability and performance are a top-level concern. The challenge with many legacy PKI deployments, such as Microsoft CA, is that you can only install one CA per server. Without built-in support for multi-tenancy and high availability (HA), your PKI footprint can get very complex, very quickly. Not to mention the growing cost of maintenance.

Whether you opt for fully managed, turnkey SaaS, or on-premises deployment, modern PKI solutions make it easier to deploy fast and scale without limitations like per-certificate fees or additional CA servers. At a technical level, any of the PKI components, such as certificate authorities (CAs), registration authorities (RAs), and validation authorities (VAs) can be spun up much faster to keep up with demand.

Adopting a SaaS-delivered or fully managed PKI can save significant time and resources as you scale, with built-in SLAs to guarantee uptime and 24/7 monitoring to ensure your PKI stays healthy and operational.

Why PKI as a Service?

Installing and maintaining a full-blown PKI requires resources and expertise. Any CA software relies on a robust technology stack, with the need for constant monitoring, maintenance, and updates.

By opting for SaaS-delivered or fully managed PKI, you reduce your internal need to manage yet another critical infrastructure component. A trusted partner ensures that your PKI is managed according to best practices and with the highest assurance, while your teams can focus on core business objectives.

04

Simplify and consolidate PKI

A typical enterprise PKI grows over time, with shifts in business needs and added use cases. Only planning for the short-term or specialized use cases often results in a bloated PKI environment with inconsistent security policies and growing costs. Moreover, older PKI systems have limitations in functionality that make them unfit to support current needs and regulatory requirements.

As demands for digital certificates increase, many security leaders are looking to simplify and consolidate their CA infrastructure and enforce better governance and control. A flexible and future-proof CA solution allows you to cover all of your PKI use cases with one platform. Instead of relying on a disparate set of CA and crypto tools, organizations can begin to consolidate their PKI use cases into a centralized platform, lower total cost of ownership, and establish a Crypto Center of Excellence (CCoE).

05

Enable automation and agility

Beyond the nuts and bolts of your PKI infrastructure, you need visibility and control over the certificates issued into your environment, both from public and private CAs. Many teams rely on inefficient spreadsheets, calendar reminders, and homegrown scripts to keep track, but shorter lifecycles and larger volumes of certificates make it near-impossible to keep up.

Choosing the right PKI solution can enable you to not just issue, but also manage and automate the lifecycle of keys and certificates. By combining highly scalable PKI with certificate lifecycle automation, organizations can address both challenges with one solution. More importantly, it gives you the flexibility to manage and automate the renewal and provisioning of certificates across all CAs in your environment, which could include other cloud-native or publicly trusted CA vendors.

Why CA agility is key

It's important to simplify and consolidate vendors where possible, but the reality is that different trust requirements and environments may drive the need for the use of multiple PKIs and CAs.

Getting visibility over your entire certificate landscape, including public, private, and cloud-based issuers, is critical to prevent outages and security risks that result from using multiple interfaces and tools to manage certificates. It also means you can remain crypto-agile and easily add or switch CA vendors as needs change and as crypto-standards inevitably evolve over time.

PKI powered by Keyfactor

At Keyfactor, we believe that teams should have the flexibility to deploy PKI how and where they need it — in the cloud or on-prem, fully managed or self-hosted. This approach helps organizations to simplify their PKI and enable digital trust across their connected landscape, whatever it looks like today and however it evolves in the future.

Better yet, we combine our PKI solutions with end-to-end lifecycle automation for keys and certificates in enterprise IT, DevOps, and even IoT and IIoT manufacturing environments. It's one platform for PKI and machine identity automation.

Why Keyfactor

Deep PKI expertise

PKI is more than just software. We have more than 20+ years of expertise in PKI engineering, architecture, and design.

Flexibility

You have the flexibility to run PKI how and where you need to, whether it's in the cloud, as a hybrid architecture, or on-premises.

Simplicity

Security only works when it's adopted. Our solutions are focused on simplifying PKI and certificates for PKI experts and everyday users.

One platform

Our customers benefit from a single platform for PKI and certificate lifecycle automation. Less complexity, more agility.

Scalability

Our solutions have been tested and proven to perform effortlessly in environments with millions, even billions, of certificates.

Trusted & compliant

Keyfactor works tirelessly to comply with industry security standards like ISO 27001, ISO 9001, Common Criteria, SOC 2 Type II, and more.

Deploy your PKI, your way

MANAGED

PKI as a Service

Available as a service

24/7 managed zero-touch PKI with an offline, air-gapped root.

SAAS

EJBCA SaaS

Available in AWS

Turnkey SaaS PKI deployed and managed by Keyfactor.

CLOUD

EJBCA Cloud

Available in AWS & Azure

Self-managed PKI deployed in your cloud environment.

SOFTWARE

EJBCA Software

Available as a virtual appliance

Deploy within your own datacenter and integrate with your HSM provider.

HARDWARE

EJBCA Hardware

Available in turnkey hardware

Deploy turnkey PKI with a full hardware and software stack and HSM.

Manage every machine identity

ENTERPRISE SECURITY

Keyfactor Command

Available on-prem, hybrid or SaaS

Prevent outages and enable crypto-agility with complete visibility, control and automation for keys and certificates.

PRODUCT SECURITY

Keyfactor Command for IoT

Available on-prem, hybrid or SaaS

Secure IoT products by design with end-to-end identity management for devices and manufacturing supply chains.

Ready to re-think your PKI?

There comes a time when every organization outgrows their legacy PKI deployment, whether it's prompted by cloud migration, CA expiration, or the need to support new use cases. Whether you're there today or you're planning for the future, we're ready when you are to start the conversation.

GET IN TOUCH

Get started on your journey to modernize PKI, request a demo from a Keyfactor expert.

Request a demo ↗

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