EBOOK

Building the Business Case for a Cloud-First PKI Strategy

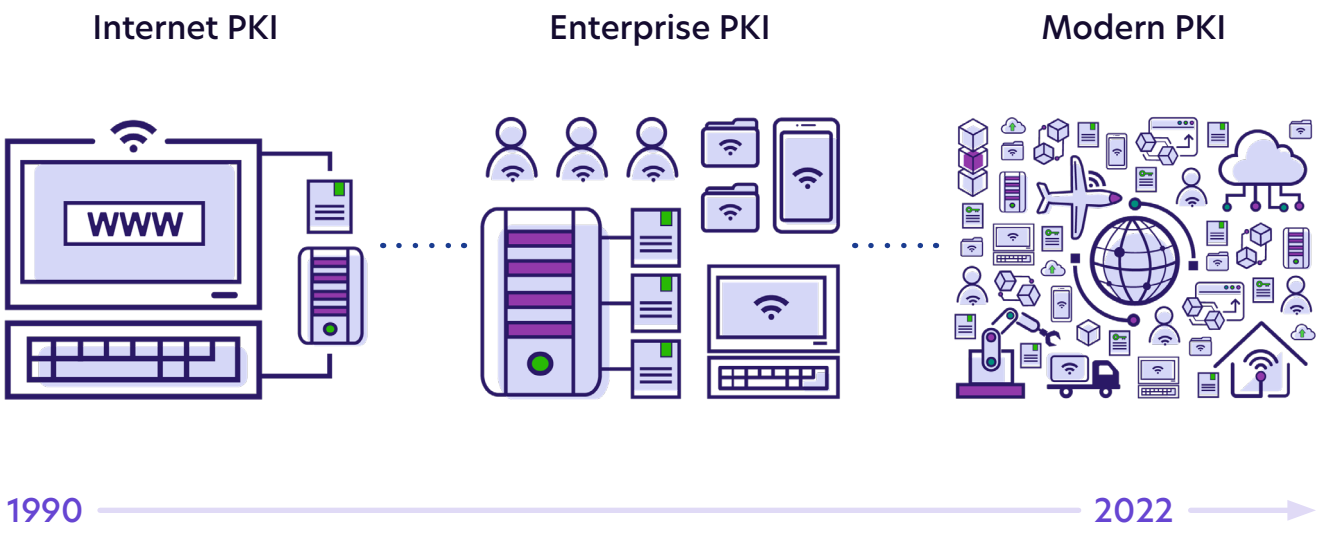
KEYFACTOR

Table of Contents

Introduction

The shift to hybrid and multi-cloud is inevitable. Today, applications need to run anywhere and scale quickly. Whether your organization has a cloud-first strategy or you're migrating legacy applications to the cloud, the advantages are well known. In this new cloud model, PKI and security teams have the opportunity to accelerate their own initiatives and embrace the benefits of cloud infrastructure.

As an essential building block for security, public key infrastructure (PKI) is critically important. Over time, the use of PKI and X.509 certificates has become synonymous with the shift from network-defined trust boundaries to a focus on identity. Overall, we've witnesses three distinct eras of PKI.



Internet PKI

The first asymmetric algorithm (RSA) was introduced in 1977, but it wasn't until the Internet went mainstream that PKI really took off. In the 1990s, publicly trusted certificate authorities (CAs) were introduced to build widespread trust on the internet. PKI enabled organizations to purchase and provision TLS certificates, primarily for their public-facing websites and applications. This era of PKI was defined by a limited number of publicly trusted certificate authorities (CAs) and long-lived certificates.

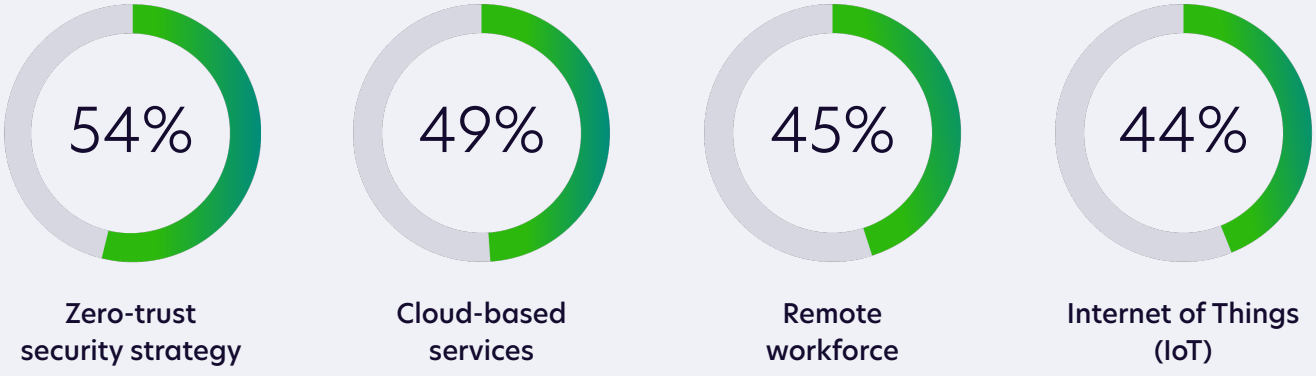
Enterprise PKI

In the years following the introduction of PKI, many organizations realized the need for internal trust. IT and security teams identified practical ways that PKI could be deployed and used internally to protect internal communications, authenticate users and devices, and digitally sign documents and code. This era of PKI was defined by widespread use of legacy PKI tools like Microsoft ADCS to issue larger volumes of certificates for users, devices, and network equipment.

Modern PKI

Today, organizations are taking full advantage of PKI to build trust within their distributed and connected environments. Everyone from security architects, network engineers, infrastructure and DevOps teams, now rely on PKI and digital certificates. PKI and CAs are deployed across the organization to support specialized use cases, making it much more difficult to manage and govern. At the same time, shorter lifespans and higher volumes are certificates introduce new management challenges.

The most important trends driving deployment of PKI, keys, and certificates



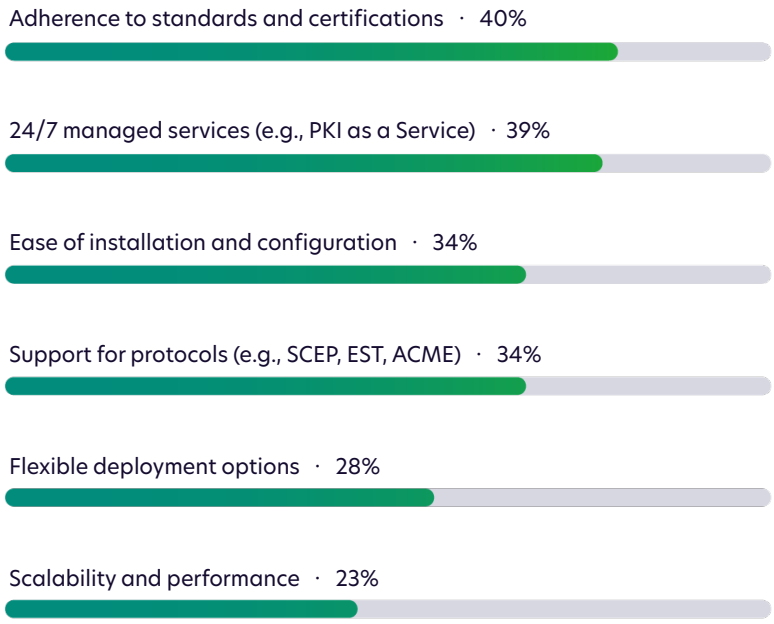
PKI and migrating to the cloud

Cloud migration, new use cases, and a general lack of expertise in PKI has forced many teams to re-consider their strategy. As the technology behind PKI and certificate management advances, new cloud-based deployment models introduce opportunities to get all the benefits of modern PKI, without the complex footprint, security controls, and workloads required to run it internally.

Barriers to adoption of SaaS-delivered PKI are also quickly fading, as vendors introduce robust capabilities and demonstrate compliance with even the most stringent regulatory standards. Today, more organizations have realized they can achieve higher service levels (SLAs) and compliance with required security mandates than they could feasibly accomplish in house.

The most important features when selecting PKI solutions

2022 State of Machine Identity Management



PKI is increasingly complex

It's clear that PKI is critical infrastructure, but many organizations don't have the available resources, expertise, or time in the day to manage it. As the number of use cases and integrations supported by PKI grows, the cost and complexity of PKI deployments can be difficult to sustain.

Increasing complexity leads to service outages and mistakes that put the organization at risk, such as unprotected private keys or CA misconfiguration. To avoid common mistakes and unnecessary burden on teams, the idea of SaaS-delivered PKI has become much more appealing.

That said, there are many ways to migrate PKI to the cloud, and several important factors to consider for your PKI program, including:

Personnel

PKI requires the right skillset to implement several important components, including a root key signing ceremony, creating a CP/CPS, safeguarding the root of trust, configuring the issuing CAs and revocation infrastructure, and maintaining certificate templates and policies.

Infrastructure

Remember, PKI is more than just CA software and certificates — it is a comprehensive set of server infrastructure, databases, HSMs, backup and disaster recovery, and certificate policies that require constant diligence. It's important to consider if your datacenter can support these requirements in a cost-effective and efficient way.

Security

As the root of trust for your organization, PKI necessitates strong security controls. Achieving appropriately high levels of security and assurance with existing on-premise infrastructure can be challenging and expensive — especially if you're not prepared for everything it entails.

Evaluating the costs of on-premise PKI

Beyond the potential complexities of running PKI internally, hosting the PKI within your datacenter can introduce several costs, both expected and potentially unexpected, including implementation, labor and infrastructure, and downtime.

Initial deployment

Whether you're re-building your PKI or you're starting from scratch, deployment costs can quickly exceed expectations.

It may seem simple to install a Microsoft CA with default configurations, but the reality is that PKI requires much more care and feeding when done properly.

Potential effort and expenses:

- PKI architecture and use case planning
- Initial configuration of CA software
- Creating certificate policy and certificate practice statement (CP/CPS) documents
- Running a root key signing ceremony
- PKI consultant services for implementation

Labor and ongoing support

PKI expertise is hard to find and even harder to retain. Even if you do have expertise on staff, shifting priorities make it difficult to give your PKI the attention it needs.

Not to mention that certificate users aren't experts, they require continuous support to request, renew, and properly provision certificates for their own applications.

Potential effort and expenses:

- Recruiting and training skilled PKI staff
- Maintaining CRL and OCSP availability
- Issuing and root CA uptime and renewals
- Server maintenance, backup and disaster recovery tests, and resiliency
- Internal training and ongoing support for certificate users
- Certificate-related outage downtime and remediation

Hardware and software

When it comes to infrastructure, various components are required to support a PKI deployment, including HSMs, servers, databases, and virtualization platforms on which you run your PKI.

For instance, running your PKI on virtualized infrastructure with proper backup and recovery incurs costly security considerations.

Potential effort and expenses:

- Offline, air-gapped root CA server
- HSMs and lockable storage
- Hardware or cloud infrastructure to host multiple CA servers
- Software licensing for servers, databases, security and monitoring software
- Vendor support contracts from several hardware and software providers

Potential effort and expenses:

- High security datacenter facilities
- Biometric and physical security controls
- Security personnel and surveillance
- High-grade and/or fire-proof safe for root key material
- Tamper-evident containers and seals
- Environmental considerations, including backup power and cooling

Security controls

Depending on the assurance levels required by corporate IT policies or external regulatory mandates, costs related to the security of your PKI infrastructure can quickly inflate beyond initial expectations.

These controls are necessary to ensure the root of trust behind your organization is protected against compromise or misconfiguration.

BUSINESS CASE:

EQ Bank

Equitable Bank

As one of the largest banks in Canada, Equitable Bank realized that their current PKI implementation couldn't support their migration to Azure. VP of Security Infrastructure, David Yu, and his team quickly built the business case for a cloud-based PKI solution.

Core challenges:

- ✕ Legacy Active Directory Certificate Services (AD CS) could not support new cloud and DevOps requirements
- ✕ Use of self-signed certificates in development environments did not meet security requirements
- ✕ Developers ran into roadblocks with certificates due to manual processes and legacy PKI
- ✕ Poor visibility led to unexpected outages caused by expired and misconfigured certificates
- ✕ Expense of running PKI infrastructure in accordance with high security standards was not feasible in house
- ✕ Internal team did not have enough time or resources to dedicated to their PKI deployment

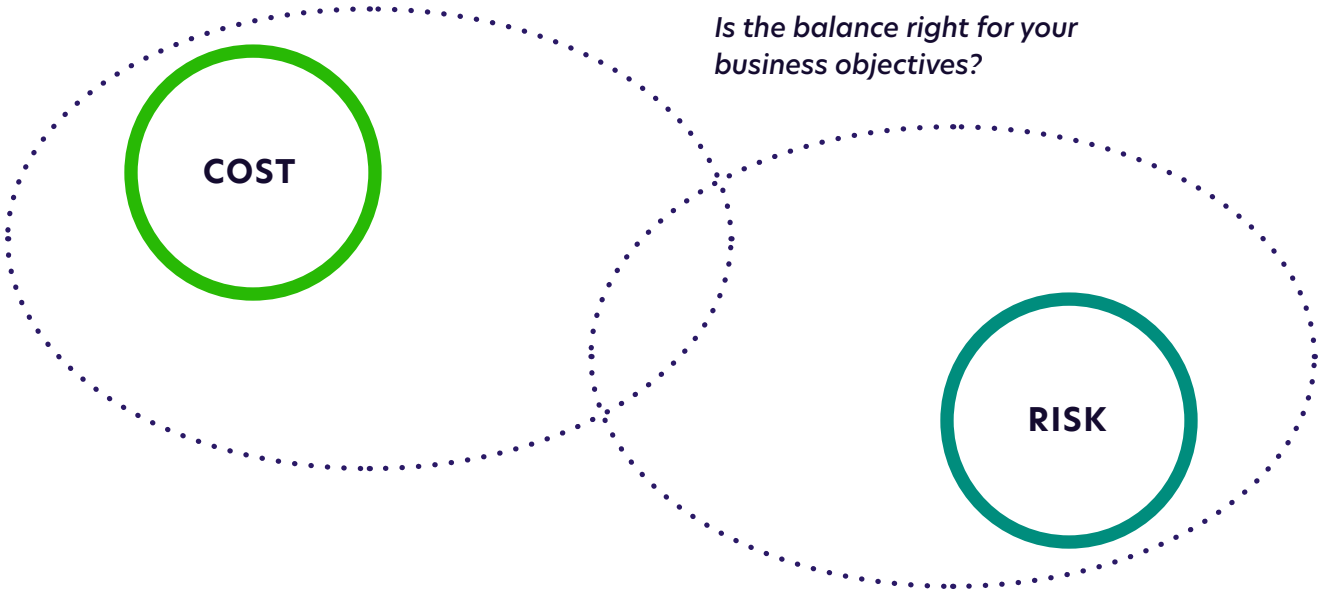
By shifting to PKI as a Service, EQ Bank was able to secure their core banking platform hosted in Azure with a robust PKI, reduced the cost and risk of running PKI internally, and enabled their DevOps teams to move faster with security.

Key results:

- ✓ Migrated from legacy AD CS to robust cloud-based PKI infrastructure in a matter of weeks
- ✓ Reduced manual PKI and certificate-related workload by 2 full time equivalents (FTE)
- ✓ Eliminated certificate-related outages entirely and supported DevOps via APIs and automation

Evaluating risk vs cost for PKI

When considering the costs of PKI implementation, organizations typically aim to lower or minimize costs and increase security. However, achieving security and cost-efficiency simultaneously creates a conundrum, and often results in tradeoffs to meet project timelines or limited budgets.



The risks of reducing costs

Hosting PKI can be expensive, so teams often look for ways to reduce costs. Unfortunately, this typically leads to shortcuts on key security controls and processes.

The costs of reducing risk

Meanwhile, because the security of PKI is critical, teams also want to eliminate risk vectors, which inevitably increases costs of PKI implementation.

As a result of this situation, achieving the right balance of security and cost-efficiency is very difficult to find, particularly when teams rely on legacy on-premise PKI infrastructure and lack the expertise to implement it properly.

Benefits of migrating PKI to the cloud

SaaS-based PKI solutions aim to solve the challenge of balancing risk with cost, allowing organizations to strike a balance and take advantage of economies of scale. Organizations can also deploy much faster, meet security requirements, and simultaneously support both cloud-native and traditional on-premise use cases.

High scalability

Enables teams to spin up new CAs and/or issue certificates instantaneously with just a few clicks

Improved security

PKI runs in highly secure, state of the art facilities and operated by compliant and audited vendors

Faster deployment

Turnkey SaaS PKI offerings reduce deployment time down from months to just days or even hours

Frees up IT

Reduces the burden on internal teams and eliminates repetitive, low-value PKI maintenance tasks

Reduced cost

Eliminates the need to provision servers, databases, HSMs, and other supporting software and hardware

Ease of integration

Many SaaS-based PKI solutions offer flexible integrations and automation out of the box

Paths to PKI in the cloud

There are many reasons to upgrade your PKI — whether it's cloud migration, root or issuing CA expiration, or the need to support more use cases. However, there is no one path to the cloud. When it comes to PKI, you have options.

Hybrid PKI

One option is to build and run your PKI internally and integrate it with your cloud-based services and applications in a hybrid architecture. Unlike older Microsoft-based PKI deployments, modern PKI solutions like EJBCA support hardware or software-based PKI that can run within your datacenter or cloud environment, but with the extensibility and scalability required to support modern hybrid and multi-cloud environments.

Turnkey SaaS PKI

Another option is to leverage a SaaS-delivered PKI, such as EJBCA SaaS, which enables organizations to offload the effort and expense of running the backend infrastructure required to support PKI. However, teams still have the flexibility to spin up and configure CAs and templates to meet their use cases and requirements. It's a balance between keeping control, but reducing some of the effort involved in PKI management.

Managed PKI

Organizations looking for a more "hands off" approach to PKI can opt for a fully managed, cloud-hosted PKI service. Often referred to as PKI as a Service, these solutions provide a zero-touch approach, with end-ot-end PKI deployment, monitoring, and management handled by a team of trained experts. These solutions also often offer an air-gapped, offline root CA protected by multiple biometric and physical security safeguards.

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.

✓ One platform

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

✓ Simplicity

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

✓ 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.

✓ 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.

Ready to migrate your PKI?

Your already to know that PKI is critical to security, but setting up the infrastructure and spending the required resources to build and operate it properly is no easy task.

With security teams under increasing pressure, a cloud-first PKI strategy can help them to simplify and scale certificate issuance on-demand as their use cases grow.

GET IN TOUCH

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

REQUEST A DEMO

CUSTOMER STORY

See how EQ Bank reduced their PKI footprint and eliminated outages with Keyfactor

READ CASE STUDY

KEYFACTOR

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale.

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