WHITLOCK IS

EBOOK

Why It's Time to Re-think Your PKI

5 reasons to move your PKI deployment to the cloud

KEYFACTOR

Table of Contents

Introduction

Whether it is securing a network, sensitive data, or connected devices, IT leaders turn to PKI as the proven technology to establish trust in their environment. With vast coverage that spans across the enterprise, PKI is a complex undertaking, requiring highly secure facilities, trained personnel, and the right hardware and software to run it effectively and keep it under control.

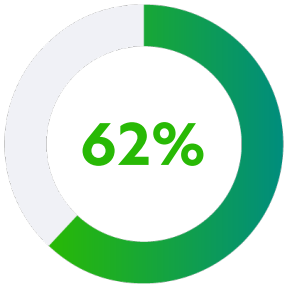
To achieve this goal with limited IT and security resources, more and more organizations are moving their PKI to the cloud. Agility and security of cloud infrastructure has enabled highly secure cloud-based PKI deployments — known as PKI as-a-service (PKIaaS) — hosted and managed by a trusted partner.

Moving PKI to the Cloud

Not long ago, IT leaders were reluctant to put any data or applications in the cloud. Now most have realized that cloud service providers like AWS, Microsoft Azure, and Google Cloud invest far more in the people and processes required to deliver reliable and secure infrastructure.

State-of-the-art data centers are built to the highest standards in security, with everything from physical access controls to multi-layered encryption. Moving to the public cloud has allowed teams to focus more attention on protecting sensitive data and mission-critical workloads, and to worry less about keeping the underlying infrastructure running and secure.

Organizations have similarly recognized that moving their PKI to the cloud — managed by industry experts with the right knowledge of standards and best practices — can help them achieve much higher levels of security and operational efficiency than is feasible in-house. As businesses become more reliant than ever on PKI for encryption, authentication and digital signatures, the importance of getting it right cannot be overstated.



of organizations have or plan to migrate their PKI deployment to the cloud.[1]

[1] 2020 Keyfactor-Ponemon Report

The Changing Role of PKI in your Enterprise

Today, the most prevalent use of PKI and digital certificates is secure web browsing, made possible through SSL/TLS certificates purchased from a number of trusted third-parties known as public certificate authorities (CAs).

Most organizations also deploy their own PKI in-house to issue certificates internally — known as a private CA or private PKI. No longer limited to a few use cases, private PKI is now emerging as a core technology to secure business initiatives like zero-trust, multi-cloud, and DevOps.

Web Servers

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

Multi-Cloud

Ephemeral certificates to authenticate containers, microservices, and workloads.

Network Devices

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

MFA/SSO

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

VPN Access

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

Internet of Things (IoT)

Mutual authentication, encryption and integrity controls for connected devices.

Secure Email

Digitally sign and encrypt emails across corporate and BYOD devices.

Devops

Signing containers and software builds, and securing ephemeral workloads.

Mobile Devices

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

Wi-Fi access

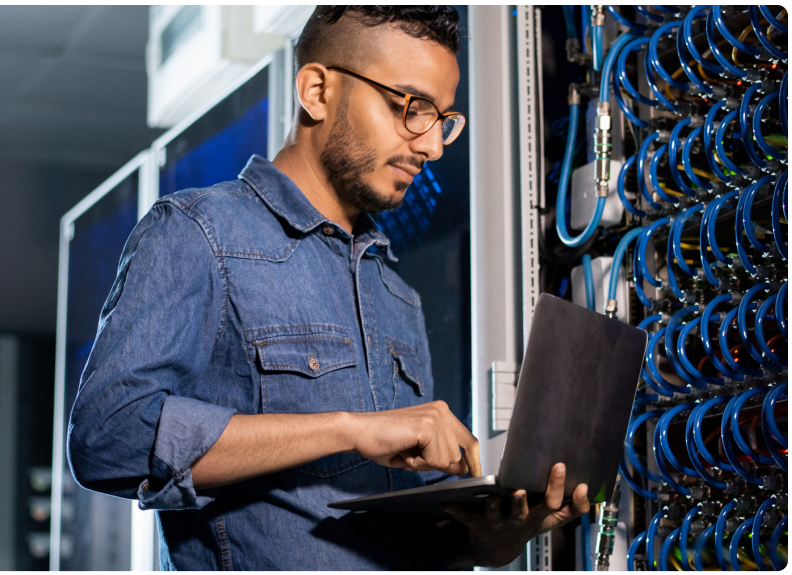
Authentication to Wi-Fi connections to ensure that only trusted users are accessing the network.

PKI supports more than 11 different applications on average.[2]

[2] 2020 Global PKI and IoT Trends Study | nCipher, an Entrust Company

Getting it Right: The Complexity of PKI

Designing, deploying and maintaining the necessary systems to support your own private PKI can be a costly and time-consuming commitment. Even a single expired certificate can render the groundwork of your cybersecurity spend useless. Worse yet, if your underlying PKI is compromised, every certificate in your environment is rendered untrustworthy. Getting it right is critical, but it is not an easy feat.



Expertise

PKI is a multi-faceted system that requires specialized expertise and dedicated IT staff to plan, build and manage throughout its lifecycle. IT personnel or outside consultants will need to design the certificate hierarchy, develop policies and procedures, implement the required software and hardware, create and test a disaster recovery plan, and track certificates throughout their lifecycle.

Significant IT resources must also be committed to support ongoing maintenance of audit logs, certificate validation and revocation, IT training, and end-user support for users that leverage digital certificates across the business.

Infrastructure

A comprehensive set of infrastructure is required to run an in-house PKI effectively. High availability, backup, and disaster recovery must be carefully planned to ensure continuous operation.

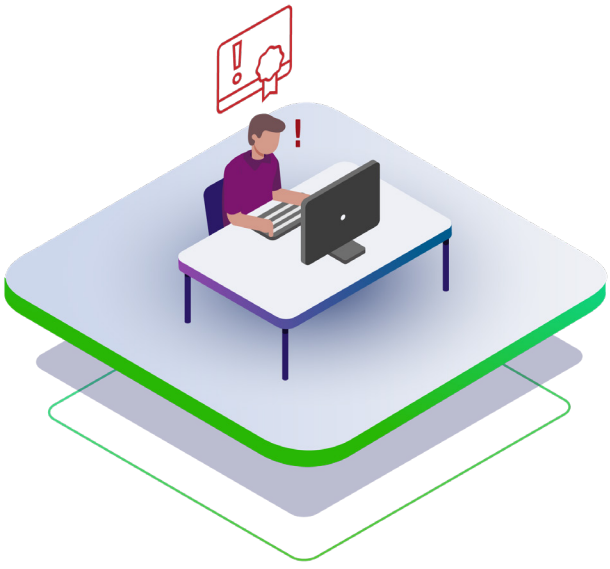
Dedicated infrastructure will need to be procured and provisioned to host the root CA, issuing CAs, revocation endpoints, enrollment processes, private key storage, and so on.

Additionally, FIPS 140-2 validated Hardware Security Modules (HSMs) must be configured to protect to the root, policy, and issuing CAs.

Security

In the interest of saving time or avoiding operational effort, far too many PKIs get deployed with lower-than-desired security controls. But most IT and security teams don't realize the impact if they lose control of their PKI, if it's compromised, or if it's mishandled internally. Because PKI supports business-critical applications, security must come first. Organizations without a highly secure facility, data center, and access controls will need to invest in a higher security level to protect their PKI.

Achieving appropriately high levels of security within your existing IT infrastructure can be challenging and expensive. The root CA is the anchor of trust in your PKI environment. The integrity of your PKI relies entirely on the security of the root CA, and requires highly specialized controls to be maintained effectively. For starters, adequate protection requires on-site security, continuous monitoring, highly trained personnel; secure vault storage, hardware-level protection, multi-person authentication, biometric controls, and of course, a proper root CA signing ceremony.



THINK YOUR PKI IS FREE?

"Free" PKI capabilities included in server operating systems can appear to be a simple, low-cost PKI solution, but the reality is that there is far more infrastructure, security, and process involved.

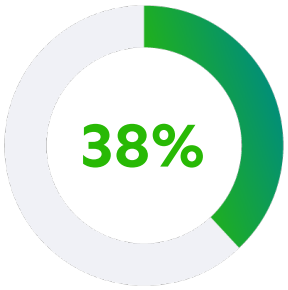
Hidden costs and complexities mean IT and security teams often overlook critical steps, only to find themselves months later with a PKI far less secure and reliable than when they started out.

Business Challenges

It's clear that PKI is taking on a more important role in security, but there's a number of business challenges that stand in the way of success.

PKI Operations Under Stress

Today, PKI deployments initially built for one or two applications are now expected to cover more users and devices than ever before. Demand for encryption and authentication has increased pressure on legacy PKI systems that weren't originally designed for this level of scale or complexity. As a result, integrity of the PKI typically degrades as new use cases are adopted without consideration for the policies and procedures set in place from the start.



of organizations say they have sufficient IT security staff dedicated to PKI deployment.[3]

No Clear Ownership

PKI has always been a bit of a technical "hot potato." The sheer complexity of public key cryptography is enough to keep most IT professionals away. And if it isn't the complexity, it's the risk. The consequences for failure within enterprise PKI is considerable. Taking responsibility for that level of risk leaves few inclined to take on the challenge.

Limited Expertise & Resources

Due to the intricacies of PKI, problems are likely to arise unless you happen to have that knowledge within your organization, and equally important, the depth in personnel to be able to execute it properly. The number of professionals specialized in the art of PKI is waning. Furthermore, it is not always considered a core operation within the enterprise.

Lack of Tools & Processes

Security teams might overemphasize focus on the infrastructure and how to get certificates out initially and underestimate the effort dealing with pending expirations and outage prevention. Without software to handle the lifecycle of certificates, expirations and outages are inevitable, causing serious disruption to business operations. Required audits also become difficult, expensive, and time-consuming.

[3] 2020 Keyfactor-Ponemon Report

In-House vs PKI as-a-Service

When it comes to private PKI, you have two options: either build your own or adopt a cloud-hosted PKIaaS solution. Build-it-yourself PKI isn't impossible — the real question is whether you want to spend the time, effort, and investment to build and maintain it yourself.

In-House PKI

Enterprise designs, builds and deploys their private PKI infrastructure, assuming 100 percent of the risk and cost of implementation.

VS

PKI as-a-Service

PKIaaS provider hosts and manages the backend hardware and software required to run the private PKI and manage certificate lifecycles. You maintain control of the PKI.

Trusting your PKI in the Cloud

Enterprises often limit their PKI deployment to components bundled into their operating system, but this may provide a false sense of simplicity. The real effort and expense of PKI lies in its maintenance. Organizations must also consider how digital transformation will change demands for encryption and authentication in the future.

Previous notions that security and control are better managed in-house are changing. As IT environments compound, enterprises are putting their trust in a reliable PKIaaS partner. With dedicated PKI expertise at their disposal, proactive compliance coverage, and multi-layered security across infrastructure and operations, PKIaaS providers can deliver a much more effective, and ultimately more secure, PKI deployment.

> **"Public-key infrastructure (PKI) and digital certificates are hard to manage. Organizations are also expanding the use of PKI within IoT and DevOps pipelines. Technical professionals need to transform the perception — and the deployment — of PKI to establish an automated management regime for PKI."**

GARTNER, THE RESURGENCE OF PKI IN CERTIFICATE MANAGEMENT, THE IoT AND DEVOPS, PAUL RABINOVICH, ERIK WAHLSTROM, 23 OCTOBER 2018

5 Reasons to Move your PKI to the Cloud

Why should you re-evalutate your PKI deployment? Here are the top reasons why our customers have made the shift to PKI as-a-Service:

Robust Security

There are many considerations when it comes to migrating your PKI to the cloud. All are important, but security is at the top of the list, and it's up there for obvious reasons. If the root key or private keys are compromised, it can result in significant disruption and downtime to PKI-dependent applications.

Since it is their core business, PKIaaS providers can commit far more resources to state-of-the-art PKI infrastructure, security, and expertise than is feasible for most enterprises. Furthermore, their security policies and practices have been tested over time and at scale, providing you with the confidence to know that your PKI is in the right hands. If your enterprise falls under attack, you also have one less critical system to restore.

Lower TCO

Moving your PKI to the cloud can take multiple security controls, maintenance tasks, and infrastructure costs completely off your hands. Frankly, the capital expenditure needed to properly manage a solid internally run PKI is considerable, forcing many organizations to make critical PKI operations a secondary task.

Adopting the right PKIaaS platform can save a significant amount of time and resources, enabling your highly skilled IT and security teams to be more productive, and allowing your PKI to get the attention it deserves. Infrastructure teams are able to focus on core projects — not getting caught up repetitive tasks like CA renewal, server patching, and HSM maintenance. Costs also become much more predictable, since the many hidden and traditional expenses of PKI are replaced with a flat rate billing model.

Scalability & Availability

A PKI supporting mission-critical applications must be available around the clock and scale up on-demand to support millions of identities. However, legacy PKI deployments typically lack support for appropriate redundancy and scalability. A "next, next, next" installation of Microsoft CA is simple, but it will not scale to support your future demands. Each new use case will add to the complexity of your initially "free" PKI solution.

By contrast, reputable PKIaaS providers have the right in-depth experience and knowledge of industry standards to help you get it right from the start – designing a PKI that is customized to your current and future business needs. High availability and scalability built into cloud-delivered PKI models support growth demands, coupled with 24/7 service monitoring to ensure that all critical components are always running. Most importantly, service level agreements (SLAs) guarantee response times and ensure that there is only "one throat to choke" should an incident occur, and it isn't yours.

Business Continuity

People and processes drive the success of PKI, but in today's workforce, personnel can quickly shift, leaving PKI in unfamiliar hands. Shifts in PKI ownership inevitably increase the risk of security gaps as inexperienced hands fall on mission-critical infrastructure. Lapses in regular maintenance tasks such as signing and publishing certificate revocation lists (CRLs) and renewing CAs can cause significant outages that take days or even weeks to remediate.

Deploying your PKI in the cloud ensures that, regardless of shifts in your IT and security personnel, your infrastructure continues to operate at full capacity. PKIaaS providers ensure that no aspect of your PKI is overlooked, from design throughout its lifecycle. System-wide outages are easily avoided by leveraging a dedicated PKI team to help you stay ahead of critical day-to-day management and maintenance tasks. All the while, built-in disaster recovery and backup provide high assurance that your critical PKI functions can be effectively remediated should an incident occur.

Lifecycle Automation

Beyond the nuts and bolts of PKI, you need visibility and control over every certificate issued. Manual scripts and spreadsheets cannot keep up with the thousands or hundreds of thousands of certificates in use across your organization today. All it takes is one expired certificate to slip through the cracks to cause a serious network or application outage.

Choosing the right PKIaaS provider can enable you with the tools to manage and automate the lifecycle of keys and digital certificates issued from both your cloud-hosted private PKI and any number of third-party public CAs. Lifecycle automation reduces the workload on your PKI team and certificate end-users, and drastically minimizes the risk of a certificate-related outages or breaches.

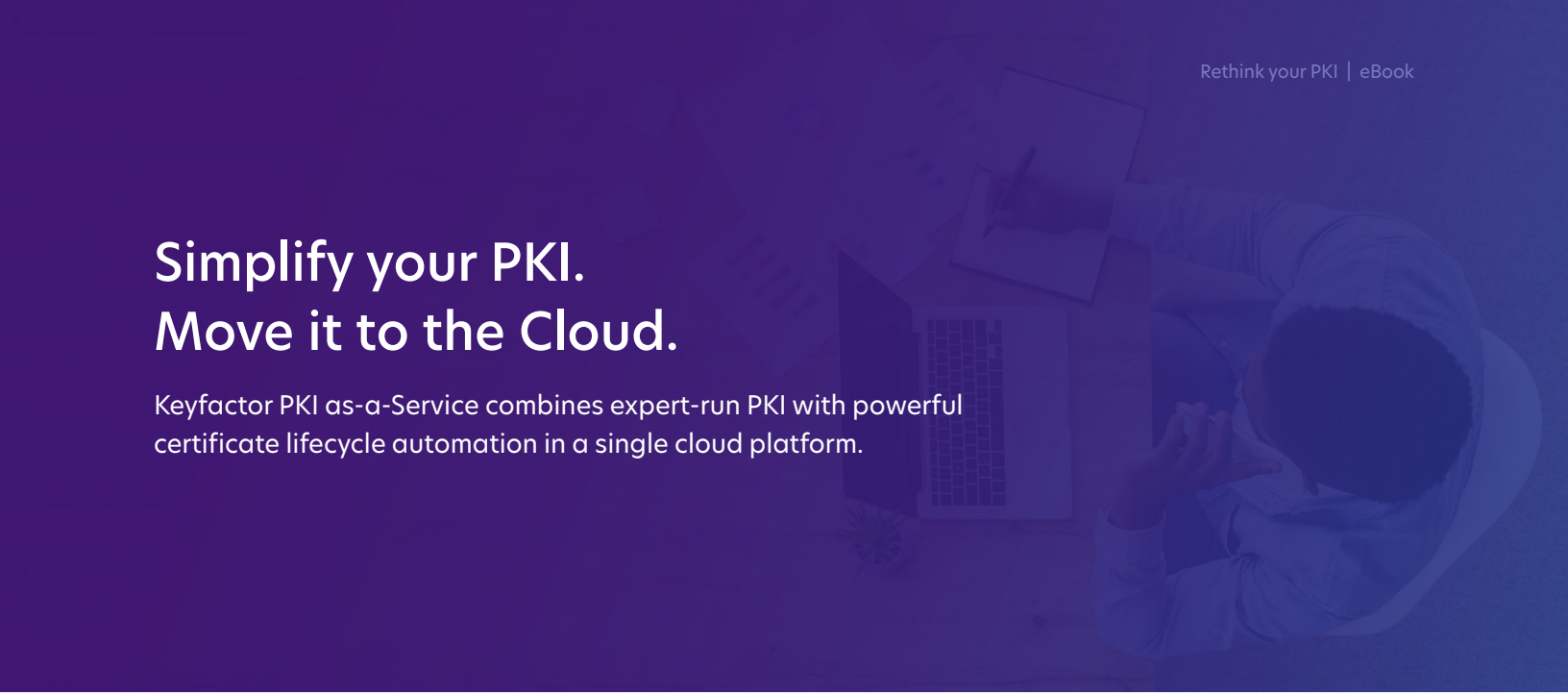
WHAT ABOUT CONTROL?

A common misconception about cloud-hosted PKIaaS is that you must give up control of the virtual keys to your kingdom. But it's easy to have it both ways — maintaining control while outsourcing complexity. It comes down to the provider you choose.

A reputable PKIaaS provider will offer a platform that gives your business complete control over root CA keys and PKI recovery materials, while design, deployment, and management tasks remain their responsibility. That way, you always retain the ability to move your PKI in-house should the need arise.

Simplify your PKI. Move it to the Cloud.

Keyfactor PKI as-a-Service combines expert-run PKI with powerful certificate lifecycle automation in a single cloud platform.



The Leader in PKI as-a-Service

PKI is critical to enterprise security, but setting up the infrastructure and hiring the skilled personnel needed to build, operate, and maintain it 24x7 is no easy task. With security teams under increasing pressure, they need a new cloud-first approach to simplify and scale PKI on demand.

1 Billion+
Certificates issued globally

10 of the Fortune 100
Run on Keyfactor PKIaaS

60%
Reduction in PKI Spend

Why Keyfactor

All-in-one solution

One vendor - combines fully-managed PKI and certificate lifecycle automation.

Tested and proven

We're the most reliable and widely adopted PKI as-a-Service platform – since 2011.

No lock-in

You retain full control over root keys and recovery materials in escrow to avoid any lock-in.

Tenured PKI experts

Our roots started in PKI consulting – no one knows how to build and run PKI like we do.

Unmatched services

Fast SLA-driven response, SOC 2 Type II audited annually, and 99% support satisfaction.

Limitless scalability

Scale up easily with high-availability and geo-redundant options.

Ready to re-think your PKI?

There comes a time in every PKIs lifespan when it must move out and scale up to the growing demands of your business. If you've adopted a cloud-first strategy, don't leave your PKI in the dust.

You already know that PKI is critical to your enterprise security, but the hassle and hardware required to keep it running and secure often just isn't worth it. Whether you're a skeptic or you're all in on cloud, request a demo to see if it's the right time to re-think your PKI.

See how Keyfactor's PKI as-a-Service combines expert-run PKI with powerful certificate lifecycle automation in a single cloud platform.

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