KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

EBOOK

5 Reasons to Move your PKI to the Cloud

WHY ENTERPRISES ARE ADOPTING CLOUD-DELIVERED PKI AS-A-SERVICE

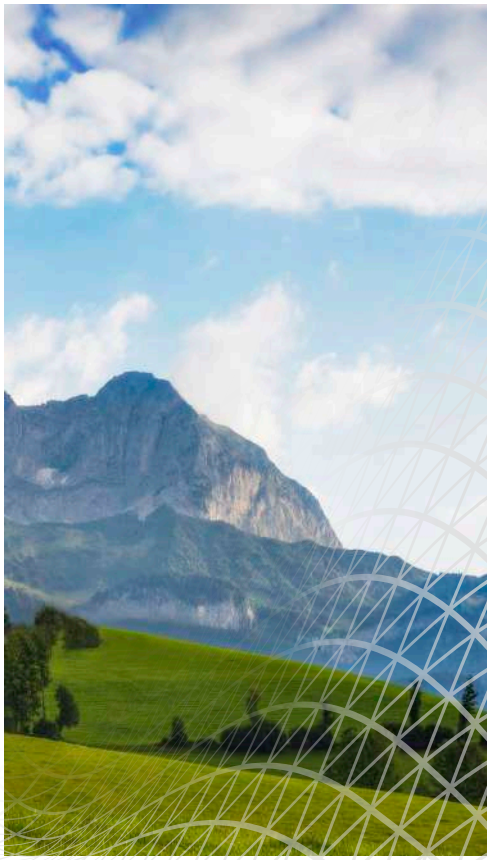

Table of Contents

Introduction

Public key infrastructure (PKI) is a fundamental security tool used by most organizations today. 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 IT and security 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.

More than half (55%) of organizations have or plan to outsource all or part of their PKI deployment.[1]

[1] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report

The Changing Role of PKI in your Enterprise

PKI establishes a digital identity for people, applications, and devices across your enterprise, ensuring that only trusted entities can gain access to data, networks, and even physical locations. IT and security teams have deployed PKI to combat a growing number of cybersecurity threats facing organizations today – from ransomware and phishing attacks to IoT device hijacking.

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 – which has taken on a larger role in the business. No longer limited to a few use cases like encrypted email or network access, private PKI is now emerging as a core technology to secure business initiatives including mobile devices, IoT and DevOps.

PKI and digital certificates are widely adopted for a multitude of use cases and applications:

WEB SERVERS

Deploy SSL/TLS certificates on external facing web and applications to enable trust for customers and website visitors.

INTERNET OF THINGS (IoT)

Enable mutual authentication, encryption and integrity controls for connected devices, gateways and applications in your network.

SECURE EMAIL

Digitally sign and encrypt emails using S/MIME for corporate devices across the organization.

MFA/SSO

Deploy multi-factor authentication for single sign-on applications such as Windows Hello, Office 365 or ServiceNow.

WI-FI ACCESS

Authentication to Wi-Fi connections to ensure that only trusted users are accessing the network without the need for passwords.

NETWORK DEVICES

Enable authentication between routers, firewalls, load balancers, and SSL inspectors to establish trusted network infrastructure.

An average of 8 different applications are now supported by an organization's PKI.[2]

CLOUD

Secure cloud-based instances and virtual servers to help establish a trusted multi-cloud environment.

MOBILE DEVICES

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

VPN ACCESS

Replace expensive and cumbersome VPN authentication solutions with password-free certificated-based authentication.

DEVOPS

Ensure security and integrity of cloud instances and containers, as well as code signing for software and firmware pushed from production.

[2] source: https://www.ncipher.com/2018/pki-trends-study

Getting it Right: The Complexity of PKI

Because of its broad, comprehensive reach, PKI is complex and can be challenging for internal teams to effectively manage. Unlike other technology, PKI has many moving parts beyond the software and hardware involved. All the components that make up a robust, secure PKI environment require significant investment of IT budget and resources – from certificate policy development and training, to infrastructure security and certificate management.

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.

PERSONNEL

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, manage certificate lifecycles, and more. 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, OCSP servers, CRL servers, 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.

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.

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.

Business Challenges

While PKI is more complicated than most people realize, it's also taking on a more critical role in the business. However, various challenges still stand in the way of a successful in-house PKI deployment:

NO CLEAR OWNERSHIP

Despite the importance of PKI, most organizations do not have clear ownership of who is responsible to manage the infrastructure and digital certificates involved. 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

PKI requires specialty knowledge around both deployment and operations. 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. While PKI operations are mission-critical to business operations, it doesn't necessarily need to be managed internally.

PKI OPERATIONS UNDER STRESS

As more stringent industry and data security regulations come to fruition, businesses are becoming more reliant than ever on PKI to guarantee trust. 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.

Only 39% of organizations say they have sufficient IT security staff dedicated to PKI deployment.[3]

LACK OF TOOLS & PROCESSES

Without the right tools and processes to manage PKI operations, there are a number of consequences that can be hard to remediate. IT specialists 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] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-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 have the right expertise and resources to get it right.

It's clear that proper management of PKI for enterprise IT and security teams is becoming a serious challenge. There is significant pressure to support the day-to-day needs of the organization while simultaneously managing business growth and new initiatives. With in-house PKI, the IT team is responsible for planning, building and managing infrastructure, as well as managing the lifecycle of every digital identity in the environment. It is for these reasons that many are looking to the cloud for relief.

IN-HOUSE PKI	VS	PKI AS-A-SERVICE
Enterprise designs, builds and deploys their private PKI infrastructure, assuming 100 percent of the risk and cost of implementation.		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 cost, risk and complexity of PKI lies in its management and maintenance. Organizations must also consider how digital transformation will change demands for encryption and authentication in the future and the impact that will have on their PKI.

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."[4]

[4] source: https://www.gartner.com/en/documents/3891976/the-resurgence-of-pki-in-certificate-management-the-iot-

5 Reasons to Move your PKI to the Cloud

Why should you re-evalutate your PKI deployment? Compliance mandates, organizational changes, and evolving cryptographic standards are all cause to consider a move to the cloud. Here are the top reasons why businesses are putting their PKI in the hands of a trusted PKIaaS partner:

01 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. In addition to specific tools used to protect keys, the facility housing critical PKI functions must be secure.

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, since your PKI is hosted safely in an isolated, off-premise cloud location.

02 REDUCED COST & COMPLEXITY

Moving your PKI to the cloud can take multiple security controls, maintenance tasks, and infrastructure costs completely off your hands. Frankly, the capital expenditure and expertise 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 needs to protect your business. Infrastructure teams are able to focus on core projects – not getting caught up in managing and maintaining PKI. Costs also become much more predictable, since the many hidden and traditional expenses of PKI are replaced with a flat rate billing model.

03 SCALABILITY & AVAILABILITY

A PKI supporting mission-critical applications must be available around the clock and be able to scale up to millions of users and devices as your enterprise grows. However, legacy PKI deployments are not designed for more than one or two applications, and 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.

04 BUSINESS CONTINUITY

People and processes drive the success of PKI, but in today's workforce, personnel can quickly shift, leaving PKI in unfamiliar hands. Finding and retaining IT and security staff capable of running PKI, not to mention multiple other responsibilities, is no simple task. 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.

05 LIFECYCLE AUTOMATION

Beyond the nuts and bolts of PKI, every digital certificate issued from your internal private CA, plus certificates issued from your public CAs, must be effectively managed throughout their lifecycle. Certificate-related issues are almost synonymous with PKI oversights. Manual scripts and spreadsheets simply cannot keep up with the thousands or hundreds of thousands of certificates in use across your organization today. It takes just 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 such as DigiCert, Entrust, Sectigo, and others. 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 due to human error or oversight.

Less than half (45%) of organizations are able to hire and retain qualified IT security personnel.[5]

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.

[5] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report

Keyfactor™ Command

PKI AS-A-SERVICE & CERTIFICATE LIFECYCLE AUTOMATION

Most everything about typical PKI and certificate management is complicated. Retaining the right people with unique skillsets, cumbersome certificate deployments and updates, the expense of management and expansion, not to mention all that's at stake if something goes wrong.

To run efficiently, systems and infrastructure must be woven together – with ongoing monitoring, real-time updates, and operating within budget. When done right, this complex orchestration helps ensure that every digital identity is covered, keeping breaches and outages at bay.

Keyfactor Command is the world's most complete and scalable cloud-based PKIaaS and certificate lifecycle automation product, providing the freedom to secure every digital identity across the enterprise. Get all the benefits of owning PKI without the risks.

A Powerful Combination

PKI AS-A-SERVICE

Get all the benefits of private PKI, without the operational complexity and cost of managing the software and hardware required to run it. You maintain control over day-to-day decisions while offloading backend tasks to our PKI experts.

CERTIFICATE LIFECYCLE AUTOMATION

Discover, manage, and automate the entire lifecycle of keys and digital certificates across your private and publicly rooted PKI to effectively prevent certificate-related outages and breaches.

✓ ROBUST, DEDICATED PKI

State-of-the-art PKI infrastructure delivered on demand from the cloud with a customer-devoted root CA and no shared infrastructure

✓ LEADING EXPERTISE

24/7/365 management and oversight by Keyfactor's world class team of PKI experts constantly ensuring operation health

✓ END-TO-END AUTOMATION

Locate all of your certificates and continuously monitor and automate their lifecycle – from issuance to renewal and revocation

✓ BUILT-IN COMPLIANCE

High-assurance and availability built into a SOC 2 Type II documented environment, including FIPS 140-2 validated HSMs

✓ RESPONSE COMMITMENTS

Proven SLAs with clearly stated, guaranteed response times

✓ COMPLETE CONTROL

Maintain complete control over the use of your root certificate authority and PKI recovery materials

READY FOR THE CLOUD?

Learn more about how Keyfactor can help you get started on your path to PKIaaS.

Talk to our experts ▸

ABOUT

KEYFACTOR

Keyfactor is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

CONTACT US

▸ www.keyfactor.com
▸ 216.785.2990