Outsourcing PKI to the Cloud

Why You Should Replace On-Premise PKI With PKI-as-a-Service

EBOOK

Executive Summary

Businesses are under an ever-increasing demand to move services online, take advantage of cloud infrastructure, and integrate extensively with other systems. This does bring significant benefits — the enterprise can take advantage of operational agility and scalability and use this to build a competitive advantage. But there are risks, too. The proliferation of new endpoints, an increase in remote working, the insistence on accessibility and integration everywhere, and the IoT revolution all come with a significant concern — security.

Managing security at scale is a major overhead for organizations. As hackers and criminals become more sophisticated, it's more important than ever to create strong, robust and proven methods to encrypt information and verify access rights. The gold standard for securing information across the network is through public key infrastructure (PKI).

When it comes to implementing PKI, businesses have some options. They can develop a DIY on-premise PKI system using services like Microsoft Certificate Authority and Active Directory Certificate Services. While this may initially seem like a good idea, as the need for PKI management grows, a DIY in-house system can quickly become overburdened and slow to react. Add to this a multitude of hidden costs and significant engineering resources, and any advantages are quickly eliminated.

Another option for businesses is to use an on-demand, cloud-based PKI solution, commonly referred to as PKI-as-a-Service (PKIaaS). PKIaaS provides a PKI platform that will rapidly and effortlessly integrate with existing networks and systems to provide best-in-class security for data transfer. Even better, PKIaaS is provided on a subscription basis, making it much easier for businesses to control budgets and remove the need for a large, upfront CapEx investment.

While we believe that PKIaaS offers significant benefits over a DIY PKI system, we realize that choosing the right security infrastructure has profound implications. To help you decide, we've explored several aspects of the DIY on-premise PKI system versus cloud-based PKIaaS platforms. By the end of this paper, you will have a clear idea of what each type of service can provide, and why PKIaaS is likely to be your better choice.

> *"In recent years, PKI has evolved from a means to protect websites, into the heart of the digital management function within the cybersecurity structure. Today, it is used to manage digital identities, applications and devices within companies.*
>
> *It is also being adopted and deployed by IT teams to combat a growing variety of cybersecurity threats, spanning distributed denial of service (DDoS) attacks to malware, and phishing attempts to the hacking of internet of things (IoT) devices."*
>
> —Computer Weekly, Outsourcing PKI to the cloud: What enterprises need to know[1]

Digital Transformation in the Enterprise Relies on Strong Security Foundations

The demand for flexible, scalable, user-focused technologies has never been greater.[2] This drive for digital transformation is irresistible, with marketplace forces demanding that companies adapt. As businesses upgrade their networks and IT systems to take advantage of this new world, a robust, responsive, and strong security infrastructure is critical.[3]

Companies need to verify that cloud environments, DevOps, endpoints, remote access, IoT devices, and other areas meet robust encryption and verification standards to access sensitive networks. Secure, encrypted access is a vital foundation for digital transformation.

PKI is a critical foundation to provide secure data transfer and encryption.

"Applications running in the cloud and data stored there are not protected by a traditional corporate security perimeter of firewalls and the like. As a result, security becomes essentially reliant on encryption and management of the keys that provide access to encrypted data. Our interviews revealed that most companies, especially large ones, do not entrust SaaS providers to host and manage their security keys. The majority prefer to hold their keys on-premises through a hardware security module, retain management control of cloud-hosted keys, or use a combination of methods."

—McKinsey, Securing software as a service[4]

A Quick Explanation of Public Key Infrastructure

PKI creates two special, secure, paired keys (public keys and private keys) through a complex algorithm. These keys encrypt data traveling between users, systems, customers, applications, and devices. Prior to transmission, data is encrypted using the “public” part of the key pairing. When the data arrives at its destination, the paired “private” key is used to decrypt the data.

Implementing public key infrastructure in the enterprise is central to allowing the secure exchange of sensitive information and authentication. Introducing, managing and supporting on-premise PKI can be challenging, requiring cybersecurity teams to balance several areas.

That’s why an adaptable, cloud-based PKI-as-a-Service (PKIaaS) solution can provide the scale and flexibility a business needs to deal with the most demanding security challenges.

PKI is becoming more central to reducing the concerns of cybersecurity managers.

As a foundational security technology implemented for decades, public key infrastructure (PKI) is already deployed in most enterprise IT infrastructures. However, the ongoing management and maintenance of an in-house PKI deployment can be difficult and requires dedicated, skilled staff — adding to overall security costs. An on-demand PKIaaS solution can significantly reduce those costs and keep them under control.

Cybersecurity Experts Know That Robust PKI Is Essential

A report from our colleagues at Dark Reading[5] highlighted some of the main concerns of security experts toward cybersecurity management:

- **70%** say that their cybersecurity staff are stretched too thin
- **49%** say the complexity of the security environment is their biggest challenge
- **40%** expect that security challenges will become a lot harder in the near future, even though budgets and staff will remain the same
- **39%** have made remote access the top cybersecurity priority

So, with the choice of DIY PKI or PKIaaS, how do they stack up?

Credential compromises are now more commonplace, with 41% of access keys remaining unchanged in the cloud in the past 90 days.

CloudStandards.org, Cloud Computing Statistics: 2020 Overview[6]

> *“Cloud-based PKIaaS or managed PKI is a growing trend with more and more IT leaders considering it as a valid option. PKIaaS providers automate client certificate lifecycles and include dedicated staff, systems, and distributed datacenters that scale and meet the growing needs of their clients, while also providing the platform to improve efficiency and effort required to manage all company certificates.”*
>
> Computer Weekly, Outsourcing PKI to the cloud: What enterprises need to know[7]

On-Premise PKI vs. Cloud-Based PKI-as-a-Service

Traditional, on-premise PKI can work — up to a point. The problem is that as networks and integrations become more complex, and endpoints grow, managing that environment at scale becomes increasingly difficult and expensive.

If you run your own on-premise PKI services, you’re limited by the capabilities and demands of your PKI infrastructure. This could mean significant extra investment as you add or update services. Instead, it makes much more sense to use an adaptable PKI that can expand as your technology footprint and user base grow.

PKI-as-a-Service is a cloud-based solution that lets you tailor and expand your PKI services as needed.

PKIaaS means you can:

- **Add and change PKI security services at any time** — Get adaptable PKI as needed, meaning you can increase capacity and expand technologies without upfront investment or concerns about demand
- **Deploy scalable PKI services quickly and accurately** — Speed and quality are essential to ramping up PKI in a scalable and manageable way. PKIaaS grows alongside your business and security needs.

PKIaaS Supports Digital Transformation in Multiple Ways

Although greater flexibility and reduced costs are powerful incentives for businesses, PKIaaS isn't just about the bottom line. There are several other significant ways that it can support your business, for example PKIaaS:

- **Automatically implements industry-leading best practices for PKI.** Stay ahead of potential attackers and breaches by using a complete PKI solution that's continually updated and takes advantage of the latest thinking in security research.
- **Introduces a baseline of "Zero Trust."** Only allow access to assets through robust security permissions tied to individuals, job roles, devices, and processes through your organization.
- **Meets compliance and regulatory guidelines for PKI security.** Ensure your PKI solution remains fully compliant with standards and regulations.
- **Controls budgets and reduces costs for PKI operations and projects.** Control PKI security costs for both your day-to-day operational needs and for any program or project that increases the scope of security in your organization.

To raise the benefits of PKIaaS, it's important to see how a DIY on-premise PKI solution could function, specifically those using Microsoft services.

Microsoft Certificate Authority, Active Directory Certificate Services and DIY PKI

Some enterprises and cybersecurity managers may still be building or using a DIY PKI system. Microsoft Certificate Authority (MCA) and Active Directory Certificate Services (AD CS) are still popular choices, but are they the right ones?

A QUICK OVERVIEW OF AD CS AND MCA

AD CS and MCA are part of the Windows Server operating system. They manage digital certificates for accessing applications and information on the corporate network. Cybersecurity teams can use MCA and AD CS to implement their own, locally-installed DIY PKI security services. MCA provisions the certificates while AD CS administers them.

Microsoft describes AD CS as follows:[8]

"AD CS provides customizable services for issuing and managing digital certificates used in software security systems that employ public key technologies. The digital certificates that AD CS provides can be used to encrypt and digitally sign electronic documents and messages. These digital certificates can be used for authentication of computer, user, or device accounts on a network. Digital certificates are used to provide:

- Confidentiality through encryption
- Integrity through digital signatures
- Authentication by associating certificate keys with computer, user, or device accounts on a computer network

You can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding private key."

Let's dig into the advantages and disadvantages.

ADVANTAGES OF MCA AND AD CS

- Active Directory integration reduces the need to reregister certificates
- Existing group policies can be used to avoid the need to creating new PKI policies
- MCA provides automated certificate provisioning while AD CS handles lifecycle management
- Certificates are automatically installed without end user involvement

This all sounds great, but unfortunately AC DS and MCA have some significant drawbacks.

DRAWBACKS OF MCA AND AD CS

- **Upfront hardware costs:** There's a significant CapEx cost for creating a DIY PKI service, including the need to protect and store private keys on secure hardware like a hardware security module (HSM)
- **Ongoing costs:** Ongoing maintenance costs for maintaining DIY PKI infrastructure can be substantial and can include deploying patches across the environment and backing up critical certificate data
- **Validation of certificates:** Extra resources and technology will be required for maintaining validation services to ensure the validity of MCA-provisioned certificates
- **PKI expertise:** On-staff PKI experts will be required to implement, manage, maintain and integrate your DIY PKI solution
- **Lack of flexibility:** As security needs evolve, you will need to quickly adapt DIY PKI to support the latest devices and use cases
- **Difficulties with compliance:** Any DIY PKI solution implemented must meet regulatory and industry guidelines and frameworks
- **Demand management:** As the need for certificates and PKI grows, it can be difficult for an MCA-centered solution to keep up
- **Limited automation:** As it is core Microsoft technology, it doesn't provide automation for every machine and device on the network

MCA struggles with provisioning and managing more than a few thousand certificates with single instance. Each user and device can require multiple certificates, so it can be easy for an enterprise to hit these limits fast. PKIaaS helps you avoid these issues, and provides many of the same advantages as MCA and AD CS.

The Hidden Costs of On-Premise PKI

DIY PKI solutions can end up costing an enterprise much more than just the amount spent on hardware, backups, integrations and support. Some of the more subtle, hidden costs associated with on-premise PKI include:

- Administrative costs for setting up:
  - Enrollment and initial authorization
  - Registration authorities and integration
  - Authentication and identity and access management
  - Certificate templates and provisioning
  - PKI policies and other security protocols
- Regulatory, compliance, logging and audit costs
- Certificate provisioning, revocation and lifecycle costs
- Costs associated with key management and backups

This all consumes network resources, server time and cybersecurity engineer expertise.

There are other hidden costs too, like integrations with other systems, communicating requirements with touchpoints, and exhaustive testing of endpoints and new implementations.

PKIaaS eliminates the majority of these costs.

See how HID Global's PKIaaS stacks up to on-premise PKI. Start comparing >>

> *"As organizations digitally transform their business, they are increasingly relying on cloud-based services and applications, as well as experiencing an explosion in IoT connected devices. This rapidly escalating burden of data sharing and device authentication is set to apply an unprecedented level of pressure onto existing PKIs, which now are considered part of the core IT backbone, resulting in a huge challenge for security professionals to create trusted environments."*
>
> —Dr. Larry Ponemon, chairman and founder of The Ponemon Institute[9]

The Need to Future-Proof the Enterprise With PKIaaS

PKIaaS allows businesses to rapidly scale and flex new services, devices, integrations, and applications without having to reinvent the wheel. This future-proofing allows companies to adapt, bringing new products to market faster and increasing competitive advantage. Some of the upcoming changes that can be better supported through PKIaaS include the following:

- Remote work is becoming the new normal, as employees choose to continue working from home
- IoT devices are increasing in prevalence and popularity, resulting in more data transfer and connectivity that must be secured
- Public, private, and hybrid clouds are rapidly becoming the new infrastructure of choice, and these environments must be carefully and securely managed
- Enterprises themselves are developing customer- and employee-facing cloud-based applications that must be secured and encrypted

PKIaaS platforms also have several other vital features that will help enterprises be ready for whatever comes over the horizon:

- They are platform agnostic, so they integrate with a huge variety of existing software, use cases, security protocols and approaches
- They are agile and flexible, so they can be scaled and changed at speed based on business, user or customer demands
- They are reactive to emerging technologies, reducing the burden of expanding the technology footprint

How HID Global's PKIaaS Can Help

HID Global's managed private cloud PKI-as-a-Service enables organizations to quickly create and deploy their own private enterprise PKI trust hierarchies to secure their networks, IT systems and IoT devices. HID adapts to multiple security scenarios and can be quickly deployed for remote working.

HID Global's PKIaaS can revolutionize your security management by:

- Offering the choice of a simple preconfigured service by dedicated Issuing Certificate Authority (CA) or a completely customized private root PKI service
- Offering full turnkey service including private root key generation ceremony and custody management of all off-line key material
- Managing all certificate validations across all systems and assets
- Providing best-in-class PKI infrastructure that aligns with industry best practices and leverages highly secure and audited technical facilities with the expertise to deliver it all
- Supporting Zero Trust with secure authentication and communications between machines, devices, IoT and virtual servers
- Offering future-proof PKI that adapts to changing needs with complete flexibility to add new services at any time
- Deploying in weeks, not months, and bringing a quick return on investment
- Providing a single pane of glass through certificate management portal for private and trusted TLS/SSL certificates
- Automating certificate lifecycle management through Microsoft Autoenrollment and other standards-based certificate management protocols such as SCEP, EST, and ACME as well as API support
- Integrating with trusted certificate services including OV, EV, Wildcard and SAN certificates as well as client certificates such as S/MIME and code signing

HID Global's PKIaaS provides encryption and authentication services to help companies secure computer and network devices, IoT systems and e-commerce transactions. HID Global's PKIaaS focuses on helping companies achieve industry best practices related to authentication and encryption, while reducing operating complexity and costs. HID's cloud-based PKI as-a Service offering allows organizations to obtain authentication and encryption services on-demand, in real time.

See how HID makes PKI and certificate management a breeze. Request a demo >>

About HID Global

HID powers the trusted identities of the world's people, places and things. We make it possible for people to transact safely, work productively and travel freely.

People use HID products to open doors, access digital networks, personalize badges, verify transactions, find information, track assets and connect with others — ensuring their identities are seamlessly accepted, anywhere, anytime.

With HID's trusted identity solutions, people get effortless and worry-free identity verification experiences — with only a tap, twist, tag, push, swipe, or simple proximity of their chosen device.

[1] https://www.computerweekly.com/feature/Outsourcing-PKI-to-the-cloud-What-enterprises-need-to-know

[2] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-ceos-new-technology-agenda

[3] https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

[4] https://www.mckinsey.com/business-functions/risk/our-insights/securing-software-as-a-service

[5] https://info.hidglobal.com/202009iampkinamcertauthcomwebwp3rdptycybersecurityproblem_LP-Request.html

[6] https://cloud-standards.org/cloud-computing-statistics/

[7] https://www.computerweekly.com/feature/Outsourcing-PKI-to-the-cloud-What-enterprises-need-to-know

[8] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11)

[9] https://www.helpnetsecurity.com/2016/10/11/future-proof-pki-implementations/

HID

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-03-30-iams-outsourcing-pki-cloud-eb PLT-05870
part of ASSA ABLOY