BUYER'S GUIDE

Cloud PKI as-a-Service

Practical Advice When Deciding to Build, Maintain, or Buy Your PKI

KEYFACTOR

It’s time to heavily maintain or build your next public key infrastructure (PKI). Build-it-yourself PKI isn’t impossible; in fact, most reading this guide already have a PKI deployed in their organization.

However, the question is whether you have the right expertise and resources to invest in a well-run PKI for the long-term. That’s when managed PKI as-a-Service becomes a viable option.

What’s Inside

This buyer’s guide is designed to help you choose the right managed PKI solution to keep up with your increasing security workloads. We highlight the core capabilities needed for a well-run PKI and give you all the evaluation criteria needed to make an informed decision.

Table of Contents

Introduction

Enterprise PKI is complex, and it's only getting harder.

Public key infrastructure (PKI) is a core mechanism in enterprise security, serving as a building block of IT for more than two decades. However, getting PKI right and maintaining it correctly can mean the difference between a highly secure environment and a serious breach.

The shift to containers, multi-cloud, and mobile platforms has created significant new challenges for IT and security teams running PKI internally, including:

No Clear Ownership

Enterprises are struggling with clear ownership for their PKI strategy. Although PKI has been labeled as critical infrastructure, there rarely is a direct line of responsibility.

Shifting Resources

Today's IT and security professionals are constantly changing responsibilities. Many carry multiple job functions beyond PKI, such as active directory managers, server managers, and other security roles.

Limited Expertise

If PKI expertise is present, these skills were derived over a long time predominantly through organic growth. This knowledge gap usually cannot be replaced if personnel changes occur.

THE SOLUTION:

Cloud-Hosted PKI as-a-Service (PKIaaS)

PKIaaS – also known as PKI as-a-Service or managed PKI – allows you to get all the benefits of well-run PKI, without the operational complexity and cost of managing the software and hardware required to run it. Your teams still maintain the control they need over day-to-day operations while offloading back-end tasks to a trusted team of PKI experts.

Finding a solution that is secure, cost effective, and scalable with your business is critical. Let's first dive into some common drivers of switching to PKIaaS.

“By attaching the notion of cryptography to a higher-level issue like digital business, the aim is for security leaders to increase their overall success in establishing a center of excellence for cryptography in their organization.”

Gartner

“Technology Insight for X.509 Certificate Management”

Erik Wahlstrom, Paul Rabinovich (October 2019)

PKIaaS, Why now?

Even if you understand the challenges with running your current PKI, it usually takes a compelling event or lack of knowledge to ask *"Do I really want to fix these challenges with my legacy, in-house PKI solution?"*

Some of these you've already experienced in the past and some will impact your business within the next few months.

SHA-1, SHA-2, Quantum

When an algorithm is no longer trusted, you're on the hook to update your PKI. The challenging shift from SHA-1 to SHA-2 should be a lesson for the quantum changes ahead.

Changes in PKI Staff

Due to the limited PKI resources you may have on staff and the expertise required to maintain PKI, workforce changes could create an unexpected knowledge gap.

Crippling PKI Outages

An offline, expired, or misconfigured CRL will result in the inability for an application/service to check the CRL prior to trusting any certificate issued by your CA. This outage can result in the blocking of services.

New Business Initiatives

Whether you are moving legacy workloads to the cloud, building new applications, or heavily investing in IoT, new changes require reconsideration for your current PKI deployment.

Exponential Growth of Certificates

With the explosion in digital certificates, is your PKI able to scale up and support the increased workload? As cloud adoption grows, and DevOps speed increases, certificate issuance and management needs to be addressed.

Imminent M&A

Mergers and acquisitions bring a whole new level of complexity to your PKI. Use this as the perfect opportunity to assess your PKI status and look for new options to support your new organization.

Certificate Authority (CA) Renewals

It's recommended that your Root CA is renewed with the same keypair after 10 years and with a new keypair after 20 years. CA renewal is a painful process, but it's an ideal time to re-consider your PKI strategy.

Only 38% of IT and security professionals say they have sufficient IT security staff dedicated to their PKI deployment.

Keyfactor-Ponemon Institute

"The Impact of Unsecured Digital Identities" 2020 Report

Core Capabilities

Let’s now look at the core capabilities offered by PKIaaS solutions in more detail.

This is not intended to be an exhaustive list; rather its purpose is to raise awareness of major capabilities and encourage vendor discussion during your buying process.

Offline Infrastructure

The root certificate authority ("root CA") is the anchor of trust in your public key infrastructure environment. The integrity of a PKI security model starts with the trust anchor and requires highly specialized controls in order to be maintained effectively.

Therefore, the most important question a PKIaaS provider must answer is, *"How are you going to protect and monitor my root CA?"*

Ask Vendors

- → Can I tour the data storage facilities to ensure a measure of confidence and trust in the security?
- → What physical and logical access controls do you use to protect the root CA?
- → Are HSMs available to protect CA keys for both the root and issuing CAs?
- → Should I need to move the hosted PKI in house, am I able to do that?
- → What evidence can be produced as to access of my root CA if I was asked to provide something to my auditor?
- → Describe the process of the root signing ceremony.

What to look for:

Root CA Protection

Offline Root CA protected by multiple layers of physical and logical security

The trust anchor of the hosted PKI managed service is an offline root certificate authority that's managed by the vendor on behalf of the customer. This means generating keys on an offline machine, which are placed within a dedicated FIPS 140-2 Level 2 hardware storage module (HSM). A solution must support the most popular HSMs on the market for customer preference.

Customer-Controlled Key Escrow

Ability to retain complete control over your root CA keys and materials

The root CA escrow process places a copy of your root CA cryptographic materials with a trusted third-party (known as an "escrow agent") in case something happens between the vendor and customer relationship. This allows you to keep control of your PKI and bring it back in-house if the situation should arise. Vendors should always allow the option to easily move your PKI.

State-of-the-Art Data Centers

Secure storage and continuous monitoring

Data centers should be powered with HD video monitoring, entry logging, and biometrics for step-by-step transparency. The vendor should follow a best practice of using a secondary data center to ensure redundancy for disaster recovery. Split data centers allow for keys to be distributed to multiple locations for extra security measures.

Controlled Physical Access

Limited physical access, and when required, carefully handled

Security measures include using materials and processes, such as: GSA level-5 security vault, fireproof protection, two-key controlled cabinets, tamper evident bags, locking cage, and 24/7 on-site security personnel.

“Gartner sees an increasing number of organizations that now rely on third-parties to manage their PKI.”

Gartner

“The Resurgence of PKI in Certificate Management, the IoT and DevOps”

Erik Wahlstrom, Paul Rabinovich (October 2018)

Cloud-Hosted Infrastructure

A well-designed PKI infrastructure includes common capabilities like high availability, backup, business continuity, and disaster recovery. These are necessary for any cloud PKI deployment whether you are deploying in-house or hosting in the cloud.

Additional focus must be placed on the abilities to manage and procure the root CA, issuing CAs, OCSP servers, CRL servers, enrollment processes, private key storage, and more.

Ask Vendors

- → Can you present a total cost of ownership using my current environment?
- → What would it cost my organization to build an identical PKI deployment in house?
- → Where does certificate management and automation software fit into PKIaaS?
- → What's the largest deployment you have had? Present hard data examples.
- → How do you use HSMs to protect our root and online issuing CAs?
- → What deployment options are considered standard and non-standard?

What to look for:

No Shared Infrastructure

Dedicated, single-tenant PKI environment with layered security

Just like your on-premise environment isn't shared with another company, your PKIaaS hosting should be safe guarded in a single-tenant environment. The solution you select should have a dedicated firewall with a "least-privilege" access model and support HSMs for online issuing CAs.

High Availability

SLA-driven availability for CA and CRL infrastructure

Your PKI is critical infrastructure that can't afford to be unavailable. Look for vendors that can provide the highest degree of guaranteed uptime 99.5% - 99.9% for both the service and CRL. A vendor should describe assurances to you if uptime is not met.

Certificate Management

Built-in certificate management and automation with PKIaaS

PKIaaS without certificate management capabilities results in an incomplete product. With integrated certificate management, teams get a single pane of glass to monitor their PKI processes and track certificate lifecycles. A combined solution should take priority during evaluation.

Unlimited Scalability

Infrastructure that scales with the growing issuance of digital certificates

Any solution can handle any small amount of digital certificates. As your digital identities grow, your infrastructure must be able to support at scale. As a best practice, the solution should build infrastructure with separate application and database layers.

“New disruptors — as well as technology shifts such as free certificates, new cloud delivery models and broken crypto — rattle the traditional PKI world.”

Gartner

“The Resurgence of PKI in Certificate Management, the IoT and DevOps”

Erik Wahlstrom, Paul Rabinovich (October 2018)

Compliance & Operations

A vendor's Information Security Management System (ISMS) should be managed by its Director of Information Security & Compliance and formally reviewed and updated on an ongoing basis.

You're about to trust your PKI design, deployment, and management of tasks to a vendor. Are you confident that their compliance and operations are world class?

Ask Vendors

- → What SOC-2 certifications do you have? How often are they renewed?
- → Can you show me in-depth security review findings from your auditor?
- → Are we able to make changes to the vendor's CP/CPS framework to fit our business needs?
- → How often do you perform PKI health checks with your customers? What does it cover?

What to look for:

SOC 2 - Type II Certified

Ensure audit and compliance coverage with SOC-2 Type II

SOC-2 Type II certification provides assurance about the controls at a service organization relevant to security, availability, and processing integrity. While SOC-2 Type I attests to the design effectiveness of a vendor's controls, Type II provides a more rigorous scope of compliance and attests to the operating effectiveness of the controls.

A Robust CP/CPS

Adopting a strong PKI framework that suits business needs

Certificate Policy (CP) and Certification Practices Statements (CPS) are excellent frameworks for defining the requirements governing a PKI, and the means by which an implementation would meet those requirements. Make sure your vendor's CP/CPS framework truly represents your organization's PKI requirements and operational processes.

Frequent PKI Health Checks

On-going customer engagements for continued success

PKI is not a "set and forget" kind of security tool. It may be tempting to leave it alone once it's up and running, but this is a grave mistake - continual monitoring and management are critical to ensuring the highest possible levels of security. A vendor's customer success team should routinely work with you on setting health checks.

Implementation and Delivery

Having confidence that your PKIaaS can be implemented and delivered in a timely manner shows how competently a vendor can meet your schedule. For some vendors, PKIaaS still takes months when it should take weeks.

However, delivery doesn't stop once the hosted environment is production ready. Your evaluation should be baselined on a continuous engagement model for on-going success.

Ask Vendors

- → What's the average response time for different severity levels? How do you describe each level? (e.g. Sev 1, 2, 3)
- → Do you offer 24X7, 365 support? Are they full-time employees or 3rd party contractors?
- → Describe the communication channels for patches, upgrades, new releases, etc.
- → On average, how many product updates can I expect within a given year? Are these mandatory?
- → Describe some of the most challenging PKI engagements you've solved in the last six months.

What to look for:

Continuous Service Monitoring

Monitor CRL and CA availability across all PKI servers/components

The use of monitoring tools and scripts can check your environment to make sure they are not blocked from issuing certificates, notified of expiring CRLs, and more. Challenge vendors to give contractually obligated SLAs for uptime.

Incident Response

Rapid response times for critical incidents and planned mitigation

If a security vulnerability is announced that affects your hosted environment, you need to know as soon as possible to plan for patch fixes. Look for guaranteed, best-in-industry response times and ask for customer references to verify response claims.

Trained PKI Experts

Proven record of PKI expertise in consulting and delivery

The old saying of "it's just software" doesn't cut it with PKI. A strong consultancy background should be required as trusted partners for PKIaaS. Make sure the team responsible for managing your PKI is well-trained and trusted to host your PKI on your behalf.

Continuous Updates

Consistency in infrastructure updates and new feature releases

Not all "as-a-service" solutions are created equal. The added benefits of PKIaaS quickly diminish when vendors fail to deliver consistent updates to critical software patches, server updates/upgrades, and new features. Make sure to ask for a rolling monthly update process and product roadmap highlights.

An estimated average of
88,750 keys and certificates
are used by organizations today to
secure data and authenticate systems.

Keyfactor-Ponemon Institute

"The Impact of Unsecured Digital Identities" 2020 Report

What to Avoid

Far too many companies trust their PKI to a vendor, only to find out that their proof of concept didn't stand the test of their production environment. Here are some practical tips and considerations from our PKI experts to help you avoid selecting a solution that isn't the right fit for your organization.

1 Tip #1: Don't Give Up Control

Any vendor that does not give you the right to own your PKI should be discounted from consideration. Ask the right questions to make sure your PKIaaS platform gives your business complete control over root CA keys and PKI recovery materials. The design, deployment, and management tasks remain the responsibility of the vendor, while you still stay in control.

2 Tip #2: Steer Clear of Shared Infrastructure

Never host your PKI on shared infrastructure. PKI's mission critical nature should not be stored within a multi-tenant environment. PKI deployments generally are not one size fits all. By not being constrained to a shared infrastructure, a single tenant solution offers more flexibility for your PKI needs.

3 Tip #3: Only Consider Combined PKI & Certificate Management

PKI and certificate management should stand together in your PKIaaS evaluation. As we've mentioned before, as soon as you issue your first certificate, you will start to have a certificate management need. Ask vendors to show the complete solution, rather than half.

4 Tip #4: Check out Reviews

This buyer's guide does not provide an exhaustive list of core capabilities, nor does it provide all the questions you need to ask vendors. Over half the time spent evaluating a vendor is done digitally and customer reviews should be included in your decision journey. Check out analyst review sites and others to see what actual customers recommend.

Certificate Lifecycle Automation

Initially, teams can get by with manually managing certificates using spreadsheets. However, this process quickly becomes impractical and inefficient as thousands of certificates get added to your network.

While some vendors only specialize in certificate management and automation, others only provide the PKI. Vendors that combine these capabilities into one offering should take priority when evaluating solutions.

Ask Yourself

- How are we currently managing digital keys and certificates today?
- How many certificates are we managing today and estimate growth over 3 months, 6 months, 1 year?
- What challenges have we faced with issuing and locating certificates before they expire?
- What are some potential network or application outage costs to our business if a certificate expires?

Best Practice

Choose a Platform That Does it All

Make things easier for yourself and choose a solution that combines PKIaaS and certificate lifecycle automation into a single cloud-based platform.

In addition to managing certificates, this will allow you to:

- Enable end-to-end automation for all digital certificates
- Locate all keys and certificates across your entire enterprise
- Monitor the status of every certificate and get actionable reports in real-time
- Completely automate certificate requests and renewals

HOW SHOULD I EVALUATE A CLA SOLUTION?

Download the Buyer's Guide for Certificate Lifecycle Automation today.

LEARN MORE

Finding the Right Fit

Finding the right vendor to work with is just as important as the functionality of the product itself. Knowing that you have the right platform, people, and deployment model to support your specific business needs will ensure successful adoption.

Deployment Flexibility

Although this guide focused on PKIaaS, the greatest flexibility comes from solutions that can easily be deployed on-premises, in the cloud, delivered as-a-service, or with a hosted PKI. The ability to quickly deploy and scale an implementation that is aligned with your current technology stack is critical.

Platform Architecture

A modern, holistic approach to PKI and certificate management must be simple, modular and distributable. The vendor should allow you to deploy components throughout your network segments and cloud infrastructure without requiring significant changes to existing workflows or configurations.

Responsive Support

This one might sound obvious, but knowing you have access to PKI expertise is invaluable. Look for a vendor that can ramp up your team quickly, align resources, and set milestones for success. Inquire about 24x7 support, initial response times, customer satisfaction and retention scores, and references.

Depth in Expertise

PKI isn't just about technology; it's about finding the level of expertise to complete your project on time and in the right way. Look for vendors that don't just develop software, but also have hands-on experience in deploying and running PKI in line with best practices.

Scalable Licensing

When evaluating vendors, be sure that the licensing model is flexible and scalable. Some vendors charge per-certificate, or per certificate instance, rather than in bundles or packages that align with your certificate count. Licensing options should help you affordably manage every certificate today, and as your business needs grow, with a predictable cost structure.

Product Innovation

Rapid time-to-value is important. However, equally important is how the product will adapt and support emerging industry trends, such as IoT and quantum computing. Ask the vendor about their vision and mission for the product. Inquire about future product releases that will benefit you and your business.

Before Evaluating PKI as-a-Service

Once you've defined your solution requirements, it's time to prepare to evaluate potential products. Here are five questions you should be able to answer before you start:

1. What are the upcoming events that will impact your current PKI deployment that necessitate an evaluation (i.e. resource changes, business initiatives)?
2. What are the specific use cases or business requirements – both existing and future – that the solution must address?
3. How much can your organization invest in properly evaluating solutions against these requirements?
4. What are the criteria required for different user groups within the organization (e.g., PKI admins, developers, security analysts, network admins, endpoint users)?
5. What are the systems and applications within the organization that rely on the use of digital certificates (i.e., web servers, load balancers, firewalls, devices, containers, etc.)?

Next Steps

Choosing the right PKI as-a-Service combined with the best certificate lifecycle automation solution has never been more important to the security and continuity of your business. Let your use cases, team skill-sets, resource constraints, and risk exposure guide your selection process.

PKI as-a-Service

CA-provided tools are a step up from spreadsheets, but they will not address complex, multi-vendor environments and only offer limited discovery and management capabilities in comparison to full lifecycle management tools.

Learn more →

Certificate Lifecycle Automation

Only a limited number of certificates can be managed manually using a spreadsheet, but this process isn't scalable. It also only accounts for known certificates, leaving organizations with gaps in visibility.

Learn more →

What about SSH keys?

If you're looking for SSH key management, we've got you covered. Keyfactor can provide flexible modules to extend management capabilities across all of your cryptographic assets, including symmetric and SSH keys.

Learn more →

EVALUATE KEYFACTOR NOW

Do you want to learn more about how complete PKI as-a-Service and certificate lifecycle automation can help improve your security posture?

SPEAK TO AN EXPERT