EBOOK

Building the Business Case for a Cloud-First PKI Strategy

KEYFACTOR

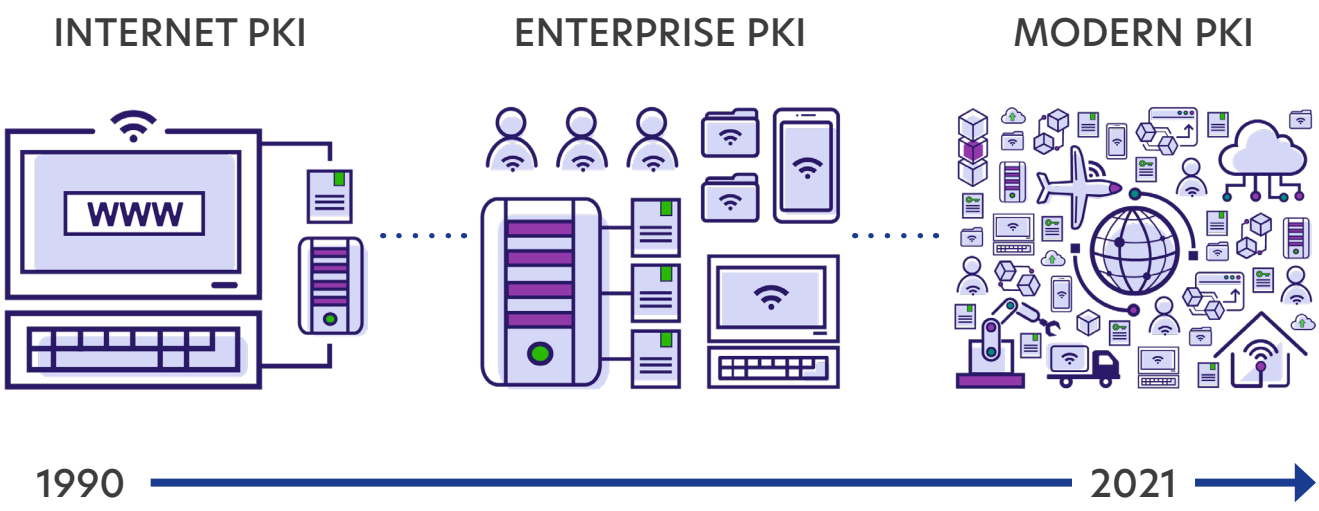
Table of Contents

Introduction

Public key infrastructure (PKI) is a core mechanism in enterprise security, serving as a building block of IT for more than two decades. Whether it's protecting a network, sensitive data, or a growing number of API-connected services, IT leaders have turned to PKI as a proven technology to establish digital trust in their business. In fact, getting PKI right can mean the difference between a highly secure environment and a serious breach.

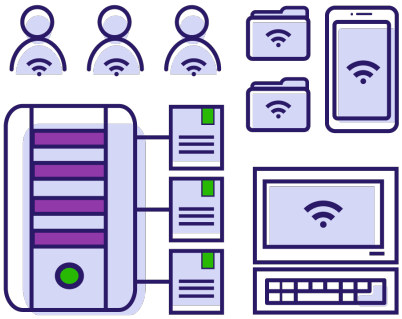
In the decades since its initial introduction, PKI has evolved considerably. The shift from network-defined trust to a focus on identity and data, the explosion of machine identities using keys and certificates, as well as increased risks due to shorter identity lifespans and evolving crypto-standards are just a few of the most recent changes to impact PKI programs.

In total, we've witnessed three distinct eras of PKI:



Internet PKI:

When the internet went mainstream in the 1990s, PKI offered a way to give websites a trusted digital identity. Specifically, it enabled us to put a digital certificate onto each website, that way when we went to Amazon to buy a book, we knew we were actually at Amazon's website. This era of PKI is defined by a limited number of public Certificate Authorities (CAs) and high-cost certificates, which were typically used only for websites and applications.



Enterprise PKI:

Next, corporations and large enterprises identified several practical ways PKI could help secure internal communications. These companies started to stand up privately routed PKIs to protect internal communications, authenticate applications, encrypt data on a device, and sign transactions digitally. This era of PKI is defined by privately deployed CAs that could issue a high volume of certificates at a low cost to secure users, devices, and internal company networks.

Modern PKI:

Today, corporations have gotten much more comfortable working with PKI and cryptography and now use it to secure all types of non-traditional IT devices, like those that comprise the Internet of Things (IoT). Think about sensors on a car, big machines, airplanes, and tractors, all of which have PKI on their electronic components. This era of PKI is defined by a multi-CA environment in which organizations issue more certificates with shorter lifespans to protect a variety of elements in the cloud and IoT and throughout DevOps processes.

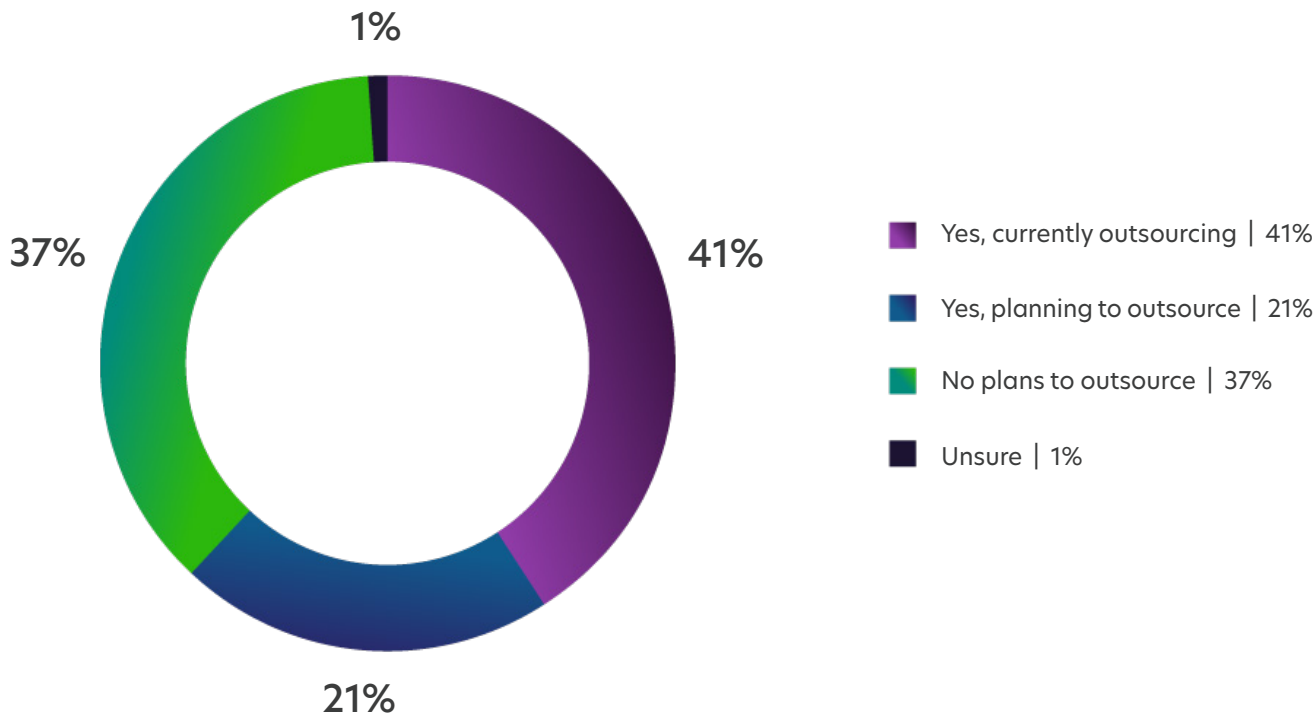
The result of this evolution is a much more complex PKI landscape, the scale of which is changing dramatically.

This eBook will explore the evolving complexity and costs of PKI, how to balance potential risks against those costs, and options for more modern PKI programs to help your organization build the business case for a cloud-first PKI strategy.

Would your organization consider outsourcing all or part of its PKI deployment?

According to the 2020 Keyfactor-Ponemon Report, most organizations have or plan to outsource their PKI deployment. Deploying and running a PKI in-house requires significant investment of resources — both human and capital.

62 percent of respondents say their organizations are currently outsourcing (41 percent) or planning to outsource (21 percent) all or part of their PKI deployment. Managed PKI or PKI as-a-Service solutions provide all the benefits of PKI, without the cost and complexity of running it in-house.



PKI is Hard & Getting Harder

Getting PKI right — namely protecting your organization without creating too much overhead for security and IT teams — has always been complex. However, the modern era of PKI is significantly more complex due to the growing scale of devices and machine identities, the speed at which they get created, and the unique nature of these entities.

This complexity often leads to costly mistakes when organizations introduce PKI, such as poor planning and design, overlooking the need for infrastructure to maintain the program, leaving the root CA and/or private keys unprotected, having insufficient training or expertise, and lacking proper certificate lifecycle planning.

To avoid these mistakes, your organization must seriously consider if you can effectively run a PKI program completely in-house. There are several complexities to evaluate as you make this decision.

The most important areas to consider include:

Personnel:

Do you have the right people on board? Do you have the deep PKI expertise that you need to design, architect, and deploy a modern PKI program?

PKI is a multi-faceted system that requires specialized expertise and dedicated IT staff to plan, build, and maintain throughout its lifecycle.

Infrastructure:

Do you have the right infrastructure in place? Can your data center support the needs of a highly secure and complex PKI program?

Remember: PKI is more than just implementing CA software — it's a comprehensive set of hardware, standards, backups, and certificate policies that require constant diligence.

Security and Operations:

Do you have the right people, processes, and systems in place to properly operate a PKI the way it was modeled and designed and to issue all of the necessary certificates?

Achieving appropriately high levels of security within your existing IT infrastructure can be challenging and expensive — especially if you're not prepared for everything it entails.

The Cost of On-Premise PKI

On top of the complexities of running a PKI program, hosting this program on-premise can prove quite costly. The cost of ownership for on-premise PKI centers around deployment, labor, and infrastructure needs.

Deployment Costs

In general, PKI has a high deployment cost, and that expense only increases if your organization is starting from scratch with PKI.

While it might seem simple to do something like install a Microsoft Trusted Root Program, the realities of PKI for today's enterprises are much more complex and, therefore, costly.

Deployment costs come from:

- Engaging PKI consultant services
- Leading PKI architecture and use case planning
- Deploying the initial installation
- Creating certificate policy and certificate practice statement (CP/CPS) documents
- Running a root signing ceremony

Labor Costs

Given the deep expertise required to maintain an effective PKI program, the labor costs of doing so can add up quickly.

Ongoing maintenance for a PKI program gets particularly involved for on-premise programs, since they involve managing schedules and maintenance for offline roots and manual reporting. These costs are long term, so it's important to consider how they will grow over time alongside your PKI program.

Labor costs come from:

- Finding and retaining skilled PKI staff
- Leading internal training for PKI admins
- Offering any required end user support
- Maintaining Certificate Revocation Lists (CRLs) and Online Certificate Status Protocols (OCSP)
- Managing the root and issuing CA renewals
- Handling server management, such as backups and patching

Infrastructure Costs

Finally, on-premise PKI programs require significant infrastructure to properly run and maintain. This infrastructure falls into two buckets: Security and hardware/software.

Security Costs

In terms of security, following best practices to run a secure on-premise PKI program involves efforts like placing offline root CAs in a vault within a cage in your data center and ensuring that your data center has the proper controls around who can access it. It might even involve installing video surveillance on your vault to ensure that if anyone is accessing it, you have evidence as to who that was and what they were doing. All of those things, especially when implemented across a multi data center model that includes multiple PKI environments or geographically distributed PKI environments, can make a big difference when it comes to infrastructure costs to build that security.

Security costs come from:

- Introducing high security data center facilities for any root CAs
- Managing biometric controls for data centers
- Implementing security personnel and/or video surveillance
- Purchasing a high-grade fire-proof safe for root key material
- Introducing tamper-evident bags and seals
- Handling environmental requirements, like power and cooling

Hardware & Software Costs

In terms of hardware and software, you need to consider everything from the hardware security modules (HSMs) to the hardware and backup software, data storage, and virtualization platforms on which you run your PKI. For instance, putting your PKI on a virtualized infrastructure and then backing it up with your backup solution comes with several costly security considerations. In this case, you have to not only consider PKI admins, but also anyone who has access to the backup data and anyone who can run exports of those virtual drives.

Hardware/Software costs come from:

- Introducing a root CA HSM and lockable storage case
- Implementing an HSM for issuing CAs
- Managing any hardware or cloud infrastructure to host servers
- Introducing server software, such as hypervisors, OS, SQL licenses, AV, backups, monitoring, and SIEM
- Handling yearly vendor support contracts for all hardware and software

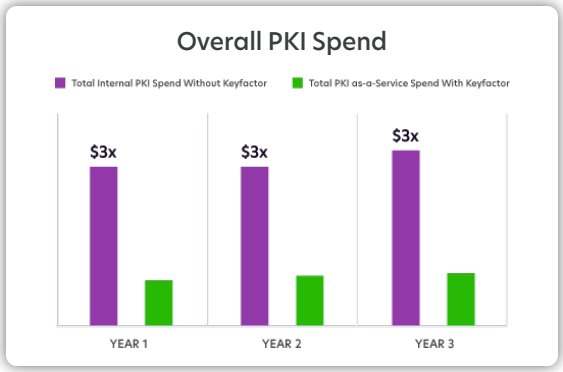
Business Case from a Global Healthcare Company

When a global healthcare company realized their current PKI was not meeting their enterprise standards, they developed a business case for PKI as-a-Service to scale with their rapid growth of certificates over a ten-year period.

This business case showed executive leadership that without proper PKI in place, their business would be susceptible to loss of reputation, business outages and fines.

Core Challenges & Business Impact

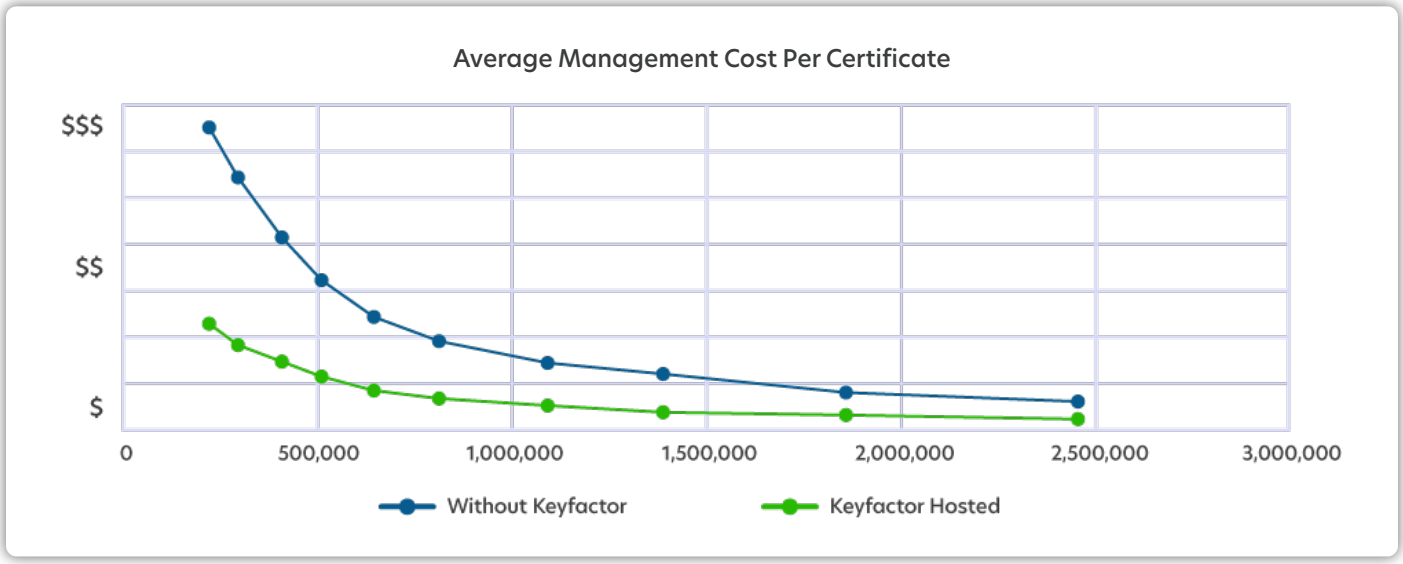
- → No central PKI and machine identity management engineering team
- → Inability to protect or revoke certificates on-demand due to poor visibility
- → No scanning abilities to discover and automate certificate lifecycles
- → No automation leads to high risk of outages and downtime
- → Unable to support and create policies to block data risks and enhance operational activities
- → Minimal continuity plan in place for PKI environment



Weighing the Costs

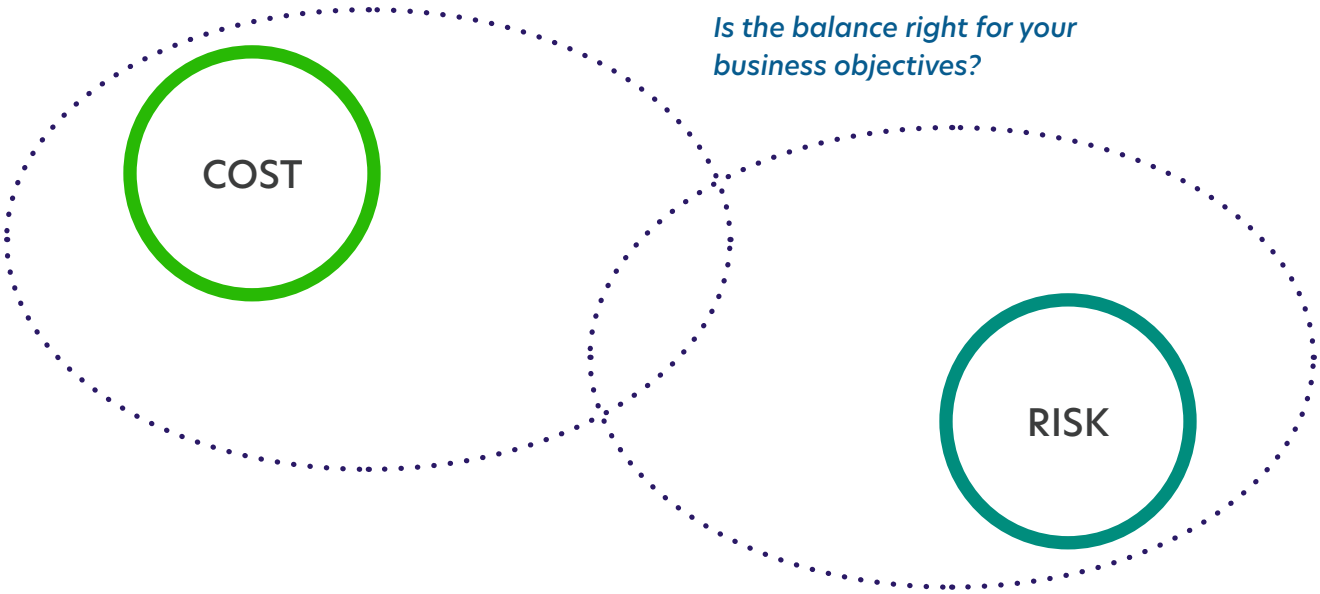
To estimate the total cost of ownership (TCO) of their on-premise PKI compared to PKI as-a-Service, this company compared the average management cost per certificate to each deployment model.

The results showed that investing more into their current on-premise PKI would cost three times more than shifting to a cloud PKI as-a-Service.



Evaluating Risk vs. Cost for PKI

When most organizations look at the impact of implementing PKI and the associated costs, they typically want to do two things: Lower costs while increasing security to ensure they meet PKI best practices. However, doing both simultaneously is often contradictory, since the more you increase security by putting additional controls around your PKI program, the more costs you're likely to incur for those controls.



The Risk of Lowering Costs

Because hosting PKI on-premise is so expensive, companies often look for ways to lower costs. Unfortunately, this typically leads to shortcuts in required security components and processes that increase risk.

The Cost of Reducing Risks

Meanwhile, because the security risks are so high, companies also want ways to decrease any potential vulnerabilities. But adding more controls typically drives up the cost of implementing in-house PKI considerably.

As a result of this situation, the goal of lowering costs while increasing security is rather difficult to achieve — at least in a traditional on-premise environment.

THE BENEFITS OF CLOUD PKI

Lowering Cost and Risk Simultaneously

Cloud PKI solves the problem of balancing cost vs. risk. Cloud PKI can strike this balance because it allows organizations to take advantage of economies of scale, or the ability to take the costs of implementing PKI and spread them across multiple organizations.

As a result, cloud hosted PKI allows for increased security (including high levels of security that most organizations can't perform internally — or that would be expensive if they can) at a lower cost compared to implementing an on-premise PKI program.

How Cloud PKI Lowers Costs

Because it is core to their business, cloud providers can commit far more resources to state-of-the-art PKI infrastructure, security, and operational excellence.

How Cloud PKI Lowers Risks

Since the cost of secure facilities and operations is shared by customers, cloud providers can offer the same level of security for a lower cost compared to any one organization implementing PKI individually.

Your Options for PKI

With all of that in mind, what are your options for introducing a PKI program? And which one is right for your organization? Three options currently exist:

On-Premise, In-House PKI

Maintain and run your PKI internally with your own resources. This approach typically leads to both high costs and high risks due to complexities around personnel, infrastructure, and security and operations.

On-Premise, Managed PKI

Maintain your PKI on-premise but hire experts to run it for you. This approach helps ease risks compared to running it in-house, largely due to improvements in personnel and operations, but has high costs since it requires bringing on an external team and maintaining the same on-premise infrastructure and security.

Cloud PKI (PKI as-a-Service)

Host your PKI in the cloud and have it managed by a team of experts. This approach reduces both cost and risk due to the economies of scale cloud providers can offer for infrastructure and security and the expertise provided by the team managing it.

The Benefits of Cloud PKI as-a-Service

Based on these options, cloud PKI built on Microsoft Azure provides clear benefits in terms of both reduced costs and reduced risk. However, it does represent a change, causing many organizations to question if the move is right for them.

The best way to evaluate if cloud PKI as-a-Service is right for your organization is to consider where you currently fall on the cost vs. risk balance scale. For example, does your organization make security compromises that reduce protection in order to meet lower cost requirements? If so, then it's worth investigating if cloud hosted PKI is a better fit for your environment.

Beyond the better cost vs. risk balance, some of the biggest benefits of introducing cloud PKI as-a-Service extend across multiple business teams.

For PKI Teams

Less backend maintenance, which leads to more time to focus on proactive priorities.

For Infrastructure Teams

Less time and money spent maintaining PKI infrastructure.

For Security Teams

A better guarantee that the PKI program will operate according to industry best practice and compliance requirements.

For DevOps Teams

The ability to easily integrate with DevOps toolsets and tap into a highly scalable infrastructure to match the speed of today's DevOps environments.

How to Evaluate PKI as-a-Service

Once you build the business case for cloud PKI, you still have decisions to make around which PKI as-a-Service provider is the best partner for your organization. The following evaluation criteria can help with this decision:

PKI as-a-Service Evaluation Checklist

Offline Infrastructure

- [ ] Highly-secured Offline Root CA
- [ ] Ability to retain control over Root CA keys
- [ ] Secure storage facilities and monitoring
- [ ] Controlled physical access

Cloud Infrastructure

- [ ] No shared infrastructure (dedicated PKI)
- [ ] SLA-driven CA and CRL availability
- [ ] Built-in certificate lifecycle automation
- [ ] Scalable infrastructure and cost model

Compliance & Operations

- [ ] SOC 2 Type II Certification
- [ ] Robust CP/CPS framework
- [ ] Root signing ceremony
- [ ] Regular PKI health checks

Implementation & Delivery

- [ ] 24x7x365 service monitoring
- [ ] SLA-driven incident response times
- [ ] Proven record of PKI expertise and delivery
- [ ] Continuous updates in hardware / software

What to Avoid

- [ ] Don't give up control of your root CA and key material
- [ ] Steer clear of shared infrastructure and multi-tenant environments
- [ ] Avoid standalone MPKI — look for certificate management included
- [ ] Avoid costly per-certificate pricing models
- [ ] Ensure in depth PKI expertise

1. Offline Infrastructure

What offline infrastructure does the partner offer? This evaluation point is important to understand the security of your root CA. Specifically, you should look for a partner that offers highly secure storage facilities for your offline root CA, including monitoring capabilities and controlled physical access.

It's also essential that your organization can retain control over the root CA key(s). This ownership is especially important because if you choose to switch providers, then you can take your root key with you and host it elsewhere or even host it yourself. Many organizations will try to lock you into a situation that makes it difficult to leave them because they own the key, so if you want to leave you're forced to reissue all your certificates — which involves significant work to say the least.

2. Cloud Infrastructure

Next, consider the cloud infrastructure each partner can offer to support your PKI program. On this point, you need to look at service level agreements for CA and CRL availability as well as built-in certificate lifecycle automation.

Equally as important is the ability to scale the infrastructure and cost model over time as your organization's needs evolve. While this scale is important, it's also critical to ensure that the partner offers a dedicated PKI without any shared infrastructure across client organizations. Avoiding this type of shared infrastructure/multi-tenant environment is the best way to guarantee that everything is isolated and secure just for your organization.

3. Compliance and Security Operations

Given that PKI is meant to increase security, it's also essential to make sure any partner meets the highest standards for compliance and security operations. This should include SOC 2 Type II Certification for trust services and a robust CP/CPS framework.

The partner should also offer a root signing ceremony to ensure integrity of the root CA and conduct regular PKI health checks for ongoing security.

4. Implementation, Delivery and Support

Finally, you need to evaluate what each partner offers in terms of initial and ongoing services and support. Ideally, you want a partner that offers 24x7x365 service monitoring and SLA-driven incident responses. As part of this, you should also consider each partner's pricing model upfront. You'll want to avoid any partners that offer a per-certificate pricing model, as this can become very expensive quickly and is not a scalable solution in the long term.

It's also critical to select a partner with deep PKI expertise and a proven record of successful PKI deliveries. This expertise should come through in the strategies and services offered as well as the partner's continuous updates to any hardware or software offered.

Ready to Simplify Your PKI?

It's time to rethink how you're deploying and managing your PKI today.

You already know that PKI is critical to your enterprise security, but setting up the infrastructure and hiring the skilled personnel needed to build, operate, and maintain it 24x7x365 is no easy task.

With security teams under increasing pressure, they need a new cloud-first approach to simplify and scale PKI on demand.

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

Built on Microsoft Azure