Cloud PKI: A Better Fit for Financial Services

Cloud PKI Delivers Security at Scale. Here’s How.
Protecting Data on Financial Networks with Public Key Infrastructure

The need for organization-wide encryption, at rest and in transit, has never been more urgent. That urgency is especially acute in industries like banking and financial services, which not only handle people’s most intimate data but are the target of relentless cyber attacks.

The Financial Services Information Sharing and Analysis Center, or FS-ISAC, recently concluded that cybersecurity is no longer just a back-office expense; cyber threats now pose critical business risks. The average cost of a data breach, meanwhile, is an eye-popping $4.24 million.

In this landscape, Public Key Infrastructure (PKI) has emerged as the gold standard for securing information across networks — and a critical piece of cybersecurity infrastructure. Deploying PKI enables companies to authenticate and authorize users, servers, applications and devices as well as robustly encrypt all data and communication between them. PKI and digital certificates are also key to implementing Zero Trust architecture, which is widely recognized for its power to protect against data breaches.
Cybersecurity Moves to the Cloud

Yet while PKI is an established and widely available technology, not all PKI solutions are equivalent in terms of complexity and cost.

On-premise PKI systems that rely on services like Microsoft Certificate Authority (MCA) and Active Directory Certificate Services (AD CS) are popular choices. However, cloud-based PKI solutions, commonly referred to as PKI-as-a-Service (PKIaaS) are quickly gaining ground, not least of all for their ability to integrate seamlessly with existing systems and relieve overstretched IT resources.

In this eBook, we’ll take a closer look at these trends — and discuss why cloud PKI is well-suited to the banking and financial services environment.
The Case for Cloud-Based PKI in Financial Services

In many industries, cloud technologies have been standard for more than a decade. Yet financial intuitions are only just starting to embrace the many benefits they offer. Cloud solutions help institutions increase agility and respond to changing customer needs. Because they are easier to scale than their on-premise counterparts, cloud systems also offer a lower-risk environment for piloting new concepts — and can be implemented at a cost that’s both predictable and easily adjusted to fit changing business needs.

Yet many institutions have struggled to migrate in-house infrastructure to the cloud without disturbing existing workflows. In the case of PKI, it’s not always easy to transfer private keys without disrupting carefully structured root hierarchies. In fact, with traditional cloud-native providers, it’s not even possible.
The Rise of Hybrid Cloud Infrastructure

The difficulty of migrating existing systems to the cloud has driven interest in so-called **hybrid cloud infrastructure**, where applications are deployed across a number of different environments, including both public cloud networks and on-premise servers.

In a hybrid cloud PKI setup, PKI management services are hosted in the cloud and delivered through a SaaS portal and RESTful API. Private root keys, however, are stored offline — ideally in a disaster-proof data center that’s managed by an experienced PKI service provider. This delivers a number of benefits:

- A user-friendly interface centralizes the process of creating, managing and distributing PKI keys
- Automation streamlines the complexity of renewing and retiring certificates
- An on-demand fee structure simplifies budgeting
- Private root keys aren’t exposed to online threats

Given the benefits, it’s no wonder that hybrid cloud is the most popular architecture among the financial services companies that deploy cloud technology as part of their primary computing infrastructures.

We’ll review best practices for hybrid cloud PKI architectures in the coming pages. First, it’s worth examining what makes on-premise PKI so problematic for most financial institutions.
The Trouble With On-Prem PKI

McKinsey research suggests that many companies prefer to manage PKI infrastructure on-premises. Yet there are a number of challenges with that arrangement:

- **Management is Difficult** — PKI requires organizations to manage hardware, software, policies and procedures for the hosting infrastructure, which is very complex. On top of it, creating, storing and distributing digital certificates to devices adds even more complexity, especially considering that the average organization must manage more than 56,000 certificates!
- **Costs are High** — The cost of computing has fallen, but servers and hardware security modules (HSMs) are still a major business expense … to say nothing of the resources you’ll need to make sure they’re properly updated and securely backed up and maintained.
- **Audits are Complex** — Regulatory audits are a massive undertaking in financial services, and every piece of security infrastructure adds a new layer of cost and complication.
- **Expertise is Hard to Find** — The expertise needed to manage PKI certificates is in short supply. In fact, 52% of security professionals said their top challenge was a lack of understanding of their PKI’s security capabilities. Smaller financial institutions, which may only have a handful of IT resources, find it especially difficult to recruit and retain the talent they need to manage PKI certificates.
- **Security is Challenging** — A lock offers no protection if its key is not secure. Private PKI keys must be protected offline, in ultra-secure, audited facilities that are often impractical for financial institutions to maintain.
- **Infrastructure is Difficult to Scale** — New use cases for PKI are emerging every day. But expanding in-house PKI isn’t as simple as adding a new server. Most PKI deployments were built for specific use cases, and can’t handle the volume of certificates required to take full advantage of the technology’s capabilities.
- **Crypto-agility Requires Major Changes** — Cryptographic standards have changed a lot in the 20+ years that PKI has been around, and they continue to evolve to meet new threats. Yet too often, organizations can’t take advantage of these developments without major changes to their infrastructure. As quantum computing is becoming reality, organization must be prepared to implement post-quantum cryptography algorithms.
According to Gartner, IT infrastructure outages can cost businesses thousands of dollars per minute. Severe network outages can take days to resolve, causing millions of dollars of damage.

Certificate-related outages can be especially problematic — as the still-chilling 2017 Equifax breach illustrates. That spring, thanks to a newly discovered security vulnerability and an expired certificate on the device inspecting encrypted network traffic, a digital attacker cracked into Equifax systems and remained undetected for the next two and a half months. The settlement, which is still ongoing, cost the company up to $700 million and untold reputational damage. In the case of server and infrastructure management in-house, Equifax made headlines again in 2022 when miscalculated credit reports were presented to consumers and lenders due to a coding issue in a legacy, on-premise server that was slated to be migrated to a cloud infrastructure. While the miscalculations were a result of a mistake made by Equifax's technology team, reports that were generated during the span of three weeks ultimately affected final lending decisions and interest rates for consumers who were already at the closing table.

In recent years, dozens of organizations have suffered breaches and service outages as a result of expired and mismanaged PKI certificates. In the case of on-premise server or infrastructure maintenance, human error remains a risk, and in some cases, could have implications on factors like customer creditworthiness, sensitive data, and more.
The Benefits of Cloud PKI

PKIaaS enables organizations to outsource the complexities of PKI while retaining control of private trust assets and visibility through a centralized management portal. Other benefits include:

- **Simplicity** — Best-in-class managed PKI systems streamline security workflows by providing a single, intuitive interface that gives executives real-time visibility into the status of all certificates across the enterprise.

- **Speed** — Cloud PKI can be integrated into existing security systems within a matter of days, rather than the months to years it takes to build in-house infrastructure. New use cases can be added just as quickly, making the solution far simpler to scale.

- **Agility** — Institutions can add capacity and expand use cases without major infrastructure investments or concerns about broader system stability. That makes cloud PKI perfect for rapidly changing business environments.

- **Security** — On-premise PKI puts an enormous burden on IT teams to adapt systems to a fast-evolving threat landscape. Managed PKIaaS vendors, by contrast, deliver best-in-class security practices without the additional headache.

- **Compliance** — Fragmented regulations make it difficult for financial institutions to adopt some cloud technologies. Yet the compliance of PKIaaS with regulations like the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, and the System and Organization Controls 2 (SOC 2) is well established. What’s more, moving PKI to the cloud also streamlines the audit process. Experienced PKIaaS vendors participate in dozens of audits per year and can fit seamlessly into clients’ audit cycles.

- **Cost** — Cloud-based PKIaaS reduces costs by eliminating the substantial expenses related to maintaining robust on-premise PKI infrastructure, from hardware and failover software to audits and salaried experts. What’s more, PKIaaS pricing is consistent and predictable, simplifying the budgeting process.

PKIaaS also supports Zero Trust environments by securing authentication and communications between machines, devices, IoT and virtual servers.
Why are Financial Institutions Turning to Cloud PKI?

Data is the lifeblood of the financial services industry. Threats to financial data come from every direction — and will continue to do so, given the proliferation of employee devices and work-from-anywhere arrangements.

Cloud PKI makes it easy to protect all these devices — and comply with the stringent security regulations that bind the industry. What’s more, powerful new uses cases for the technology are emerging all the time. Financial institutions rely on PKI to:

- Power passwordless authentication for users and devices
- Secure internal users, devices and applications through private certificates
- Secure website with public trust TLS/SSL certificates
- Prevent Business Email Compromise (BEC) by signing and encrypting email with S/MIME certificates
- Establish trust with customers and partners through Extended Validation Code Signing certificates
- Digitally sign documents with identity-based document signing certificates.
Best Practices for Cloud PKI

Hybrid cloud architectures are ideal for PKI. Beyond that, financial institutions should look for vendors that maximize security and streamline compliance by:

- Generating and storing private keys offline, in fully air-gapped systems
- Using a separate security world for each customer, storing private keys in a Hardware Security Module (HSM) that’s unique to each
- Using M of N controls to maintain a segregation of duties to authorize root key generation
- Protecting private keys at a vault in a disaster-proof granite mountain, according to Department of Defense (DOD) specs
Case Study: North American Credit Union Goes Cloud

A $1B North American credit union was looking for a cost-effective way to encrypt all data flowing into and within its network. A management consultant recommended PKI, but with only 500 employees — and an IT team of just three people — executives knew they lacked the expertise to establish, host and manage the infrastructure in-house.

However, executives were also uncomfortable with the idea of hosting PKI in the cloud and losing control of their private keys. That’s why they selected HID Global’s hybrid cloud PKIaaS, which enables them to host private keys on premise and put everything else in the cloud. The HID PKIaaS management portal gives executives complete visibility into the status of all keys and certificates, while the on-premise architecture enables them to access private keys at any moment and maintain root hierarchies.

“HID Global’s Public Key Infrastructure-as-a-Service (PKIaaS) helps organizations experience all the benefits of having an internal PKI without needing to manage the infrastructure. The company offers a one-stop global solution for PKI services across an enterprise in the long term.”

Swetha Krishnamoorthi,
Senior Industry Analyst, Cybersecurity at Frost & Sullivan
Maximizing Security, Minimizing Complexity

PKI’s complexity should not prevent financial institutions from taking full advantage of its capabilities. PKI is a versatile solution, able to efficiently secure users, devices and applications and encrypt all communication between them. Moving it to the cloud makes the technology as convenient as it is powerful. Cloud PKIaaS streamlines IT workflows while controlling costs and complying with strict regulations — a perfect fit for financial services.

Learn more about the power of PKI:

- Dive deeper into how PKI is being deployed in financial services and other industries in our Case Study Collection.
- Get tips on finding the perfect fit for your organization in our eBook, PKI Automation Strategies.
- Book time with one of our PKI-as-a-Service experts to discuss your business needs.