From Spreadsheet Chaos to Crypto Control: Your Guide to Future-Ready PKI

BUYER'S GUIDE

From Manual Mayhem to Managed Trust: Future-Ready Your Posture with HID PKIaaS

Spreadsheets, missed renewals, and human error are no match for today's fast-paced, high-stakes digital environments. As certificate lifespans shrink and quantum threats loom, organizations need more than just visibility—they need control.

HID PKI-as-a-Service (PKIaaS) offers a smarter, scalable way to manage public trust TLS certificates and private trust certificates. By automating certificate lifecycles and eliminating manual processes with PKIaaS, your team gains freedom to focus on strategic priorities while reducing the risk of outages, compliance failures, and security gaps.

This guide will help you:

- Understand the benefits of PKIaaS
- Identify must-have features like Certificate Lifecycle Management (CLM), discovery, and Post-Quantum Cryptography (PQC) readiness
- Choose a provider that's built for the future

Let's find the right fit for your organization—before your next certificate expires.

"When implementing enterprise-level certificate life cycle management at scale across multiple PKIs and use cases, purchase of CLM tooling is likely unavoidable to deliver the capabilities required."

- Gartner, Buyer's Guide for PKI and Certificate Life Cycle Management, Sarah Almond, May 29, 2025

Organizations of all sizes and across all industries face a growing pressure to manage digital certificates more effectively. As certificate volumes grow, lifespans shrink, and threats evolve, PKI is no longer just an IT tool—it's a core enabler of digital trust.

Most enterprises share the same high-level objectives when modernizing their certificate lifecycle management (CLM) strategy:

- Eliminate unmanaged certificates to reduce unknown risks and gain visibility
- Support dynamic, hybrid environments with flexible issuance and revocation
- Reduce expiry-related outages through proactive lifecycle controls
- Lower operational overhead and free up valuable IT and SecOps resources
- Demonstrate and improve compliance with internal and external requirements
- Manage short certificate validity periods (now 90 days or shorter)
- Rationalize tooling and reduce platform sprawl—one pane of glass
- Enable crypto-agility to switch algorithms with minimal disruption
- Build resilience against compromise, outages, and unexpected change

These aren't theoretical targets—they are urgent, measurable goals that map directly to real business risk. Manual certificate management, however, is fundamentally incapable of supporting these objectives at scale.

	Features					
Objectives	**Discovery**	**Reporting**	**Notifications**	**Automation**	**Multi CA**	**Integrations**
Eliminate unmanaged certificates	■					
Support dynamic environments				■		■
Reduce expiry outages	■		■	■		
Reduce overheads				■		■
Improve compliance	■	■				
Manage short validities				■		■
Rationalize tools/single pane of glass					■	■
Improve crypto agility				■	■	■
Improve resilience	■	■	■	■	■	■

Source: Gartner
823796_C

Gartner, Buyers' Guide for PKI and Certificate Life Cycle Management, Figure 2:

In our opinion, Gartner's matrix makes one insight especially clear: achieving the most common CLM objectives depends directly on the presence of key automation features—discovery, notifications, integrations, multi-CA support, and especially end-to-end lifecycle automation.

Many enterprises rely on in-house solutions like Microsoft Certificate Authority and Active Directory Certificate Services to manage their PKI.

While this approach may seem cost-effective at first, it often leads to hidden complexity and mounting overhead.

Why Manual Certificate Management Can’t Keep Up

Complexity. Cost. Capacity. Private PKI needs a smarter approach.

Many organizations still rely on in-house solutions like Microsoft Certificate Authority (CA) and Active Directory Certificate Services (ADCS) to manage their private PKI. While this may seem cost-effective initially, it often leads to hidden complexity and operational strain.

Common challenges with in-house Private PKI include:

- High upfront investment in servers, HSMs, and enrollment infrastructure
- Ongoing maintenance costs for patching, compliance, and backups
- Resource drain as skilled IT staff are diverted from strategic initiatives
- Security pressure to stay ahead of evolving threats with constant monitoring
- Scalability issues as certificate volumes grow across users, devices, and environments

HID PKIaaS for private trust eliminates these burdens with a fully managed, scalable solution that integrates easily with your existing systems, enabling:

- Fast deployment without infrastructure headaches
- Simplified operations and reduced overhead
- Centralized visibility and control
- Crypto-agility and PQC readiness for future-proofing

Private PKI is essential for internal systems, IoT devices, and secure communications—but manual management is no longer sustainable.

Public TLS/SSL Certificates at Scale: Why Automation Is Essential

Shorter Lifespans. Higher Stakes. Automation is now a necessity.

With the CA/B Forum's newly introduced schedule that reduces public TLS certificate lifespans down to 47-days by 2029, manual in-house certificate management is no longer sustainable, meaning the time to start thinking about automation is now.

Key challenges with Public PKI include:

- Frequent renewals: With 47-day certificate lifespans, certificates must be replaced up to 6–8 times per year
- Risk of outages: Missed renewals can lead to service disruptions and compliance failures
- Operational burden: Manual tracking and renewal is time-consuming and error-prone
- Need for automation: Timely issuance, renewal, and revocation require end-to-end lifecycle automation

HID Enterprise SSL-as-a-Service helps organizations:

- Automate certificate lifecycles to eliminate human error
- Manage both public and private certificates form a single pane of glass
- Maintain compliance with industry standards
- Scale certificate management across domains, users, and services

Public PKI is foundational for external trust—but without automation, it becomes a liability.

With the CA/B Forum's shorter certificate lifespan officially mandated, automation has moved from **best practice to baseline**. But it doesn't stop there — crypto-agility and PQC-readiness must now enter every security team's roadmap.

HID

SPOTLIGHT ON MOBILE DEVICE MANAGEMENT (MDM) WITH MICROSOFT INTUNE

Connector models place certificate management at the center of a constantly flowing circuit with several components:

- Mobile devices request certificates from the provider's servers
- The server requests authentication from Azure Active Directory (AAD)
- AAD sends a token through the server to Microsoft Intune
- Microsoft Intune validates and decrypts data and approves sending certificates

Interested in learning more about automation models? **Explore our infographic for an at-a-glance comparison**.

Automation is No Longer Optional

With certificate lifecycles moving towards 47 days, manual management is unsustainable. Automation is mandatory to ensure timely issuance, renewal, and revocation, reducing the risk of outages and compliance failures. Automating your PKI certificate lifecycles starts with finding the right automation model. There are three common methods:

Vendor Specific Models

This model installs a specific agent on each device, which communicates with the central management console to track and manage certificate lifecycles. This agent is proprietary to the management provider, and each platform requires a different agent.

Vendor Agnostic Models

Vendor agnostic models don't directly install software onto user devices. Instead, the device communicates directly with the management console through the cloud. The device's privileged information — IP addresses, usernames and passwords — are stores on the host server and used to perform certificate lifecycle events.

Connector Models

Connector models, like HIDs PKIaaS, leverage open-source certificates, allowing customers to choose the appropriate certificate based upon their operation system and tool set. These connectors manage certificates independently, eiminating the risk of centralized console failure. They are also vendor agnostic, allowing organizations ownership and control of certifictes, even if they move to a different provider.

HID

Your Checklist for Selecting a Future-Ready PKI Provider

To keep pace with shrinking certificate lifecycles and increasing operational demands, organizations need a PKIaaS provider that delivers efficiency at scale. Use this checklist to evaluate providers based on automation, lifecycle management, and seamless integration with your existing infrastructure.

CERTIFICATE DISCOVERY

Will you be able to automatically discover and inventory certificates across all environments?

CERTIFICATE LIFECYCLE MANAGEMENT

Does your provider offer end-to-end CLM for automated issuance, renewal and revocation?

POST-QUANTUM CRYPTOGRAPHY READINESS

Does the provider offer crypto-agility to switch algorithms without disrupting operations?

EASY, FAST DEPLOYMENT

Will your PKIaaS service be fully functional and operational in days — or months?

CONTROL OF YOUR ASSETS

Will you own your private keys — and be able to take them with you?

SCALABILITY FOR THE FUTURE

Can you add new use cases as needed — without a hefty fee per certificate?

GUARANTEED SLA

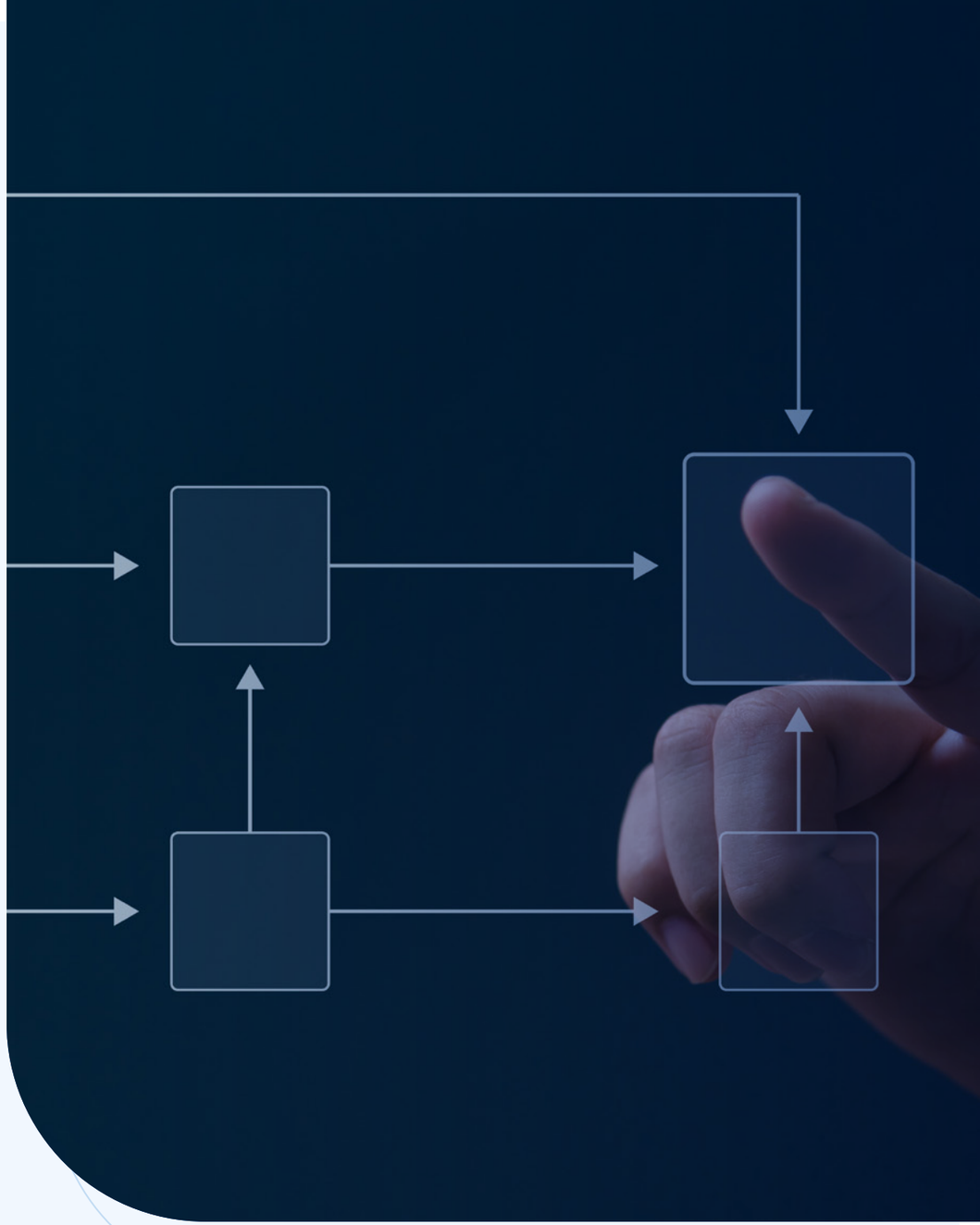
Does the provider guarantee an SLA upwards of 99.9% — or much lower?

GEOGRAPHICAL DISTRIBUTION

Is data stored regionally with redundant architecture — or in one vulnerable place?

CUSTOMIZATION

Can you design and customize certificate hierarchy and profiles to support any use cases?



HID

Preparing for the Post-Quantum Era: Why PQC Belongs on Your PKI Roadmap

"PKI and CLM roadmaps should take this into account including the required visibility and agility to support such a migration." "Postquantum readiness also hinges on visibility and agility, but across all cryptography usage."

— Gartner, Buyers' Guide for PKI and Certificate Life Cycle Management, 2025

The Reality:

Quantum computers are advancing—expected to break RSA and ECC algorithms by 2029 (NIST)

NIST has standardized PQC algorithms: In August 2024, NIST approved the first four post-quantum algorithms for Federal Information Processing Standards (FIPS).

What are Your Organizations Needs:

- **Visibility:** Know where legacy cryptography is used
- **Agility:** Transition seamlessly without service interruption
- **Automation:** Reissue and rotate at enterprise scale
- **Post Quantum Computing Support:** Capability to adopt new PQC algorithms rapidly

From Risk to Resilience: How PKIaaS Strengthens Compliance

Compliance is no longer a checkbox—it's a continuous process. A modern PKIaaS provider should support evolving standards, offer detailed audit trails, and ensure alignment with industry regulations. Look for capabilities that reduce compliance risk while simplifying reporting and governance such as:

FIPS 140-2/3 LEVEL 3 COMPLIANT HSM

This level of certification indicates strong security and implementation of best practices. As industry standards evolve, so should your provider's compliance roadmap.

M OF N SECURITY CONTROL MODEL OF OFFLINE ASSETS

Determine how many security controls are used by your organization and the provider.

OFFLINE AND ONLINE KEY MATERIAL BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER RECOVERY

Ensure they have a plan in place if the unthinkable happens.

STRINGENT SECURITY CONTROLS

High security standards and adherence to best practices mean compliance and quality. Look for a vendor with certifications such as SOC 2 Type 2 Compliance.

HID

Beyond the Basics: Evaluating Advanced PKI Capabilities

Your PKI provider should do more than issue certificates. Evaluate their technical architecture for scalability, high availability, and support for hybrid and multi-cloud environments. Look for advanced features like:

OUT-OF-THE-BOX INTEGRATION WITH ENTERPRISE TOOLSET

Can you plug-and-play the service, or will you jump through complex hoops?

SINGLE-VENDOR SIMPLICITY FOR PUBLIC AND PRIVATE TRUST CERTIFICATES

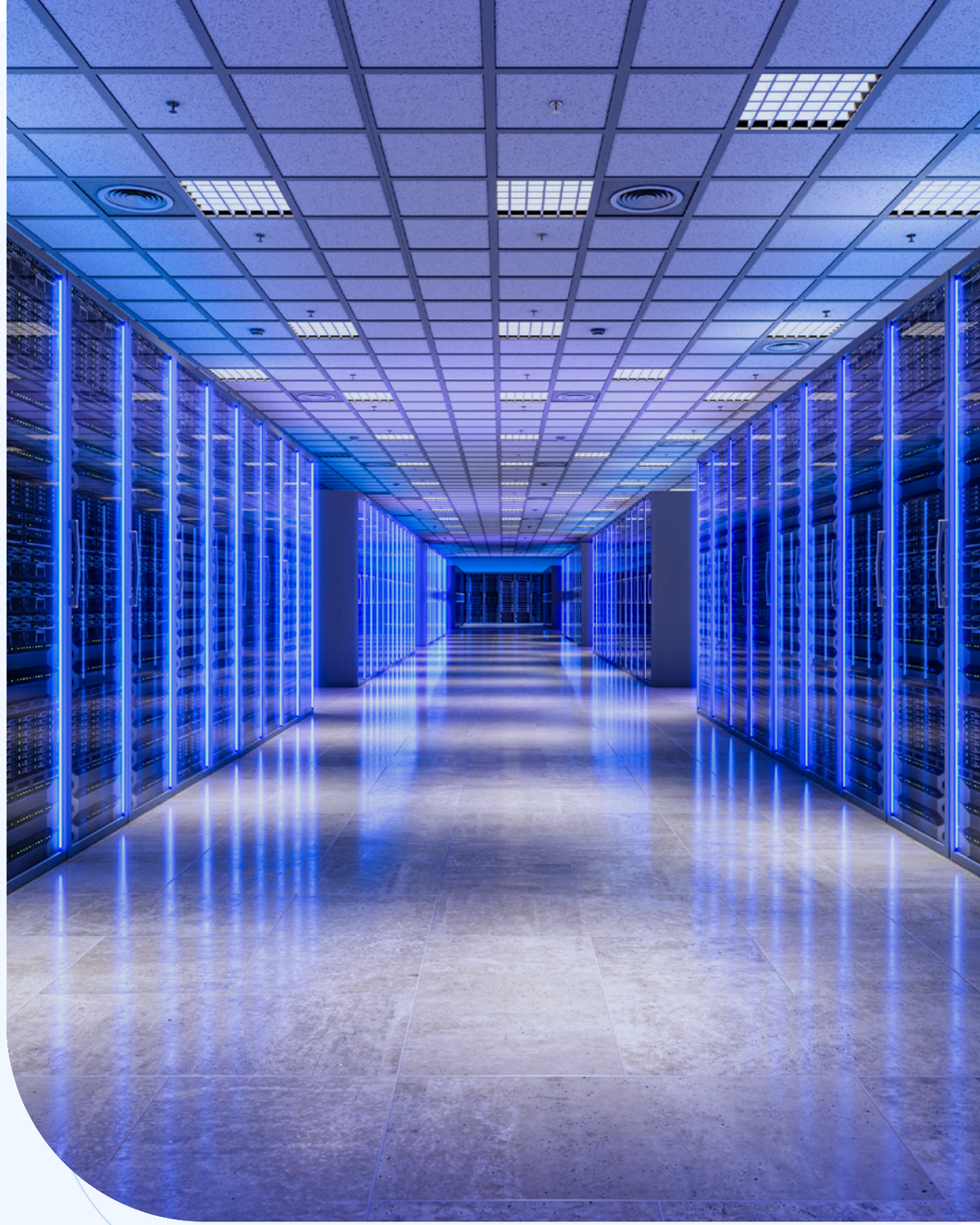
Are they a Swiss Army knife or just the scissors?

AUTOMATED CERTIFICATE LIFECYCLE MANAGEMENT FOR EVERY SYSTEM AND DEVICE

Can they cover everything, or will there be gaps?

HIGHLY SCALABLE CERTIFICATE VALIDATION THROUGH OCSP AND CRL

Will there be up to date certificate revocation information available?



Real Results, Real Flexibility, and Real Stories of Satisfied Customers

From transportation to manufacturing, organizations are rethinking how they manage digital trust. Whether replacing spreadsheets, scaling high-volume certificate issuance, enabling on-demand provisioning, or building private PKI environments, HID customers are solving complex challenges with flexible, automated solutions. These stories highlight how PKIaaS is helping teams across industries prepare for post-quantum cryptography (PQC), embrace crypto-agility, and take control of their certificate ecosystems—on their terms.

A global **utility company** needed a private PKI infrastructure to provide certificates for both their products and the tools that communicate with them. Their millions of devices required a highly scalable solution that would work with their existing systems.

Choosing HID PKIaaS meant fast certificate issuance, whether volume was high or low. This scalability also allowed them to use the solution without a significant upfront investment.

A **transportation company** was experiencing a rapidly expanding trusted SSL and user certificate infrastructure. They needed a full-service PKI provider at a predictable cost for on-demand issuance of certificates.

HID PKIaaS self-service console allows them to leverage their existing systems for easy certificate management — all with a predictable subscription model.

An **international gaming platform** was juggling high-volume internal certificate demands and multiple internet domains that all needed protection. They needed a fully branded private PKI solution with an offline root CA and multiple online issuing CAs.

HID PKIaaS works with their Venafi TrustAuthority key and certificate management platform to manage all their certificate needs under one vendor.

Future-Ready PKI Starts with HID PKIaaS. Discover the HID Difference today.

Managing PKI in-house can drain valuable IT resources—especially when organizations are responsible for maintaining infrastructure, ensuring compliance, and scaling to meet internal demands. Separately, the rise of short-lived public TLS certificates has introduced new challenges, requiring frequent renewals and robust automation to avoid outages and compliance failures. While some organizations turn to PKIaaS to offload this burden, not all providers simplify the process. Many introduce hidden complexity with per-certificate pricing, lackluster automation, or fragmented platforms that require juggling multiple vendors.

HID PKIaaS is different. It is future-ready by design.

HID PKIaaS is more than secure. It is designed to evolve— supporting the emerging use cases of today, the post-quantum standards of tomorrow, and the challenges of the future.

With HID PKIaaS, you receive:

- Seamless integration with your existing systems
- Customizable automation tailored to your workflows
- Scalable, flexible deployment across public and private certificates
- Global infrastructure for high availability and performance
- Predictable subscription pricing—no surprises
- Expert support from a team that understands your needs

Ready to learn more about PKIaaS from HID?
Visit our website or request a demo.

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

2025-08-12-iams-future-ready-pki-guide-en PLT-05875
Part of ASSA ABLOY