# PKIaaS Buyer's Guide

## Discover Certificate Control that Doesn't Control You

# Managing PKI is Complex — Make it Simple with PKIaaS

PKI-as-a-Service (PKIaaS) untangles the complex knots of Public Key Infrastructure (PKI), freeing up your IT team to focus on mission-critical tasks and eliminating the costs and risks of expired certificates. Certificate lifecycle automation is a must-have with today's ever-expanding device ecosystems, and organizations around the world are turning to PKIaaS providers to simplify their certificates.

Which provider is right for you?

This buyer's guide outlines the benefits of PKIaaS as well as the basics of selecting a PKIaaS provider with best-in-class service and the ability to meet your needs. Read on to discover what to look for, what to avoid and how to find your perfect fit.

For more on the benefits of automating PKI certificate management, read our white paper, **The Role of PKI in Protecting Enterprise Networks**.

HID

# Why PKIaaS?

Robust enterprises have robust IT teams — but even they have their limits. Some organizations opt to use services like Microsoft Certificate Authority and Active Directory Certificate Services to manage certificates in-house. Unfortunately, this has several drawbacks, including:

- Upfront costs for things like Servers, Hardware Security Modules (HSMs), Setup of enrollment, registration and templates etc.
- Ongoing costs, like those for maintaining compliance, deploying patches, data backup and management
- Key IT resources are pulled from mission-critical tasks
- Staying ahead of attackers requires constant surveillance
- Management becomes increasingly complex as additional devices and certificates are added

PKIaaS eliminates these struggles while providing seamless security — often working with systems your organization has in place already. This means easy, fast integration and simple management.

A recent survey by HID Global and Dark Reading found that **70%** of cybersecurity staff are stretched too thin, and **40%** anticipate increased security challenges in the near future — budgets and staff, however, will remain the same.

### 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 to the

Interested in learning more about automation models? Read our eBook, **PKI Automation Strategies: Finding the Perfect Fit for Your Organization.**

# Selecting an Automation Model

Automating your PKI certificate lifecycles starts with finding the right automation model. There are three common methods:

### AGENT MODELS:

This model installs an 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.

### AGENTLESS MODELS:

Agentless 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 stored on the host server and used to perform certificate lifecycle events.

### CONNECTOR MODELS:

Connector models, like HID Global's PKIaaS, use open-source certificate utilities that are already embedded into common platforms (like Microsoft Intune). These connectors manage certificates independently, eliminating the risk of centralized console failure. They are also vendor agnostic, allowing organizations ownership and control of their certificates, even if they move to a different provider.

# Selecting a Provider: Operational Efficiency

Gain certificate control that doesn't control you by asking about:

### 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 your own level of automation — or is it one-size-fits-all?

# Selecting a Provider: Robust Compliance

Achieve compliance by ensuring that your provider offers:

### FIPS 140-2 LEVEL 3 COMPLIANCE HSM

This level of certification indicates strong security and implementation of best practices.

### 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.

# Selecting a Provider: Technical Architecture

The right PKI automation provider applies best-in-class technology with unparalleled expertise. Look for technical architecture 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?

### PROVIDE TRUSTED SSL AND PRIVATE PKI

Do you have one-stop-shop service provider who can cover all your certificate needs?

### HIGHLY SCALABLE CERTIFICATE VALIDATION THROUGH OCSP AND CRL

Will there be up to date certificate revocation information available?

# Selecting a Provider: Flexible Solutions

Managed PKI shouldn't be one size fits all. Each industry has unique challenges, needs and concerns — select a provider with the flexibility to tailor a custom solution that works with your existing assets and investments. Here are just a few examples of PKIaaS by HID Global at work in diverse organizations:

A **financial services** organization was tied in knots dealing with multiple certificate providers and external websites, as well as inconsistent use of their internal certificate management programs. They already had Microsoft's Certificate Authority (CA)— but not the dedicated IT staff to manage it.

With PKIaaS from HID Global, they now have a single place to manage all their certificate types that works with their existing investments in staff, products and platforms.



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 Global's 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 Global's 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.

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

HID

# Make PKI Simple with PKIaaS from HID Global

Your IT team shouldn't have to shoulder the burden of Public Key Infrastructure and manual certificate management, especially with the prevalence of short-lived certificates and the increasing number of connected devices. PKIaaS ensures your cyber security posture stay up to date without additional cost or personnel — as long as your PKIaaS provider fits you, that is. Unfortunately, some providers only add to the complexity, tasking you with frustrating per-certificate pricing and one-size-fits-all automation, or leaving you to manage multiple providers for different certificate types and platforms.

PKIaaS from HID Global takes the complexity from managed PKI and turns certificate automation into a simple, secure and seamless machine. This unique managed PKI is:

Easily Integrated

Customizable Automation

Scalable, Flexible Solutions

Geographically Dispersed

Available for Public and Private Digital Certificates

Priced on a Subscription Plan

Serviced by Leading Experts

Ready to learn more about PKIaaS from HID Global?
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: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

**For more global phone numbers click here**



2021-04-08-iams-pki-certificate-control-rg PLT-05875

Part of ASSA ABLOY