AXIAD

PKI Modernization

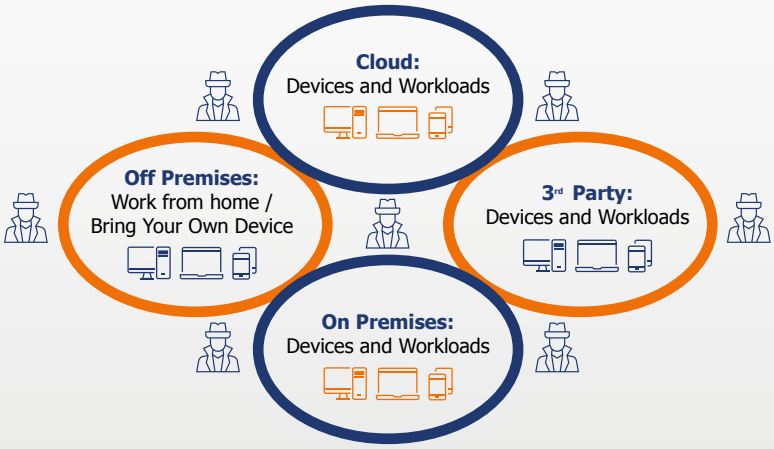
OVERVIEW OF USE CASE

The speed of innovation – whether for business or for a government agency – is increasing in terms of new online services, new combinations of goods, services, and partners, and new ways of looking at the world. This speed arises from more specialized devices, more sophisticated workloads, and more interdependencies based on electronic interchanges.

Devices critical to the organization are expanding:

- **Cloud:** Devices and workloads are increasingly being migrated to public and/or hybrid cloud environments.
- **On-premises:** While the strategic direction might be the Cloud, for security or pragmatic reasons (such as prohibitive cost of migration), many devices and workloads still remain on-premises.
- **Off-Premises:** Increasingly, organizations need to support Work from Home and personal Bring Your Own Device (BYOD) pools of devices.
- **3rd Party:** Since efficiencies arise from integrating with consultants, vendors, suppliers, and purchaser devices and workloads, 3rd party devices and workloads are increasingly becoming part of the environment.

Machine Security Exposure Surfaces Are Expanding



However, threat actors and online criminals are increasingly taking advantage of the expanding security exposure surface to execute a variety of attacks – such as Supply Chain, Adversary-in-the-Middle, and social engineering – that erode the digital trust that is absolutely required for innovation.

Public Key Infrastructure (PKI) provides the certainty and the ability for authentication to be automated at scale. But most PKI systems have been cobbled together over literally decades. The original architects have most often been replaced by high-priced consultants. As a result, most organizations do not have the deep PKI expertise needed to create a PKI infrastructure, to make it available globally, to operate it efficiently, and to maintain it over time.

A cloud-native PKI approach delivered as a service is an ideal foundation for organizations to provide best-practices machine and interaction authentication in a reasonable timeframe and without breaking the bank. This approach has the advantages of addressing hybrid needs (such as device validation and interaction validation) and providing consistency across entire environment.

The need to innovate at speed requires a modernized and unified PKI across the organization

CHALLENGES

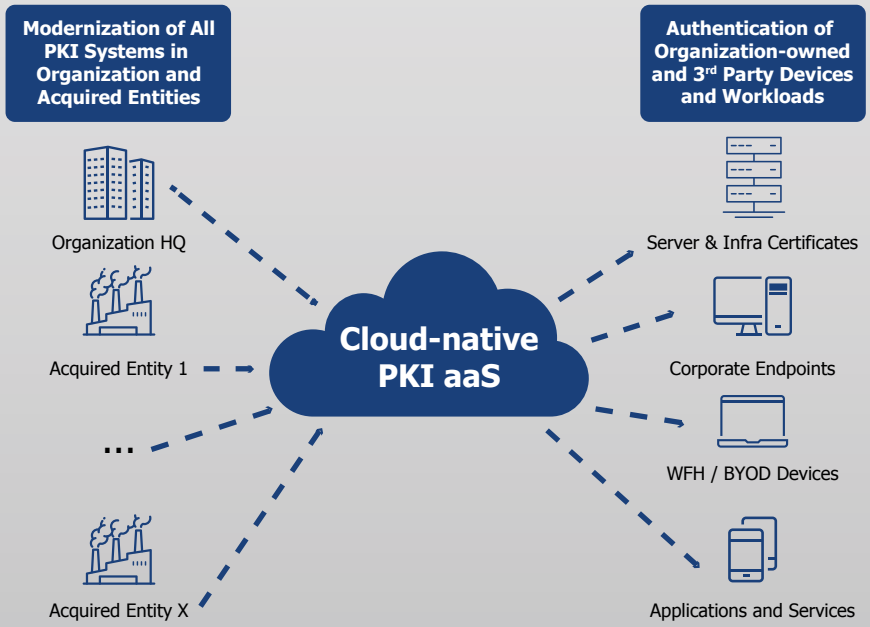
To achieve the needs outlined above, there are significant PKI challenges to overcome:

- **New Uses and Needs:**
  - **Expanded Device Pool:** Organizations want to authenticate remote, WFH, and 3rd party devices.
  - **Extend PKI to Virtual Entities:** Organizations want to leverage PKI for Virtual Machine, Container, and other non-physical entity authentication – but legacy systems may not have this capability.
  - **Defense Against Targeted Attacks:** PKI is the target of threat actor-led attacks but legacy systems are not hardened.
- **Expertise Gaps:**
  - **Reliance on Consultants:** PKI expertise is scarce today and so organizations rely on consultants.
  - **Critical Initial Configuration:** PKI infrastructure must be carefully set up. An error can mean the entire stack needs to be rebuilt.
  - **Complex Management:** PKI ongoing management is complex. Per a 2020 study, most surveyed organizations spend $3 million annually to manage their PKI implementation.
  - **Service Level Agreements:** On-prem systems often struggle with PKI availability. In fact, 83% of organizations had a PKI-related outage in a 12-month period.
- **Challenging Environment**
  - **Hybrid Environments:** Many organizations will run a hybrid cloud and on-premises environment indefinitely.
  - **Outdated Components:** PKI systems often include outdated components such as back level Microsoft CA systems that should be replaced for efficiency and for manageability.
  - **Business Units Interrelationships:** Organizations often have business units that need to be isolated from headquarters and each other yet need to have trusted interrelationships.

A MODERNIZED PKI IS A MUST HAVE

In summary, organizations need to modernize their PKI infrastructure with a SaaS approach. The approach should be able to handle PKI for the organization along with semi-independent business units. It should also span all devices and workloads including 3rd party.

Since migration may be unfeasible for some applications, the PKI system should support hybrid on-premises and cloud-native machines and workloads. The PKI should embrace new capabilities such as certificates for emails and attachments as well as extend to future use cases such as code signing.



Organizations need a Modernized SaaS PKI that that meets the need of Hybrid On-premises and Cloud Environments

INTRODUCING AXIAD CONDUCTOR

Leveraging the power of the Axiad Conductor platform, Axiad's PKI as a Service (PKIaaS) is a consolidated, highly customizable, and scalable PKI for providing the digital trust required for your organization to innovate and thrive. machine (device and workload) and interaction authentication. Axiad PKIaaS provides highly secure certificates at scale and everywhere it's needed – including partner, vendor, and Bring Your Own Device (BYOD) machines. Emails and attached documents can be matched with a certificate of the end user, thereby verifying origin and non-repudiation of emails. The combination of product functionality and the SaaS delivery model helps lower the cost of operating an in-house PKI and allows organizations to consolidate or retire costly / aging existing PKI systems.

KEY FEATURES

Consolidated: Serves all machine certificate needs, everywhere across the environment

- **Consistent:** Generates certificates consistently across OSs, workloads, services, and more
- **Unified PKI:** Consolidates multiple PKI components – typically multiple Certificate Authorities (CAs) – into a single comprehensive, scalable package
- **Full Coverage:** Handles all machines (including WFH, BYOD, and partner), workloads (VMs, Containers, etc.), and interactions (emails and attached documents) across the entire environment

Highly Customizable: Fits into the most complex environments

- **Custom Certificate Authority:** CA topology, templates, and policies are customizable using both default templates and selectable templates for specific needs
- **Custom Certificates:** Creates custom certificates and approval workflows without coding using customizable templates
- **Broad protocol support:** Supports wide range of protocols, connectors, and standards for the automated distribution and renewal of digital x.509 certificates
- **Integrated:** Supports wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

Scalable: Works for any size organization

- **Seamless scalability:** Cloud-based operations hosted by a major CSP in multiple geographies provide seamless scalability
- **PKI without overhead:** Offloads resource-intensive PKI setup, management, and maintenance
- **Ready Migration:** Designed to make migration from on-premises PKI straightforward and without compromise in functionality

Deep PKI Expertise: Axiad provides PKI expertise to ensure highly available and reliable operations

- **24x7 Operations:** Operations and support are available on a 24x7 schedule
- **Maintenance and Upgrades:** Maintenance is applied by the Axiad team to ensure stability of the service and to upgrade functionality
- **Services:** Design, onboarding, and customization assistance is available from our Professional Services team

Platform Capabilities: Leverages Axiad Conductor Platform capabilities

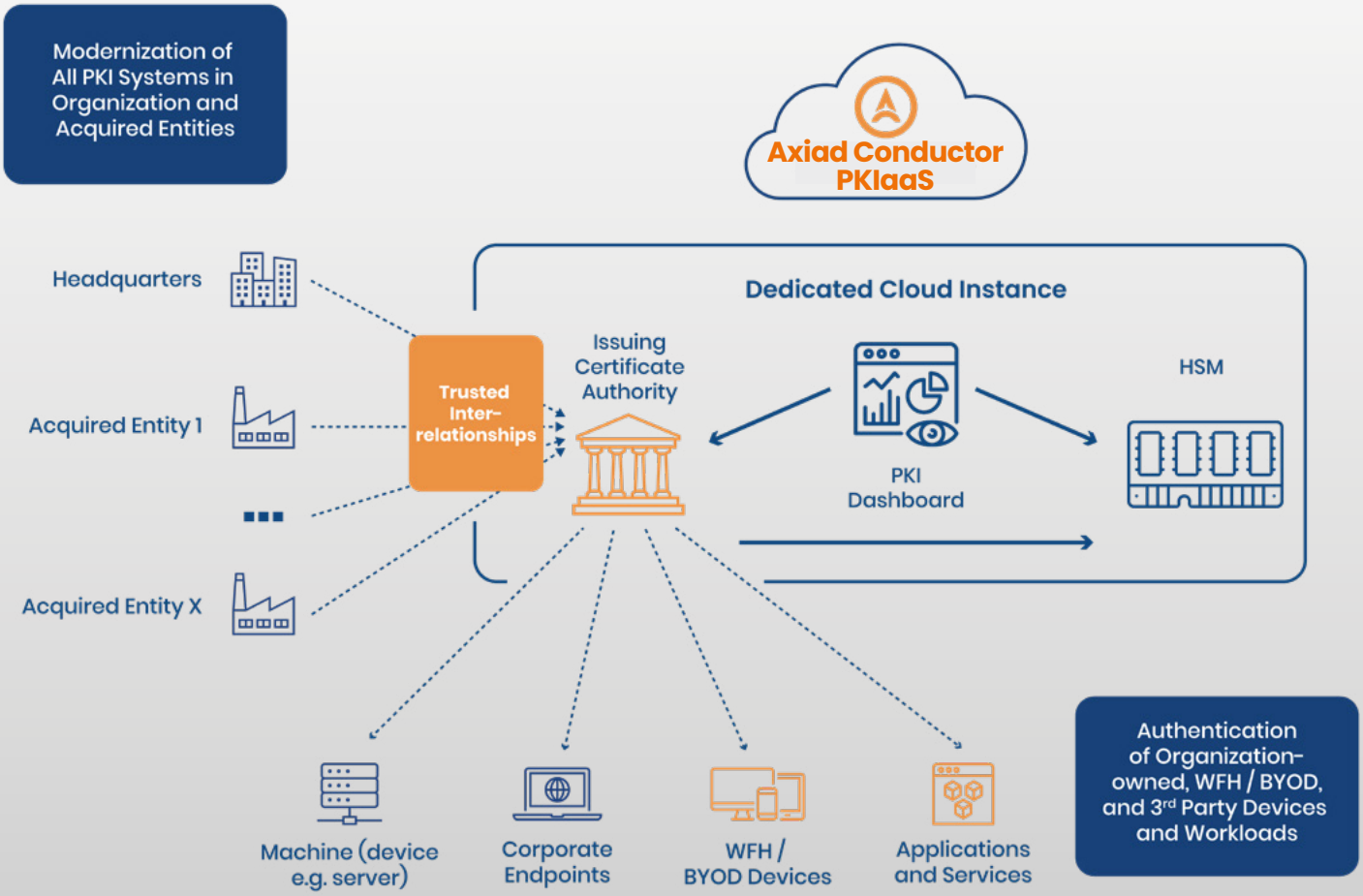
- **Secure by Design:** Customers receive a Dedicated Instance for secure isolation
- **HSM:** Customer root keys are stored in a HSM

OPERATION

Axiad Conductor PKIaaS runs in a dedicated cloud instance for each customer. Within the instance:

- **PKI Dashboard:** Provides a single pane of glass for management of existing certificates, the creation of custom certificates, and for configuring and managing the Certificate Authority.
- **Issuing Certificate Authority:** Ensures that certificates are issued and validated at scale over the cloud.
- **HSM:** The customer's root keys are consolidated into a HSM that is partitioned for security.

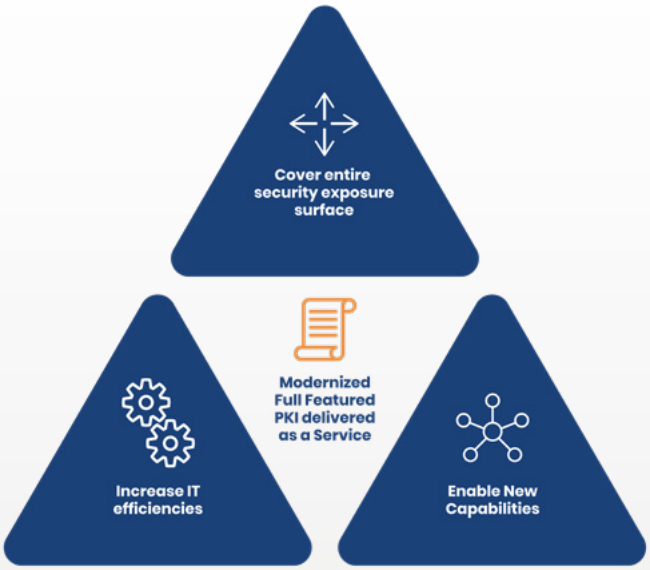
On-premises, off-premises (including WFH and Bring Your Own Device), and 3rd party devices and workloads are authenticated by PKIaaS, wherever they are located. Utilities accessed from the PKI Dashboard make certificate provisioning efficient and rapid.



HOW AXIAD HELPS YOU

Axiad's PKIaaS provides PKI Cloud Modernization with core capabilities that may not be possible with legacy PKI implementations:

- **Cover the entire security exposure surface**
  - Span Work From Home (WFH), Bring Your Own Device (BYOD), and 3rd party machine authentication
- **Enable New Capabilities**
  - Enable new capabilities such as interaction authentication and code signing
- **Increase IT efficiencies across the authentication landscape**
  - Enhance operational efficiencies, manage SLAs, and minimize maintenance



USE CASES

There are several major use cases enabled by a modernized PKI:

1. Consolidate all machine certificate needs: In addition to physical devices, authenticate Virtual Machines, Containers, and other non-physical entities.

2. Improve core SLAs / minimize IT resources: Cost-effectively migrate to the cloud for maximum coverage while conserving precious IT resources.

3. Enable new capabilities such as email and attachment certification: Ensure that the sender is not impersonated and the enclosure is not added by a threat actor.

4. Enhance IT efficiencies across the authentication landscape: Instead of operating PKI as a silo, gain the advantages of a unified cloud platform that also authenticates end users across the entire ecosystem.

Each use case is outlined below.

1. Consolidate all machine certificate needs

Axiad Conductor PKIaaS consolidates all machine certificate needs across the entire environment. The package provides certificates to all machines (including WFH, BYOD, and partner) and all workloads (VMs, Containers, etc.).

Axiad PKIaaS has numerous customization capabilities to ensure that all organizational needs can be met with a single system. The built-in customizable Certificate Authority can be modified in terms of topology, templates, and policies. As compared to legacy CAs, the Axiad CA provides full capabilities but with increased efficiencies due to Axiad's management utilities.

A wide range of protocols, connectors, and standards are supported that enable efficient distribution and renewal of x.509 certificates. Integrations with a wide range of protocols, connectors, and standards enable interoperation across the Identity Ecosystem.

Advantages include the replacement of outdated PKI systems that are expensive to maintain, elimination of back level versions of components such as Microsoft CA, and reduced IT effort.

2. Improve core SLAs / minimize IT resources

For many organizations, availability and reliability of the PKI system is difficult to attain much less maintain. With Axiad PKIaaS, operations are hosted by major CSPs in multiple geographies to provide seamless scalability and to ensure localized regulations are more easily met. Maintenance is automatically applied by the Axiad team. Further, upgrades to take advantage of new identity fabric capabilities are also performed by Axiad automatically and without charge.

Finally, a cloud-based portal provides efficient utilities for the management of certificate issuance, renewal, and revocations. The portal provides warnings when certificates are nearing the expiration date, thereby minimizing the chance of an expired certificate causing an outage.

Advantages include the improvement of service levels for the PKI system, higher availability due to the reduction in certificate-related outages, and reduced IT effort.

3. Enable New Capabilities

Axiad PKIaaS enables certificates to be leveraged in new capabilities such as certifying interactions. For example, interactions (emails and attached documents) can be certified to ensure that the sender is trusted and the attachment was not added by malware or a threat actor. Also, certification ensures that the email cannot be repudiated.

In addition, capabilities such as code signing can be implemented with PKIaaS. Since it must work in sync with the development systems at the organization, it would require a customized implementation.

Advantages include the direct reduction of social engineering attacks, reduced rates of malware invading the environment, and greater flexibility in accommodating custom projects.

4. Enhance IT efficiencies across the authentication landscape

Instead of operating PKI as a silo, organizations can leverage a unified cloud platform that also authenticates end users across the entire ecosystem. Sharing the Axiad Conductor platform, Axiad PKIaaS shares services with Axiad Certificate-Based Authentication (CBA). As a result, end user authentication can easily be added across the organization.

By leveraging a combined PKIaaS and CBA approach, the organization can enhance operational efficiencies, manage SLAs, and minimize overall maintenance. As an example, by efficiently managing certificates across the organization, IT resource demands can be minimized.

Other advantages of a shared approach:

- Common mapping: End users and devices can be mapped to the appropriate business entity efficiently and without confusion.
- Synergistic Authentication: The device can be authenticated automatically before the end user authenticates, thereby increasing security substantially.
- Consistent Security Across Organization: Strong device authentication (PKI) can be matched to strong end user (CBA) authentication, keeping security consistently high.

ORGANIZATIONAL OUTCOMES

Strong positive outcomes are driven by Axiad's approach:

- **Expand business opportunities:** This approach safely encompasses 3rd party and a wide range of devices and workloads into the security ecosystem. As a result, partner offerings can be safely leveraged by organization-owned resources, thereby maximizing potential business solutions.
- **Reduce Business Disruptions:** As mentioned in the introduction, PKI management and security issues result in business disruption in terms of outages or breaches. With certificate expiration date tracking and prompting, business disruptions can be avoided. Further, due to a hardened PKI infrastructure, breach risks are minimized.
- **Maximize Security Flexibility:** Legacy PKI most often only authenticates resources that are controlled by the organization. With Axiad, security flexibility is maximized by enabling all devices and workloads to be authenticated regardless of location or ownership.
- **Improve End User Satisfaction:** Today, end users often have to respond to device authentication prompts. PKI machine authentication, despite embodying a more rigorous level of security, is automated and transparent to end users. As a result, end user satisfaction will increase – a win-win for IT!

BENEFITS FOR THIS USE CASE

Increase Innovation

Leverage digital trust to innovate more products and services and speed their delivery

Maximize Security

Provide certificates to every component in your infrastructure, closing doors for hackers

Minimize Overhead

Minimize the labor and IT resources required to provide digital trust for your org

---

[i] Ponemon: "The Impact of Unsecured Digital Identities" study, 2020.

[ii] Venafi: CIO Study: "Outages Escalating with Massive Growth in Machine Identities" white paper, 2023.

AXIAD

About Axiad

Axiad is an identity security company tackling the growing threat of compromised credentials, which drive over 70% of enterprise breaches. The sprawl of human and non-human identities across organization silos creates security blind spots that existing tools fail to secure. Axiad tackles this problem head-on, detecting identity risks and poor credential hygiene across systems, providing actionable insights, and enhancing security without needing a complete overhaul. Axiad makes identity simple, effective, and real. Discover more at axiad.com or follow us on LinkedIn.