

PKI As A Service (PKIaaS)

The foundation for scalable, crypto- agile machine identity security

How Accutive Security helps enterprises replace legacy PKI infrastructure, without inheriting the same operational problems in a new platform.

109:1

Nonhuman identities now vastly outnumber human identities.

2029-35

The NIST / CNSA 2.0 quantum readiness deadline

Weeks, not months

Typical time-to-production for PKIaaS vs. a self-built, on premises PKI deployment.

PKIMM Terms

The PKI maturity enterprises achieve when PKIaaS is paired with Accutive Security's managed services.

Accutive Security implements and operates PKIaaS across:



Executive Summary

PKI as a Service (PKIaaS) is a cloud-based delivery model that provides fully managed PKI capabilities, including:

- key management
- private certificate issuance
- lifecycle automation, and
- cryptographic policy enforcement

All of this is provided without the need for organizations to maintain on-premises PKI infrastructure. For most enterprises, on-premises PKI, particularly aging Microsoft AD CS environments, was designed for the era that featured fewer machines, longer certificate lifetimes, and stable cryptographic algorithms. That era has ended. Machine identities now outnumber human identities 109 to 1, post-quantum migration timelines are critical for regulated industries, and the cryptographic infrastructure underneath all of it must be able to change faster. Rather than deploying and operating hard-to-scale and hard-to-maintain on-prem PKI infrastructure, organizations are moving to PKIaaS to scale fast, stay resilient, and maintain crypto-agility in today's machine identity landscape.

Accutive Security provides platform-agnostic implementation and managed services for leading [PKIaaS platforms](#) including Keyfactor, AppViewX, Palo Alto NGTS, DigiCert, Entrust and HID. Unlike broad generalist security firms and volume-driven resellers that cover every domain superficially, Accutive Security operates as the Cryptography, Data Protection and Identity Security Center of Excellence providing both the expert guidance to select the right solution and the certified technical expertise and support to implement, integrate, operationalize, optimize, and manage it.

The Forces Driving the PKIaaS Shift

Legacy PKI was built for a different era. These six pressures are making it unsustainable.



Infrastructure burden

CA hierarchy design, HSM lifecycle, OS patching, DR engineering, and 24/7 monitoring: all responsibilities sit on internal teams that are already burdened.



Machine identity scale

Microservices, Kubernetes workloads, IoT devices, and agentic AI systems are pushing certificate volumes well beyond what on-prem PKI was architected to handle.



Post-quantum readiness

Introducing PQC-hybrid certificates on a legacy CA (particularly ADCS, which does not support quantum-resistant algorithms) is a multi-quarter re-engineering project. PKIaaS platforms absorb that complexity at the service layer.



Multi-cloud and hybrid trust

Enforcing consistent trust across AWS, Azure, GCP, and on-prem through a single-region, customer-managed CA creates structural gaps in coverage, revocation, and policy enforcement.



The PKI expertise gap

Specialized cryptographic engineers are scarce and hard to retain. PKIaaS offloads infrastructure operations so available expertise goes toward governance and architecture.

Why Choose PKIaaS Over Legacy On-Prem PKI

Dimension	Legacy on-premises PKI	PKIaaS
Deployment	Months of infrastructure build-out	Production-ready in weeks
Scalability	Hardware-bound	Elastic; scales with workload demand
Automation	Custom scripts; manual renewal workflows	API-first: ACME, SCEP, EST, REST
Visibility	Minimal reporting; limited visibility	Built-in dashboards, audit logs, CLM-ready integrations
Resilience	Single-region, customer-engineered HA	Multi-zone / multi-region with provider SLA
Operational burden	High; internal teams own patching, HSM lifecycle, OS maintenance, DR	Consumed as a managed service
Crypto agility / PQC readiness	Algorithm transitions require multi-quarter re-engineering of CA infrastructure	PQC roadmap progress inherited from platform provider

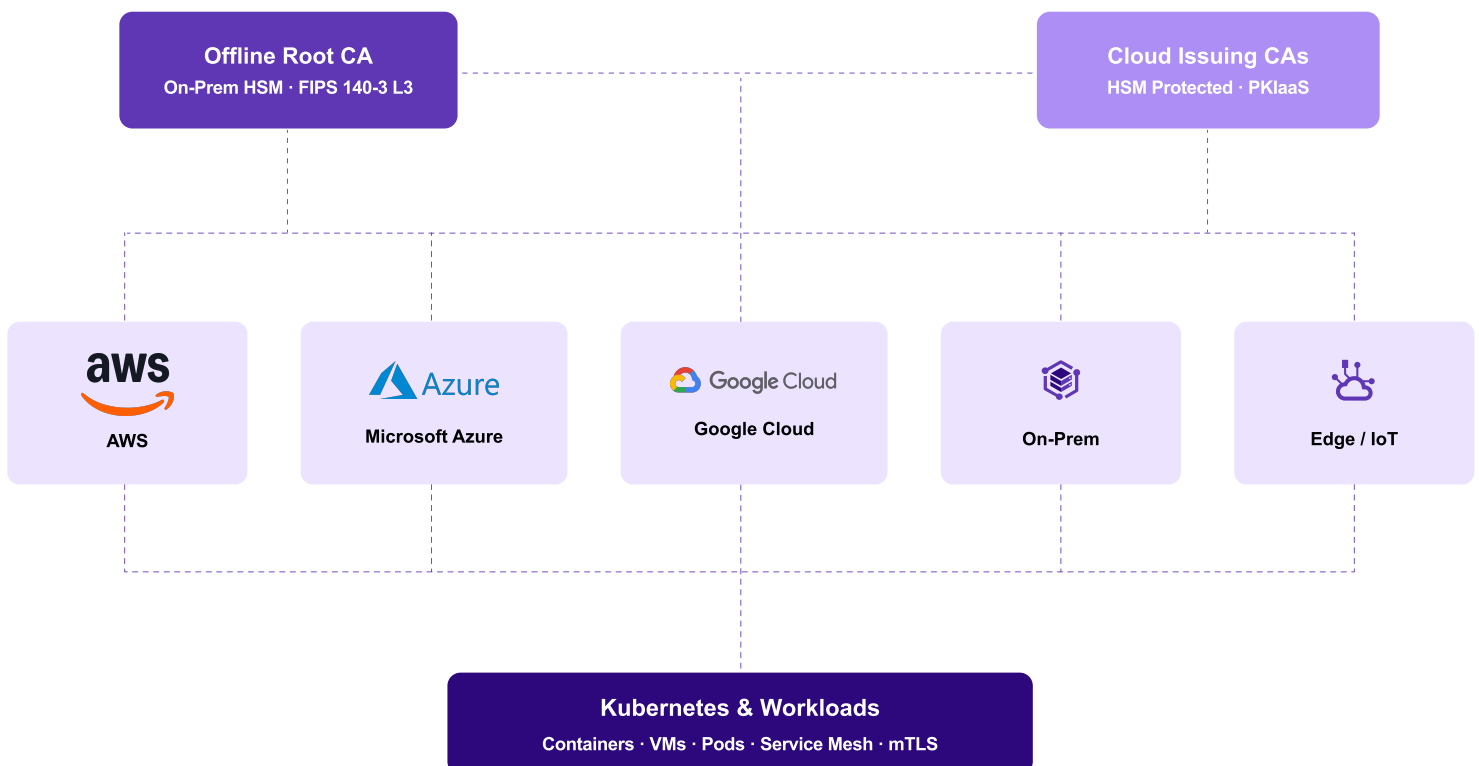
Hybrid PKI: Keep Your Root CA On Prem, Everything Else on Cloud

Full migration to PKIaaS is the right destination for many enterprises, but it is rarely a single-step transition. Data sovereignty requirements, regulatory mandates, air-gap obligations, and existing hardware investments often require Root CAs to remain offline on-premises, even when Issuing CAs and the operational service layer move to the cloud.

This hybrid architecture is a mature, well-established deployment model. An air-gapped offline Root CA, protected by an on-premises HSM, signs one or more cloud-hosted Issuing CAs. All certificate issuance, renewal, and revocation operations run through the cloud service layer. Workloads spanning on-premises, AWS, Azure, GCP, and Kubernetes receive certificates from the cloud Issuing CAs, while the root of trust never leaves the organization's physical control.

For enterprises in regulated industries, including financial services, healthcare, and public sector, this model satisfies sovereignty and audit requirements while delivering the operational and scalability benefits of cloud-hosted PKI.

Accutive Security designs and implements hybrid architectures across all supported PKIaaS platforms, including FIPS 140-3 Level 3 HSM integration for the offline Root CA layer.



Our PKIaaS Approach:

We Help You Select the Right Platform, Then Build, Migrate, and Operate It

Most PKIaaS engagements stall at platform selection. Overlapping capabilities, different sovereignty models, and diverging PQC roadmaps make the decision consequential and hard to navigate alone.

Accutive Security helps you through it:

- **Platform-agnostic selection:**

We are certified delivery partner for Keyfactor, AppViewX, DigiCert ONE, Entrust, HID, Thales, and Palo Alto Networks NGTS. The recommendation follows your architecture requirements, not deal registration economics.

- **Certified engineering depth:**

Platform-specific certifications and PKI migration programs delivered across industries. Deep expertise in a focused domain, not generalist coverage across hundreds of product categories.

- **Full lifecycle engagement:**

We cover the complete program: PKI assessment, architecture design, trust model definition, controlled migration, operational handoff, and ongoing managed services.

- **Innovation Lab access:**

Evaluate PKIaaS platforms hands-on before committing to a vendor. Working proof of value replaces theoretical comparison.

How We Migrate Your PKI: A 5-Phase Migration Path with a Clear Start, Middle, and End

PKI migration is an infrastructure program, not a software deployment. Accutive Security's five-phase methodology runs from discovery through full legacy decommissioning.

01

Phase 1 PKI Discovery and Assessment

Full inventory of trust chains, CA hierarchy, certificate templates, issuance volumes, and shadow certificates. Establishes the baseline the migration plan is built on.

02

Phase 2 PKI Architecture and Trust Model Design

Workload prioritization, hybrid coexistence design, CP/CPS alignment, and platform selection. Defines where the Root CA lives and which workloads migrate in which sequence.

03

Phase 3 Controlled Issuance from PKIaaS

New certificates issue from the PKIaaS platform while the legacy CA coexists during transition. Private keys are never migrated, transition happens through natural attrition.

04

Phase 4 Expansion and Optimization

Automation is extended across workload types: Kubernetes, DevSecOps pipelines, Zero Trust network access, and IoT device identity.

05

Phase 5 Legacy PKI Decommissioning

The step most vendors do not scope. Accutive Security's decommissioning methodology covers revocation, CRL/OCSP teardown, CA key archival, and compliance documentation, closing the operational and audit liability the legacy CA carries.

Shared Responsibility Model: The Platform Covers Infrastructure. Governance Is Still Yours.

Buying the platform gets you the infrastructure. Achieving PKI maturity requires governance, policy, integration, and operational discipline that sit entirely on the customer side of the table. That is precisely where Accutive Security's engagement model focuses.

Responsibility area	PKIaaS provider	Customer	Where Accutive bridges the gap
CA infrastructure, HSM lifecycle, OS patching	✓ Owned and operated by provider	—	—
Platform availability and multi-region resilience	✓ Covered by provider SLA	—	—
Platform upgrades and security patches	✓ Provider managed	—	—
Certificate policy and CPS definition	—	✓ Provider managed	Policy authoring, CPS documentation, CP/CPS alignment to regulatory requirements
Trust hierarchy design and CA naming	—	✓ Customer decision	Architecture design and trust model definition as part of Phase 2
Certificate template governance	—	✓ Customer-owned	Template rationalization, lifecycle policy design, and ongoing governance
Issuance automation and workflow integration	Protocols provided (ACME, SCEP, EST)	✓ Customer integrates	Integration services across Kubernetes, DevSecOps pipelines, MDM, ITSM, and SIEM

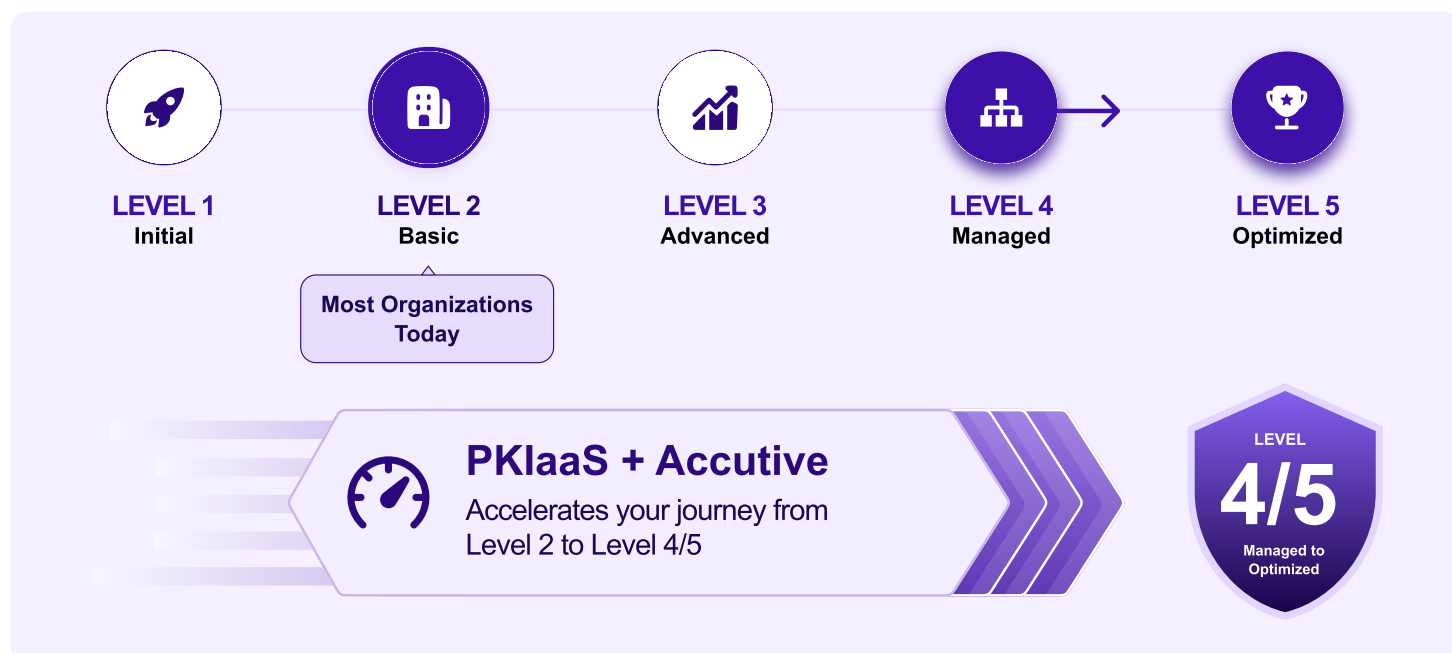
Monitoring, alerting, and incident response	Platform telemetry provided	✓ Customer operates	Managed services: monitoring, alerting, and incident response on the customer's behalf
Compliance reporting and audit evidence	Logging and audit trails provided	✓ Customer assembles and presents	Audit readiness support aligned to PCI DSS, HIPAA, DORA, eIDAS, and NIS2
Legacy PKI decommissioning	—	✓ Customer responsibility	Phase 5 decommissioning methodology; revocation, CRL/OCSP teardown, key archival, compliance documentation

Most Are at PKI Maturity Level 2.

PKIaaS + Accutive Takes You to Level 4/5

Most enterprises running legacy on-premises PKI sit at Level 2 (Basic) or the lower boundary of Level 3 (Advanced). PKIaaS, paired with Accutive Security's governance, integration, and managed services, is the practical path from Level 2 to Level 4 (Managed) or Level 5 (Optimized). The platform delivers the infrastructure maturity; Accutive Security delivers the operational and governance maturity.

As a member of the PKI Consortium, Accutive Security leverages the proven PKI Maturity Model as a standardized framework to evaluate organization's progress across five levels:



Solution Selection Criteria:

Questions to Ask Before Selecting a PKIaaS Platform

Accutive Security works through each of these before making a platform recommendation.

01 Where do your CA private keys live, and under whose control?

Confirm FIPS 140-3 Level 3 validation and evaluate BYOK/HYOK models where sovereignty requirements apply.

02 What is the vendor's PQC roadmap?

FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) support are the baseline to verify, along with a published timeline for hybrid PQC certificate profiles.

03 How deep is the automation?

ACME, SCEP, and EST are table stakes. Evaluate REST API coverage and native integrations with Kubernetes cert-manager, HashiCorp Vault, and your MDM platform.

04 What does the SLA actually cover?

Confirm availability architecture, regional data residency options, and SLA terms, particularly for regulated industries with data localization requirements.

05 Does the platform's CLM layer meet your requirements?

Or does it require a separate CLM tool for certificate discovery, policy enforcement, and reporting?

06 Can the platform enforce your CP and CPS at the issuance layer?

Including algorithm restrictions, key size floors, and certificate lifetime limits.

07 Does the vendor support legacy CA decommissioning, or scope it out?

Confirm offline Root CA integration, legacy CA coexistence during transition, and whether decommissioning is part of their methodology.

The Platforms We Implement, Integrate, and Operate

Certified Service Delivery Partners

Accutive Security holds certified implementation and managed services status with the following platforms:

KEYFACTOR

Purpose-built enterprise PKI and CLM at scale, with particular strength in complex PKI environments, IoT device identity, and code signing governance.



Automation-first CLM and PKI platform with deep workflow orchestration, cryptographic posture management, and strong DevSecOps pipeline integration.



CLM and SaaS-based private PKI, providing enterprise-wide certificate visibility, CA-neutral orchestration, and policy-driven automation across network infrastructure and SASE environments.



Unified platform bringing together private CA, public certificate management, device trust, and document signing under a single management experience.



PKI-as-a-Service for IoT device identity and workforce credentials, spanning the convergence of digital and physical identity.

Why Organizations Trust Accutive Security with Their PKI



15+ years
partnering with

leading PKI
platforms



5/5

Rating on Gartner
Peer Insights



PKI
Consortium

Member of PKI
Consortium

Ready to Modernize Your PKI?

Book a PKI Modernization Consultation Now

Social Links