ACCUTIVE SECURITY

The Auth + Crypto products and services company

Solution Brief

Private & Secure PKI, Streamlined & Trouble-free

Cloud-Based PKI Protects & Enables Your Distributed Teams, Networks, and Devices

Recent shifts in technology and society have strained the first-generation PKI (public key infrastructure) systems, which handle and distribute internal TLS certificates, to their limits. Network administrators, developers and information workers have all transitioned to remote work, each requiring enhanced machine-to-machine authentication and encryption on their essential systems.

Existing PKIs are expiring when security teams are overwhelmed with workloads larger than ever before. Simultaneously, companies are accelerating the pace and importance of their digital transformation initiatives.

Numerous PKI teams are already grappling with fragile, challenging-to-maintain internal PKI systems that demand continuous attention and immediate upgrades. Suddenly, the number of sites and services needed to support customers and partners has doubled or tripled, demanding even more focus from already stretched teams. In many scenarios, this has led to a painful collision: Internal teams have less time, yet they are also addressing exponentially more requests that carry an even higher urgency level.

Accutive Security is the de-facto industry expert in authentication and cryptography. With two decades of PKI innovation, Accutive Security is a reliable partner capable of providing a turnkey, cutting-edge internal PKI solution that is cost-efficient and rapidly deployable, delivering quicker time-to-value. It also meets the scalability and residency requirements of businesses with global data center operations.

Cloud-Based Secure PKI at a Glance

Cloud-Based Private PKI is a SaaS solution offsetting the costs and complexities of developing, distributing, and managing private trust X.509 digital credentials for your network infrastructure, devices, and users.

- Provides preset digital certificate issuance profiles for mobile and network devices
- Establishes adaptable root and intermediary issuing CA structures to suit business requirements
- Automates enrollment and issuance for Microsoft desktops and laptops
- Allows real-time rotation, substitution, or revocation of any certificate group.

Advantages

- Ease your private PKI with a wholly managed, SaaS-oriented service
- Substitute antiquated, fragile systems with contemporary, swift PKI architecture
- Direct limited resources to high-value projects as service preserves your internal PKI

Obstacles

PKI can be challenging if you don't have the right operational staff or a center of excellence around you for questions or help. It's an intricate system requiring a proficiency level that is tough to attain and maintain, particularly as the number of machine identities that organizations need for security escalates.

Revamping Windows PKI

Numerous organizations have established their private PKI on Microsoft Active Directory Certificate Service (ADCS), the Windows server function that empowers them to offer public key cryptography, digital certificates, and digital signature capabilities to their entity. Now they find themselves struggling to stay abreast with the continuous flow of patches, updates, hot fixes and vulnerabilities that Microsoft necessitates with AD and SQL Server. These Microsoft PKIs are nearing their end and need to be updated on stringent timelines.

Agile PKI

The world of digital certificates is rapidly evolving, as evidenced by the Google Chromium Project's recent plans to further reduce Transport Layer Security (TLS) certificate lifespans from 13 months, or 398 days, down to a mere 90 days. This transformative shift, announced in Google's "Moving Forward, Together" roadmap, intends to bolster the security of online communications and provide more robust defenses against cyber threats.

Validating Security, Ensuring Compliance

The catalog of regulatory norms, security frameworks, and compliance directives that confirm the solidity and honesty of internal encryption procedures keeps expanding. PCI DSS, NIST, and ISO have all incorporated requirements for enhanced cryptography and updated protocols in their latest releases. Moreover, industry-specific mandates, like NERC CIP prerequisites for energy suppliers and FFIEC for banking and HIPPA in healthcare, are anticipated to respond to the surge in remote working with new machine-to-machine stipulations in the foreseeable future.

Transitioning PKI to the Cloud

Cloud infrastructures bring a consistent set of advantages across numerous technology fields: the capacity to rapidly scale up or down in response to fluctuating business needs; controllable and predictable expenses; and the agility needed to promptly support new initiatives. PKI isn't an outlier. Cloud-based PKI solutions offer both the convenience and straightforwardness of SaaS and the manageability needed to adapt swiftly to changing business demands.

PKI at Corporate Scale

Microservices design, containerization, and DevOps toolchains all amplify the amount of TLS connections that an internal PKI must manage. The launch of millions of IoT devices has contributed even more. Utilizing TLS to secure worker endpoints, mobile devices, and network devices has added further. Collectively, these shifts have significantly amplified the scale of challenges PKI teams must tackle. PKI that was conceptualized and implemented a decade ago just can't keep pace anymore. A novel approach is essential.

The Answer: Cloud-Based Secure PKI

The optimal method to alleviate the pain and risk inherent in internal PKI is to employ specialists to handle it for you. The Cloud-Based Secure PKI solution is a sturdy, adaptable, and highly secure remedy that addresses your immediate private PKI requirements—demanding virtually no time or effort from your own InfoSec team. It also doesn't necessitate a horde of consultants and a substantial services budget.

A Fully Administered, Trouble-Free PKI Service

Cloud-Based Secure PKI is completely managed by experts on the service team. Your advanced PKI is tailored to your needs, utilizing the CAs, roots and intermediaries required by your enterprise. Each customized PKI is engineered with current best practices for design, implementation, and security in focus, ensuring your PKI employs the most recent capabilities and protocols.

Preconfigured Certificate Issuing Profiles

Certificate issuing profiles are vital tools that can either make or break your private PKI. These profiles configure the content for TLS certificates, set security limitations, and outline input and output forms for certificate enrollment. Cloud-Based Secure PKI encompasses profiles for cloud-native procedures as well as for mobile, telephony, and network devices. These templates significantly streamline your private PKI solution without compromising security or functionality.

SaaS-Oriented, Cloud Hosted PKI

Your InfoSec squad will have full API- and GUI-based access to the hosted solution, enabling them to modify configurations as necessary or perform custom tasks.

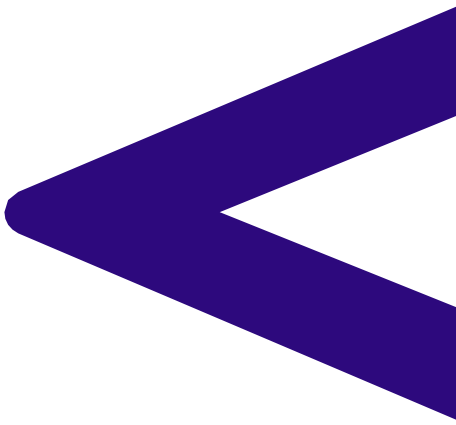
However, unlike your old PKI, you don't need to establish your own servers, arrange requests, validate functions, upgrade databases, and monitor connections (and fix them if they disconnect). Cloud-Based Secure PKI provides you with the personalization that modern PKI solutions demand, but with a high degree of simplicity and quick time-to-value.

Auto-Enrollment Compatible

In today's threat environment, all systems are critical systems, not just web servers and app servers. Microsoft Active Directory Certificate Service (ADCS) enables Microsoft servers and devices in your organization to automatically enroll for TLS certificate coverage. Auto-enrollment automates a labor-intensive process, and by integrating with it, Cloud-Based Secure PKI ensures the largest portion of your IT estate isn't unprotected from the security TLS certificates offer.

Inbuilt Security Controls and Best Practices

Industry top practices for PKI and trust infrastructure are continually evolving. Every Cloud-Based Secure PKI is deployed with contemporary best practices for security and control, incorporating completely air-gapped and perpetually offline infrastructure, along with key generation and storage in a DoD-spec, vaulted, granite-protected facility.



Operating Mechanism

Cloud-Based Secure PKI is a hosted, fully administered SaaS service that enables your InfoSec groups to concentrate on external, public-facing systems, while your internal, private PKI requirements are fulfilled by a reliable, automated, and cloud-based solution

Cloud-Based PKI	
PKI Features	• Adaptable root and intermediate CA structure setup • Issuance of RSA and ECDSA CA and certificates • Offline root key custody administration • Overseeing online issuing CA(s) signing, operations, and documentation • Offline and online key material business continuity planning and disaster recovery procedures • Management of all certificate verification processes, including high-availability implementation and highly scalable OSCP and CRL processes • HSM processes and high-availability model for continuous operations • Web-based certificate administration portal • Continuous secure operations of all online issuing CAs in FIPS 140-2 level 3 hardware • Automatization for MS autoenrollment and other standard-compliant certificate management protocols like SCEP, EST, and ACME, along with API support • Construction and execution of private trust hierarchy architecture(s) • Turnkey processes and documentation for root key generation ceremonies
Service and Support Features	• Guidance and support for current PKI migration to the Service managed service, as well as guidance and recommendations for migration of CA key material obtained in acquisitions • 99.9% availability and uptime • U.S. and European data center operations • 24x7x365 availability, support, security monitoring
Integrations and Services	• **Mobile Device Management:** Microsoft Intune, Airwatch by VMWare, MobileIron, Citrix ZenMobile, Jamf Now, Jamf Pro and more • **Microsoft Auto-Enrollment:** Windows desktops. servers and laptops • **Network and IoT Enrollment:** SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport) • **Applications and Developers:** ACME2 for cert-bot and more integrations; complete REST API

CONTACT INFORMATION

27068 La Paz Road, Suite 245 Aliso Viejo, CA 92656

Toll Free 888.666.8315

Contact Us

www.accutivesecurity.com

Accutive Security provides comprehensive information technology solutions which include enterprise security; IT application development; systems integration; lending platform services; and professional services to clients in industries ranging from financial services, healthcare, technology, entertainment, and retail. Accutive Security is a specialized team of experienced professionals with years of industry, business, and IT expertise dedicated to developing IT solutions that exceed our clients' expectations.