AppViewX PKI | Solution Overview

AppViewX

Scalable, Secure, Quantum-Ready PKI. Without the Complexity.

Challenge

Your private PKI was built for a different era. Legacy on-premises infrastructure like Microsoft AD CS wasn't designed for today's certificate volumes, hybrid and multi-cloud environments, or post-quantum cryptography. Every new use case means another work-around on infrastructure that's already at its limit.

Operational burden and costs keeps growing

Running compliant in-house PKI means constant manual effort, from hardware refreshes to daily operations, and the expertise it needs is hard to find and harder to retain.

Without integrated CLM, certificates become a liability

In-house PKI typically lacks integrated certificate lifecycle management and policy enforcement. Certificates go untracked, expirations cause outages, and compliance stays manual and reactive.

Modern infrastructure has outgrown legacy PKI

On-premises PKI wasn't built for multi-cloud, DevOps, IoT at scale, or PQC. Stretching Microsoft AD CS to cover them piles complexity onto an already constrained foundation.

Legacy PKI has no clear path to PQC migration

NIST has finalized the first set of PQC standards and plans to deprecate and disallow RSA and ECC algorithms. Most in-house PKI has no native path to PQC, and retrofitting one onto aging infrastructure is risky.

AppViewX PKI

Replace Your Legacy PKI with a Crypto-Agile, CLM-Integrated SaaS Solution

AppViewX PKI replaces the complexity of in-house private PKI with a simplified, scalable, and secure solution that supports current and future use cases across your enterprise. Set up CA hierarchies in minutes. Issue private certificates at scale. Manage every public and private certificate—across all CAs and environments—from a single centralized console, without buying hardware or depending on scarce PKI specialists.

AppViewX PKI integrates natively with AppViewX CLM for end-to-end certificate lifecycle automation. When certificate lifespans shrink or cryptographic standards change, your PKI adapts automatically and without re-architecture.

Simplified

Reduce PKI operational complexity, even in the most demanding environments. Centralize lifecycle management for all public and private CA-issued certificates to eliminate misconfigurations, outages, and security gaps.

Scalable

Scale with your business on demand across hybrid, multi-cloud, IoT, and DevOps environments. Pair with AppViewX CLM for deep integrations across CAs, ITSM, DevOps, and cloud to manage your entire certificate program.

Secure

Enforce PKI compliance with crypto-agile, policy-driven automation aligned to industry and organizational standards. Issue NIST-standardized PQC and hybrid composite certificates for post-quantum resilience.

What It Delivers

Private PKI Built for How Your Enterprise Operates Today—and Where It's Going Next

Modern and Agile PKI

Provision enterprise-grade private CAs in minutes via virtual key ceremony. Deploy CAs in regions of your choice with flexible, template-based configuration for CAs and end-entity certificates. Reusable CA policy configurations, defined manually or generated from a CPS document, reduce configuration drift across deployments.

Guided PKI Modernization

Move from Microsoft AD CS to AppViewX PKI in hours, not months. For larger environments, the AD CS Migration Wizard supports multiple concurrent CA migrations, automatically discovering instances, preventing duplicate runs, and providing full visibility into in-progress and completed migrations.

PQC-Enabled Issuance

Issue PQC certificates using NIST-standardized algorithms: ML-DSA and SLH-DSA. Hybrid composite certificates preserve backward compatibility throughout your migration. HSM-backed PQC key generation supports quantum-safe CA creation, certificate issuance, and code signing workflows.

Robust CA Security

Protect CA keys in FIPS 140-2 Level 3 HSMs. Bring your own HSM or use AppViewX-managed keys. Airgapped/Offline Root CA support, M of N key control, and real-time OCSP keep your CA environment audit-ready.

CLM-Integrated PKI Management

Gain a single-pane-of-glass view across certificate discovery, lifecycle automation, and policy-driven control for all public and private CAs. Native CLM integration lets you roll out PQC and hybrid composite certificates at scale and enforce PKI policies consistently.

Extensive Native Integrations

Connect to leading HSMs (Fortanix, Utimaco, Entrust, Thales), AWS CloudHSM, and Azure Key Vault. Integrate with CAs, DevOps toolchains, ITSM, SIEM, and MDMs via APIs. Auto-enroll certificates using ACME, EST, SCEP, NDES, CMP, or Windows Auto-enrollment.

What PKI and Security Teams Get

Modernize PKI without disrupting operations	Move from Microsoft AD CS to AppViewX PKI incrementally. Your CA structure is discovered, mapped, and recreated automatically, so existing operations stay intact throughout.
Free your team from PKI operational overhead	Eliminate hardware procurement, infrastructure maintenance, and scarce PKI specialist dependency. Your team focuses on higher-value work; AppViewX PKI handles the rest.
Prove compliance without the scramble	Template-based CP/CPS, centralized audit logs, and real-time alerts on CA and CRL expiry mean auditors get reports pulled from the platform—not evidence assembled through manual projects.
Build post-quantum readiness into your PKI today	Issue PQC and hybrid composite certificates today. When your environment is ready to fully migrate, your PKI already is. No separate initiative required.

Replace your legacy PKI and get quantum-ready-without the operational risk.

Schedule a PKI assessment today.

AppViewX
info@appviewx.com
www.appviewx.com
+1 (212) 400-7541