AVX ONE | PKIaaS

AppViewX AVX ONE PKI-as-a-Service

Modern, Secure, and Scalable Private PKI-as-a-Service

Enterprises rely on private PKI (Public Key Infrastructure) to ensure identity, security, and trust within their internal and closed ecosystems of machines, users, devices, and applications. While on-premises PKI solutions like Microsoft CA (MS ADCS) were once considered the gold standard, organizations are now recognizing the hidden costs, complexities, and limitations of managing PKI in-house. As use cases evolve and the shift to Post-Quantum Cryptography (PQC) accelerates, the challenges of legacy on-premises PKI solutions are becoming more apparent.

Challenges

- *High Operational Costs*
- *PKI Expertise Required*
- *Lack of Effective Certificate Lifecycle Management (CLM) and Integrations*
- *Outdated Hardware/Software*
- *Scalability and Flexibility Issues*
- *Security and Compliance Risks*

The AppViewX Solution

AppViewX AVX ONE PKI-as-a-Service (PKIaaS) is a modern, agile, and secure PKI solution that seamlessly supports all private trust use cases. Whether ensuring compliance with data protection regulations, building ecosystem trust, or securing assets with strong authentication and encryption, AVX ONE PKIaaS delivers a comprehensive, scalable, turnkey private PKI solution.

With AVX ONE PKIaaS, you can quickly set up compliant, secure private CA hierarchies tailored to your specific needs, and begin issuing certificates in minutes. As a cloud-based service, there's no hardware to purchase or infrastructure to deploy. AVX ONE PKIaaS is part of the AppViewX AVX ONE Platform, which combines modern PKIaaS with end-to-end certificate lifecycle management automation for all private and public certificates, from a centralized console.

Why AppViewX AVX ONE PKI-as-a-Service

Modern

- Modern cloud-based PKI
- Lower TCO, no hardware to procure and manage
- SaaS PKI frees up valuable IT time and resources
- PQC certificate issuance and CLM enables quantum resilience
- Quickly and seamlessly set up CA hierarchies with secure virtual key ceremonies

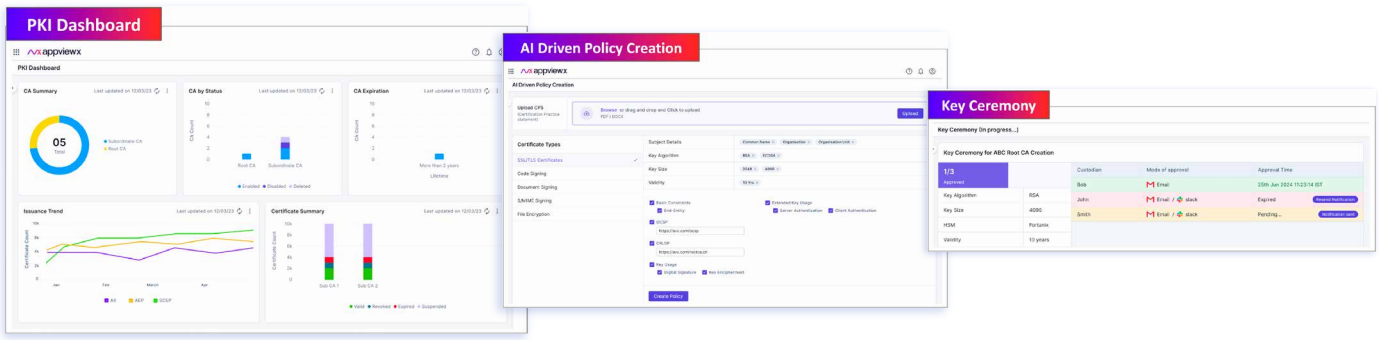
Agile

- Fully integrated CLM automation
- Scale on demand
- IoT scalability and performance
- Built-in Lift and Shift to effortlessly migrate away from legacy PKI offerings (MS CA, EJBCA)
- Simple, standardized template-based deployment - with support for custom configurations

Secure

- Highly available, secure and compliant Infrastructure
- Backed by FIPS 140-2 Level 3 HSMs to ensure full security and performance
- Flexible HSM integration support (Bring your own HSM)
- Secure Admin/Custodian Management (M of N control)
- Airgapped/Offline Root CA for high-security environments
- Real-time OCSP

Modernize and simplify your Private PKI | **Rapidly Issue, Scale, and Adapt** | **Strengthen Security and Maintain Compliance**



Centralized console for Administrators to securely monitor, manage, and maintain strict control over CAs.

Modern and Agile PKI

- Enterprise-grade private Certificate Authority (CA) provisioned in minutes via virtual key ceremony
- Support for multi-cloud enrollment and management
- CAs provisioned in regions of choice
- PQC-enabled issuance - support for the new NIST-standardized PQC encryption algorithms - Dilithium, SPHINCS+ (as well as Falcon) for PQC readiness
- Simple, flexible template-based deployment for CAs and end-entity certificates to ensure secure, standardized PKI operations across the organization
- Highly customizable certificate templates, policies and fields, including extensions, keys, key lengths, and validity periods (i.e. flexible support for custom IoT certificate attributes and device-based policies)
- Lift and Shift to seamlessly replace existing in-house PKI with AVX ONE PKIaaS
- Support for native Windows Auto-enrollment and silent provisioning of certificates without an additional client footprint

Robust and Secure CA Environment

- Highly secure FIPS 140-2 Level 3 HSMs to ensure safety of CA Keys and accelerate cryptographic operations.
- Support for Airgapped/Offline Root CA for high-security environments to minimize risk of exposure and compromise
- Facilitates Bring Your Own Key (BYOK) allowing you to retain full control over your encryption keys
- X.509 CRL and real-time OCSP certificate validation
- Strict access and security policies with multi-factor authentication to access all CAs
- Utilizes the M of N concept for strict, authorized control over all CA key operations
- Template-based CP (Certificate Policy) and CPS (Certificate Practice Statement) for audits and compliance

Simplified PKI Management - Fully Integrated with AVX ONE CLM

- Single-pane-of-glass view for complete certificate discovery, lifecycle automation, and policy-driven control
- PQC CLM - Full support for discovery and CLM automation for PQC-enabled certificates
- Centralized and automated CLM across diverse environments such as multi-cloud network devices, DevOps, containers, etc.
- CA-agnostic CLM for all certificate types, across all of your public and private CAs from one platform

Highly Available and Scalable Infrastructure

- IoT scalability and performance—the ability to provision certificates at speed and massive scale
- Designed to auto-scale with enterprise needs, handling large volumes of certificate requests efficiently and without compromising performance
- Certificate Authority (CA) load sharing for high availability, optimal performance, redundancy, and scalability

Extensive Native Integrations

- Flexible integrations with leading HSMs (Fortanix, Utimaco, Entrust, Thales) and cloud solutions (AWS CloudHSM, Azure Key Vault) - including support for bring your own HSM
- Seamless API-based integration with multiple CAs, Windows Auto-enrollment, cloud services, DevOps toolchains, ITSM, SIEM, and MDMs.
- Auto-enrollment protocol support – EST, SCEP, NDES, Windows Auto-enrollment, CMP, ACME

AppViewX Inc.,

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226

appviewx