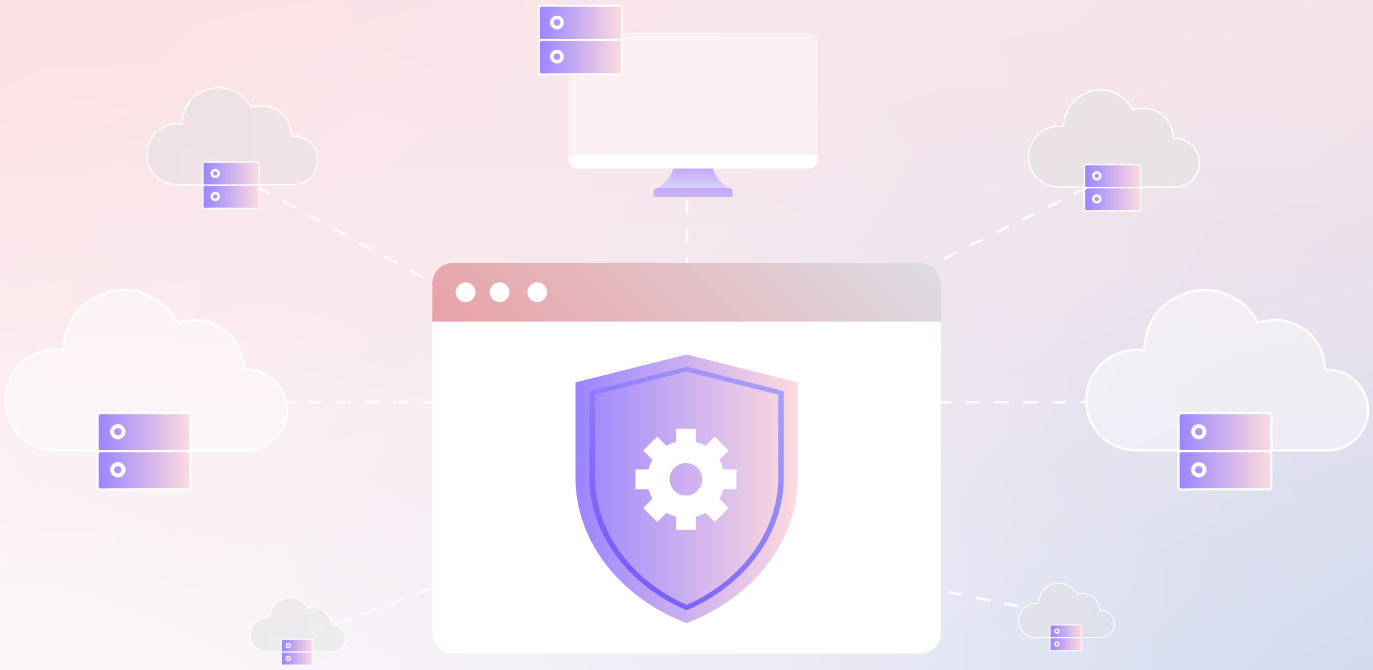
appviewx

Solution Brief

AVX ONE CLM

Automated and Intelligent Certificate Lifecycle Management for Crypto-Agility and Machine Identity Security



Overview

Public key infrastructure (PKI) and digital certificates are the foundation of data security and digital trust in modern-day business. They play the critical role of providing trust for machine (non-human) identities—authenticating workloads, applications, services, machines, and devices—and encrypting their communications. These digital identities ensure that all our online transactions and communications, such as banking, healthcare, retail and more, are confidential and secure. Managing them responsibly is critical for ensuring data security, maintaining uninterrupted services, preserving customer trust, and driving business growth.

However, certificate management has grown increasingly complex over the recent years. Many organizations are struggling to take control of their certificate ecosystems, exposing themselves to certificate-related outages, security breaches, and compliance issues.

Several factors have led to the growing complexity and challenges in certificate lifecycle management:

- The widespread adoption of cloud services, microservices, containers, and IoT has driven a steep rise in the volume of digital certificates. Factoring in new PKI use cases like IoT, organizations are now provisioning thousands to upwards of millions of certificates at speed. Controlling this certificate sprawl and managing certificates at scale, especially in hybrid and multi-cloud environments with distributed workforces, is a massive challenge facing organizations today.

- Certificate management encompasses the entire lifecycle of a certificate, from enrollment and provisioning to renewal or revocation. Many organizations still use manual processes, such as spreadsheets, homegrown tools, and CA-provided solutions for certificate management, which are often ad-hoc and unreliable. They create serious gaps in certificate lifecycle management, leading to outages, vulnerabilities, and non-compliance.

- Winds of change continue to blow in the PKI industry, presenting unique challenges:
    - The CA/Browser (CA/B) Forum has approved Apple's proposal to gradually reduce public TLS certificate lifespans from today's 398 days down to just 47 days by 2029. This means, by March 15 2029, certificates will need to be renewed almost every month—a big shift from the once-a-year cadence that PKI and security teams are used to now.
    - Google and Mozilla's decision to distrust Entrust CA due to compliance failures is driving enterprises to adopt a multi-CA strategy and quickly migrate to new trusted CAs to avoid service disruptions, highlighting the need for CA and crypto-agility.
    - With NIST releasing the first set of post-quantum cryptography (PQC) encryption standards, the push for PQC readiness with crypto-agility has intensified.
    - The compliance landscape is evolving rapidly with new mandates and updated standards across industries for data privacy and security, calling for more streamlined CLM operations.

Current Challenges in Certificate Lifecycle Management

Poor Visibility and Insights

Visibility is non-negotiable for efficient certificate lifecycle management in distributed hybrid multi-cloud environments. Centralized visibility into all the certificates in the infrastructure is essential for complete control over the certificate ecosystem. Insight into certificate information, such as—where a certificate is located, when it expires, the CA that issued it, the cypher suite or crypto algorithm, and the endpoint(s) it is provisioned to—helps proactively monitor certificates for expiry and vulnerabilities. However, when using spreadsheets, homegrown monitoring tools, and CA-provided CLM solutions, manually discovering certificates from all sources across the infrastructure and capturing crucial information becomes difficult, creating security blind spots. As a result, many certificates expire or go rogue, causing application outages and security breaches.

Manual Inefficiencies

Manually managing certificate lifecycles is slow, error-prone, and inefficient. Resorting to manual processes for critical certificate lifecycle management operations like enrollment, provisioning, renewal and revocation can delay applications and devices from going online quickly, and can also result in downtime, outages and security weaknesses. As the volume of certificates increases and their lifespans reduce, certificate renewals and provisioning become far more frequent, requiring close monitoring and significant manual effort. Spreadsheet-based certificate lifecycle tracking systems can stretch over thousands of rows, increasing the likelihood of missed renewals, provisioning delays, human error, misconfigurations, and vulnerabilities.

Typically, many cross-functional stakeholders are involved in developing, deploying, and managing a single application. Likewise, multiple groups handle the certificates used to secure applications. Given the amount of people and effort involved, the margin for delays, errors, and misconfigurations is significantly higher when certificates are requested and provisioned manually.

Weak Policy Enforcement

Enforcing a PKI policy is critical to regulating access and controlling certificate issuance. Manual processes do not support creating or enforcing certificate policies and templates, leading to variations in crypto standards, use of vulnerable self-signed certificates, and procuring certificates from unapproved CAs. Manual processes also do not allow establishing certificate ownership, another critical aspect that helps enforce accountability for certificate actions and prevent unauthorized access. Lack of clear ownership and approval workflows leads to unknown certificates expiring and unauthorized or rogue certificate issuance, creating security risks and non-compliance issues.

Lack of Crypto-Agility

As the PKI landscape evolves, so should certificate lifecycle management. This is why crypto-agility is critical. It helps stay ahead of the changes and adapt quickly without any impact on the business. When cryptographic algorithms are updated or deprecated, it is essential to have the ability to replace algorithms quickly at scale. Or, when a CA is distrusted, the ability to move to a new trusted CA immediately is key to prevent outages and service disruptions. Manual processes do not provide the necessary visibility, automation, and policy control required to build this level of crypto-agility, leaving organizations struggling to respond to cryptographic weaknesses, compromises and security breaches.

Simplify Certificate Lifecycle Management and Build Crypto-Agility with AppViewX AVX ONE CLM

Complete Visibility, Unrivaled Automation, and Continuous Control

AppViewX AVX ONE CLM is an automated certificate lifecycle management (CLM) solution designed to simplify PKI and machine identity management across complex hybrid multi-cloud environments. It provides holistic visibility, end-to-end automation, and policy-driven control to ensure trust for machines, workloads, applications, and cloud services.

By streamlining CLM for all certificate types across leading public and private Certificate Authorities (CAs), AVX ONE CLM enhances enterprise-wide crypto-agility, mitigates machine identity risks, and empowers cross-functional teams to focus on innovation and growth.

AVX ONE CLM Key Features

- Smart Discovery
- Centralized Certificate Inventory
- Actionable Insights Dashboards (such as 47-Day TLS, PQC, and Enterprise Crypto-Scoring)
- Closed-loop Automation Workflows
- Intuitive Self-Service
- Zero-touch Policy Enforcement
- Alerting, Reporting, and Logging
- Extensive Native Integrations and Auto-Enrollment Protocol Support
- Secure Key Management

Features and Benefits of AVX ONE CLM

1. Smart Discovery to Eliminate Security Blind Spots

Being aware of the entire certificate inventory is key to preventing certificate-related outages and security risks. AVX ONE CLM helps discover all public and private certificates across your hybrid multi-cloud environments through an automated discovery process. It provides flexible scanning methods to help discover certificates from your IP networks, managed devices, cloud accounts, CAs, Kubernetes clusters, and CT logs. You can run these scans on demand or at scheduled intervals to continually discover new certificates. Smart Discovery also allows you to optimize the discovery process by adjusting scanning intensity, running discovery scans in smaller batches, or setting discovery rules to balance discovery time and ensure smooth network performance. Automated and CA-agnostic certificate discovery helps build complete visibility and eliminate the risk of unknown, rogue, and non-compliant certificates.

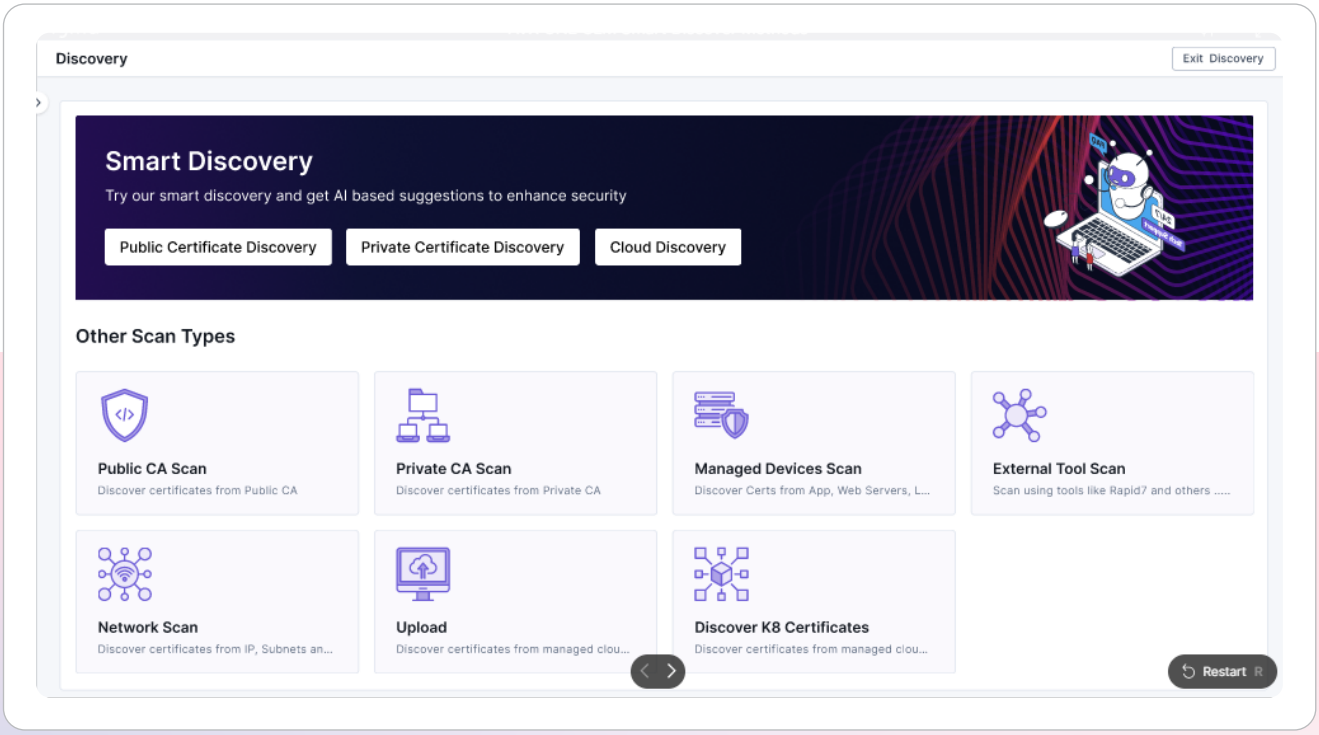


Fig1.Smart Discovery

2. Centralized Certificate Inventory for Holistic Visibility

To help maintain complete visibility of the certificate ecosystem, AVX ONE CLM consolidates all discovered certificates in a centralized inventory along with essential certificate information such as the certificate location, owner, expiry date, chain of trust, crypto standards, and more. This inventory serves as a single source of truth for managing both public and private trust certificates, ensuring full CA and crypto-agility. You can customize the inventory to display over fifty different columns of certificate-related details and metadata based on your need for granular visibility. You can also segment certificates into groups, such as server, client, code signing, and device certificates to simplify renewals and revocations. Having single-pane-of-glass visibility helps monitor certificates effectively for expiry and vulnerabilities to remediate issues in time.

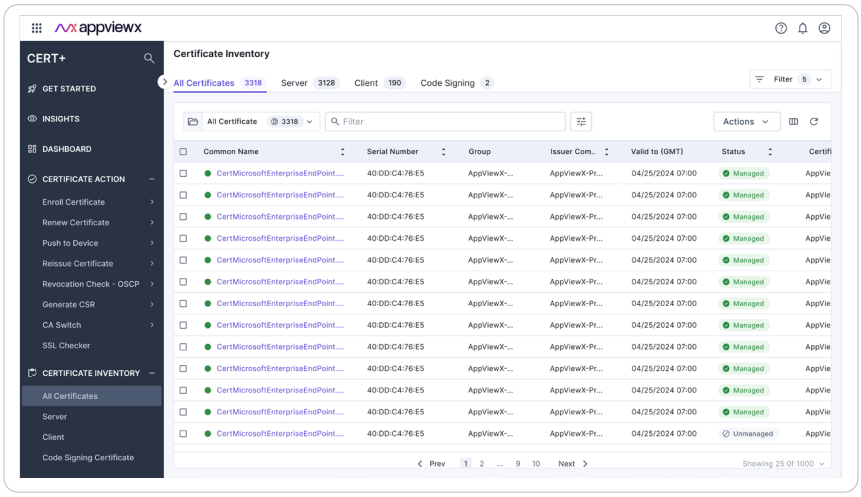


Fig2.1. Centralized Certificate Inventory

3. Industry-Leading Dashboards for Crypto Insights

When it comes to keeping up with changing PKI trends, having just visibility of certificates is not enough. You also need insights into your organization's cryptographic health. AVX ONE CLM is built with the intelligence to provide you with powerful Insights dashboards. These graphical dashboards help you assess your overall crypto health, and understand where your organization

stands in terms of preparing for 47-Day TLS certificates and PQC readiness. You can simply click on any of the widgets within the Insights dashboard to drill down and take appropriate action, optimizing your security and compliance posture.

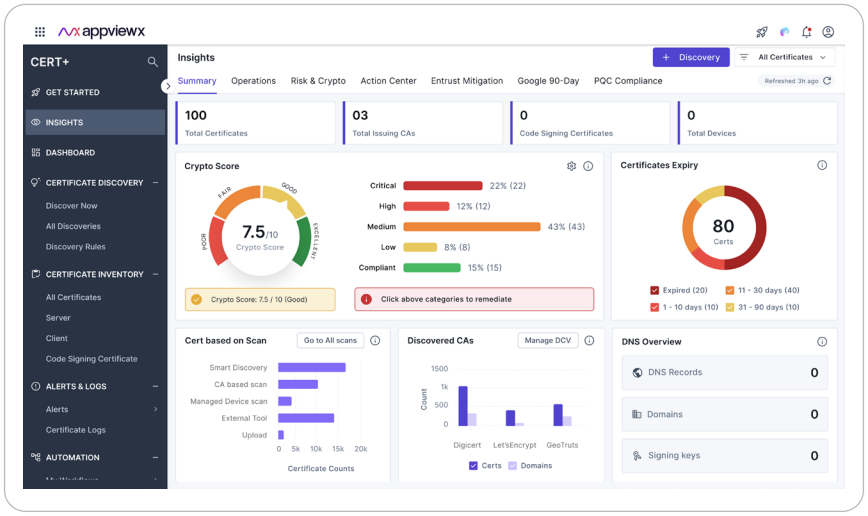


Fig3.1. Insights Dashboard

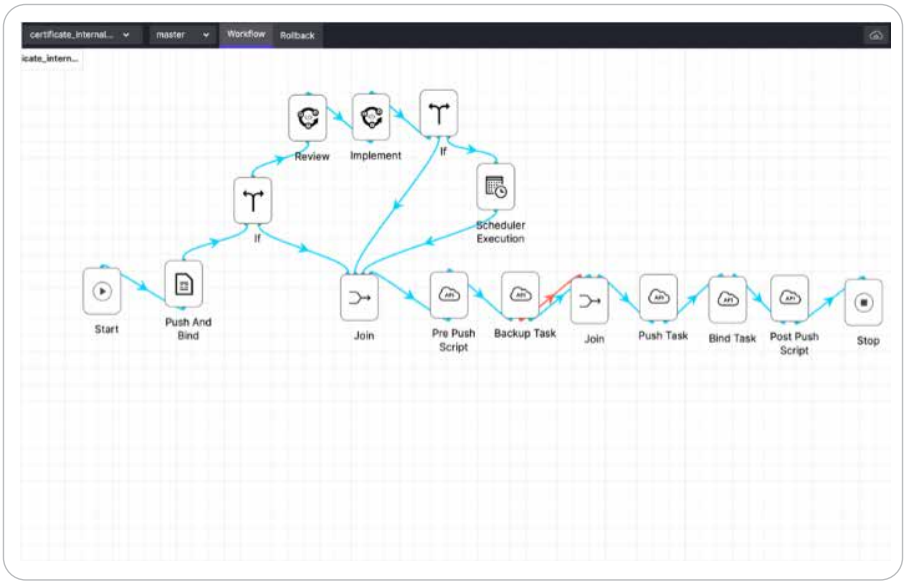
4. Closed-loop Automation for Accuracy and Higher Efficiency

The core of AVX ONE CLM is its advanced automation capabilities. With easy-to-use automation workflows, REST APIs, pre-built integrations, and auto-enrollment protocol support (i.e. Windows auto-enrollment, ACME, SCEP, EST, etc.), AVX ONE CLM automates every stage of the certificate lifecycle. Flexible and out-of-the-box automation workflows help tailor CLM automation to your business requirements. One of the key highlights of AVX ONE CLM's automation is its ability to automate end-to-end, as a closed loop, starting with certificate enrollment and issuance and concluding with the last mile steps of certificate provisioning, like binding the certificate to the right application or endpoint. Note that the last mile of certificate binding is still a manual step in many CLM solutions in the market, requiring human intervention. Using AVX ONE CLM's automated workflows, you can configure any number of CLM actions, triggers, and approvals, reducing administrative burden, preventing misconfigurations, and allowing IT teams to focus on other critical tasks.

AVX ONE CLM also promotes effective cross-functional operations through certificate self-service. It provides a robust user portal featuring custom branding, personalized dashboards, and automation capabilities to allow cross-functional teams to generate, request, and issue certificates from approved Certificate Authorities (CA) on their own—significantly simplifying certificate operations for all users across the organization.

AppViewX understands that CLM automation is critical for building crypto-agility and quickly adapting to big changes like managing shorter-lived certificates, switching between CAs, and transitioning to post-quantum cryptography at scale. To help you rewire quickly and respond to changes or threats with confidence, AVX ONE CLM automation enables crypto-agility through:

- Auto-renewals for frequently renewing and provisioning shorter-lived certificates
- Ready-to-consume or custom workflows that can automate CLM functions according to your needs
- CA-Switch feature to quickly and seamlessly switch from one CA to another (in just 5 simple steps!)
- PQC certificate CLM processes to ensure PQC readiness and help you upgrade your cryptographic infrastructure to PQC at scale



5. Robust Policy and Compliance Engine for Security and Compliance

Standardizing certificate processes is key to regulating access to certificates and keys and eliminating security and compliance issues. AVX ONE CLM allows PKI administrators to define and enforce an enterprise-wide PKI policy to ensure adherence to best practices in certificate issuance, use of crypto-standards, and access privileges, eliminating weak and non-compliant certificates. Along with policies, AVX ONE CLM also provides role-based access control (RBAC) to enable conditional access and ensure secure certificate provisioning. You can tag certificates with additional metadata and group them based on business needs, applications, or teams for easy access and policy management.

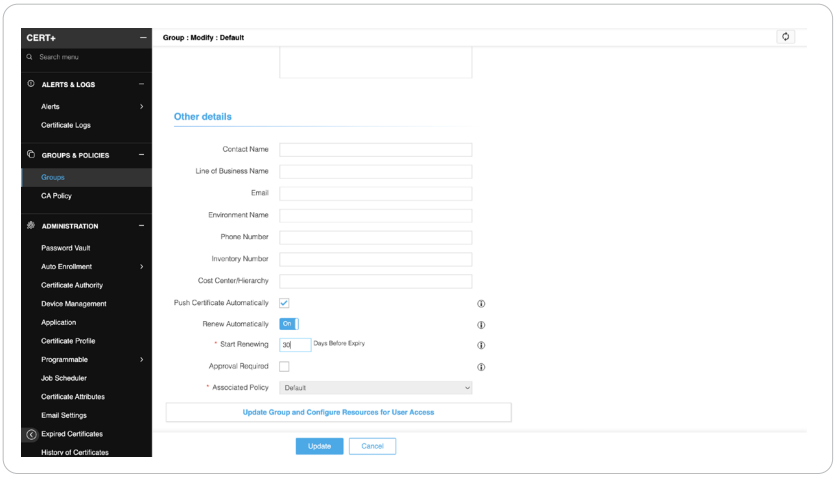
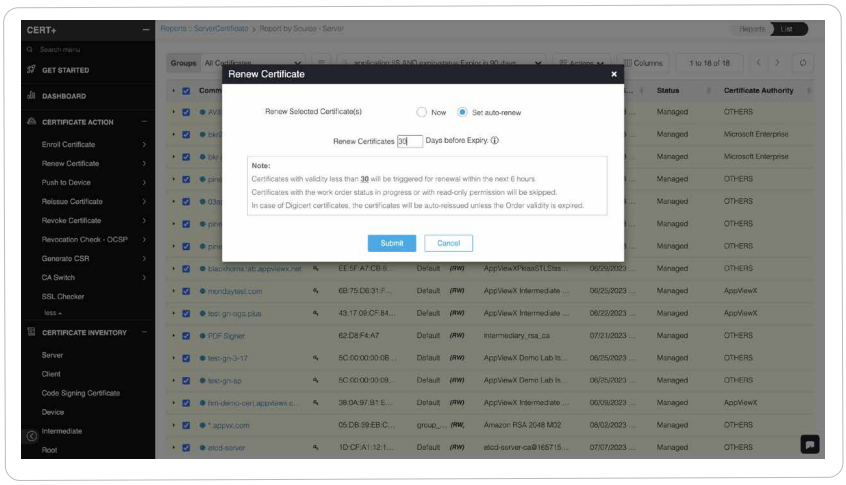


Fig5.1. Policy Settings



6. Alerting, Reporting, and Logging for Streamlining Audits and Compliance

AVX ONE CLM provides custom alerts for certificate expiry notifications to ensure timely renewals, approvals, or escalations. This helps stay on top of expiring certificates to prevent application outages and security weaknesses. Alerts can be delivered via emails for manual actions or via simple network management protocol (SNMP) traps for automation and integration with ITSM and SIEM solutions.

AVX ONE CLM also provides audit logs and pre-configured dashboard reports for audits and regulatory compliance. Users can customize these reports as per their needs. Audit logs record all certificate-related activities and configuration changes to make both internal and external audits easier. These logs can be transported into enterprise log storage systems for long-term storage as per enterprise policies. You can also generate periodic reports on certificate and key compliance to keep up with industry standards.

7. Extensive Native Integrations and Auto-Enrollment Protocol Support to Cater to Multiple CLM Use Cases

AVX ONE CLM provides seamless API-based integrations with multiple Certificate Authorities, cloud services, DevOps toolchains, ITSM, SIEM, and MDMs to automate certificate lifecycle management. It also offers auto-enrollment protocol support— ACME, EST, SCEP, Native Windows Auto-enrollment, and Microsoft Intune—to simplify certificate enrollment for DevOps and IoT. Additionally, AVX ONE CLM fully integrates with AVX ONE PKIaaS a turnkey, modern, and compliant PKI-as-a-Service for all private trust certificate use cases.

8. Secure Key Management for Robust Data Security

AVX ONE CLM enforces secure key management by generating them either on the target machine, key management system (KMS), or in the hardware security module (HSM). Automated workflows pushing certificates and keys to associated devices further minimize human access to keys, preventing unauthorized key roaming and any potential key compromise.

Flexible Consumption Models

AVX ONE CLM can either be consumed as a service or deployed in the enterprise network. Irrespective of how the solution is consumed, the features and benefits remain the same and are available from one centralized console.

SaaS – Operated by AppViewX

Available as a service, AVX ONE CLM is fully managed and updated by AppViewX. Customers can directly set up an account, instantly start using it and realizing value to solve certificate management challenges.

On-Prem and Hosted Deployment

The CLM automation capabilities of AVX ONE CLM can also be deployed within a customer's environment in hypervisor-based VMs, private clouds, or public clouds using AWS, GCP, Microsoft Azure, and others.

Get Started Today

Partner with the leader in automated certificate lifecycle management and PKI solutions committed to the success of Managed Security Services Providers.

Visit www.appviewx.com/partners to get started or contact info@appviewx.com to become a partner.

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