appviewx

AVX ONE Certificate Lifecycle Management (CLM): Closed-Loop Automation

Robust certificate lifecycle management automation to boost efficiency, minimize risk, and ensure crypto-agility

The Winds of Change Continue to Reshape the PKI and CLM Landscape

As enterprise organizations increasingly adopt application modernization, cloud initiatives, containerization, IoT, and AI strategies, the demand for digital certificates has skyrocketed. Public Key Infrastructure (PKI), once a behind-the-scenes player, has now become a critical component of enterprise security. From securing access to remote servers, cloud applications, DevOps workloads, and APIs to securing VPNs, corporate WiFi networks, and email communications—certificates are everywhere, safeguarding our digital infrastructure and ensuring trust in our systems

But this critical foundational technology that supports identity-first security is now on the verge of rapid disruption, driven by powerful trends such as:

- **Shorter TLS certificate validity periods proposed by industry giants like Google and Apple**
- **NIST's release of post-quantum cryptography (PQC) standards and the race to achieve PQC readiness by 2030 when today's widely used encryption algorithms are slated for deprecation**
- **New compliance mandates from the Certificate Authority/Browser (CA/B) Forum, including those for code signing and S/MIME**
- **Evolving security and data privacy regulations that demand streamlined, compliant, and efficient certificate lifecycle management**

These trends are unlike anything we have seen before. They are new problems that demand innovation and agility. More and more CISOs are now realizing that PKI can no longer operate quietly behind the scenes. And, here's the big question facing every CISO today: Is our PKI agile enough to keep up? Can our CLM system adapt quickly to changes without impacting business operations?

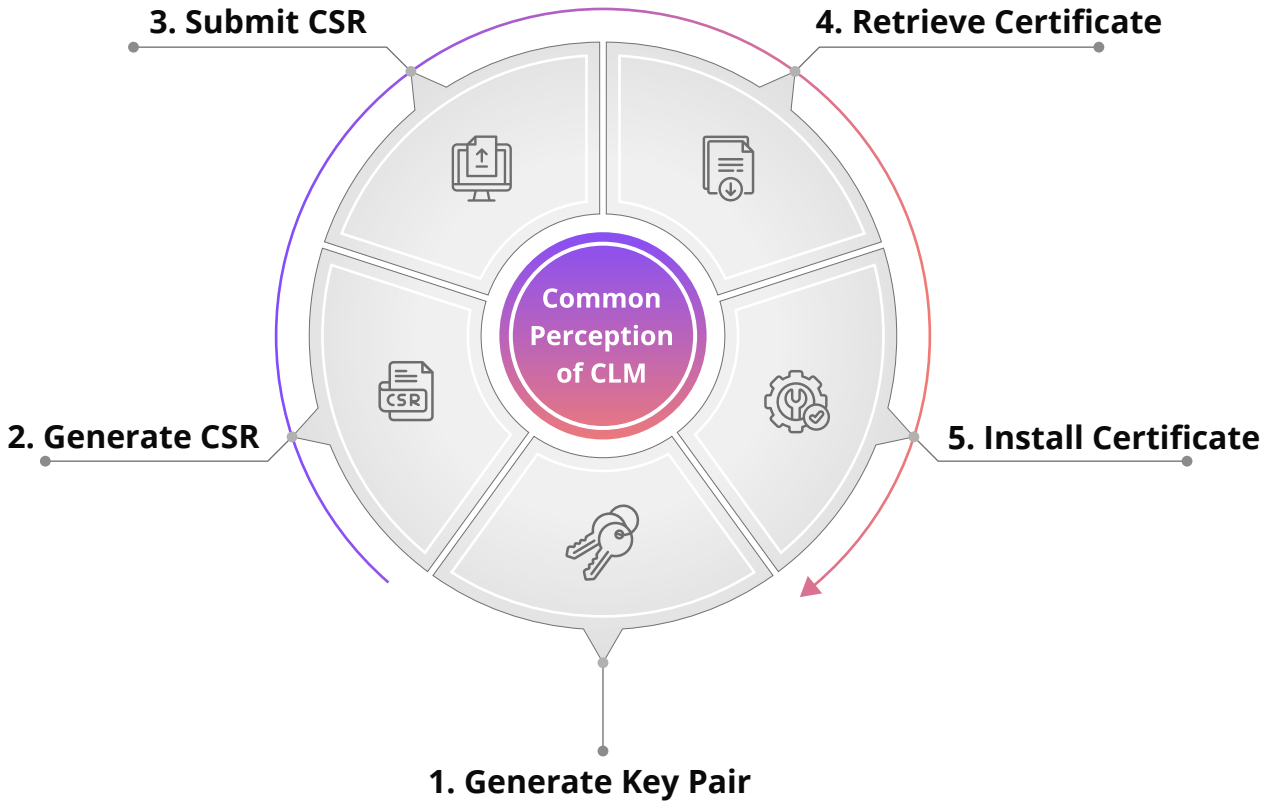
Crypto-agility isn't just a buzzword. It's a true measure of how resilient and future-proof your PKI and cryptographic systems are. Yet, most organizations are far from achieving crypto-agility. In fact, many are still struggling with basic questions about their certificate and PKI ecosystems, such as what certificates do we have? Where are they stored? How are they being used? Due to this lack of clarity, many continue to grapple with operational inefficiencies, costly outages, security risks, and compliance violations.

Why is Certificate Lifecycle Management Challenging for So Many?

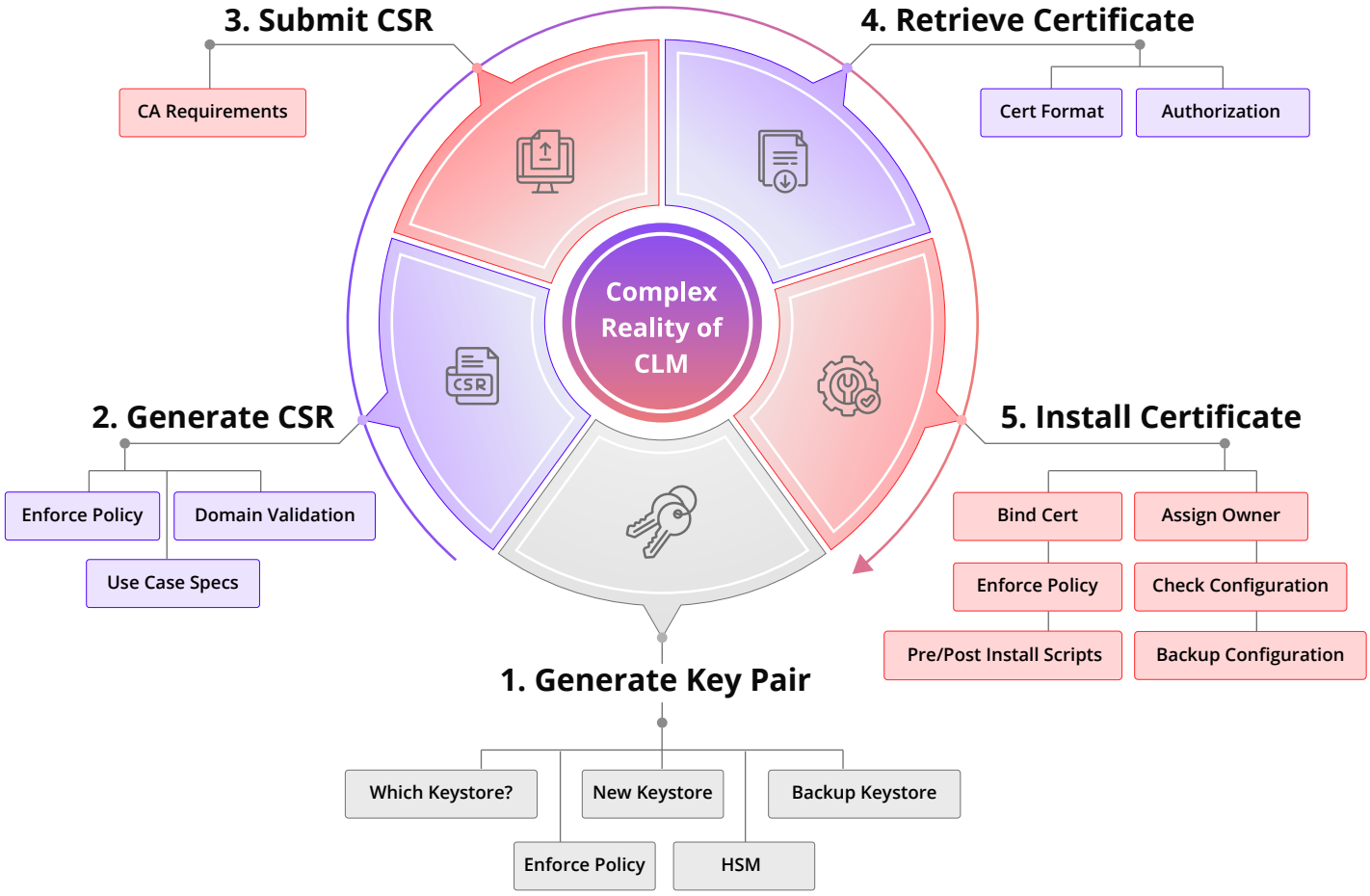
Managing certificate lifecycles might seem straightforward, but it's anything but simple. PKI and security practitioners know this better.

Mechanics of Managing a Certificate

Common perception of managing a certificate is that it is a simple, admin task at face value.



But in reality, it is multi-faceted and complex.



Many organizations manage this multi-faceted process with spreadsheets, homegrown tools, or fragmented solutions offered by various Certificate Authorities (CAs). While these methods may have worked in the past for a handful of certificates, they're simply not up to the task anymore. As businesses scale and adopt hybrid and multi-cloud strategies, the number of certificates to manage is skyrocketing. Manual processes are too outdated, inefficient, and siloed to keep up with the scale and certificate management demands of today's dynamic IT environments and endpoints.

Think about it: Tasks like generating and submitting the CSRs, retrieving the certificates, and installing them are crucial to keeping applications and devices secure and online. However, when managing these processes manually for a large volume of certificates, delays and mistakes are almost inevitable. A missed certificate renewal or a configuration

mistake during provisioning can disrupt critical applications and devices, directly impacting business operations and revenue.

And here's the catch: With Google and Apple now pushing for shorter certificate validity periods, the challenges will only grow. With shorter-lived certificates, renewals and provisioning will become far more frequent (four times a year or even on a monthly basis), demanding constant attention and significant manual effort. When tracking thousands of certificates across sprawling spreadsheets or siloed CA tools, it's only a matter of time before something falls through the cracks, leading to expired, rogue, or non-compliant certificates.

It's not just about volume, though. Managing certificates often involves multiple teams—developers, IT, DevOps, security, and more—all working together to deploy and secure machines, applications, workloads, services and more. A single application might involve input from multiple groups for development, deployment, delivery, and ongoing management. Each group has its own role in securing the application with certificates. With so many people involved, the potential for misconfigurations, delays, and discrepancies in cryptographic standards is amplified when processes aren't policy-driven or automated.

Another major challenge is managing certificates across third-party systems. In a typical IT operation, enterprises use various solutions for authentication, authorization, monitoring, ITSM (IT Service Management), and SIEM (Security Information and Event Management). For seamless operations, certificate lifecycle management must integrate with these systems. However, with manual processes, integration isn't an option. Imagine handling ITSM ticketing tasks manually for every certificate renewal or update—it's slow, tedious, and error-prone. This lack of integration creates operational silos and disconnected workflows, leaving organizations grappling with inefficiencies.

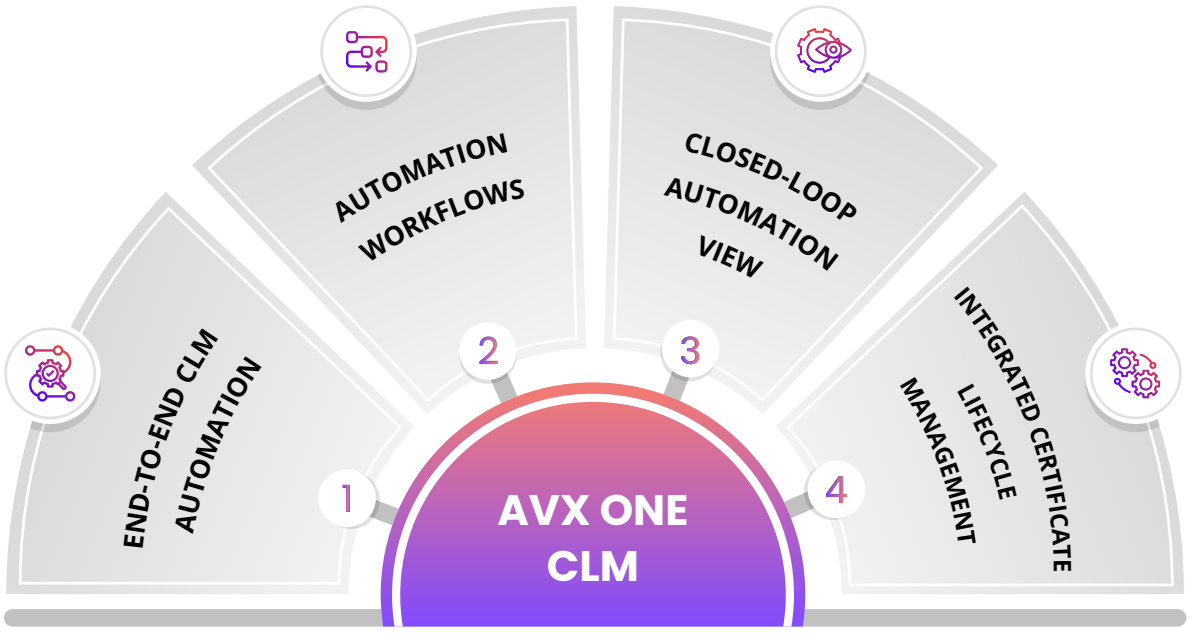
The result of insufficient certificate management is a process that feels like it's working against you, not for you. It is essential to also understand that manual methods aren't merely inefficient—they completely undermine crypto-agility, leaving your digital infrastructure vulnerable and unprepared for the demands of the future.

Agility at Its Core: The AVX ONE CLM Automation Advantage

Certificate lifecycle management (CLM) is far more challenging than it often gets credit for. As we have seen before, it's a complex process with a lot of moving parts. The truth is, most organizations are either dealing with disruptive certificate-related outages and vulnerabilities or pouring countless man-hours into preventing them—an exhausting game of whack-a-mole. And in the middle of this chaos, the idea of achieving crypto-agility seems almost impossible. But here's the thing: there's a better way to do this - Automation.

AVX ONE CLM Delivers Unrivaled Automation

AppViewX understands that automation is the ultimate true game-changer when it comes to tackling the challenges of modern-day certificate lifecycle management. It is key to achieving crypto-agility, mitigating vulnerabilities, preventing outages, and preparing for Post-Quantum Cryptography. We also know that CLM isn't a one-size-fits-all solution. Every organization has unique use cases and requirements and AppViewX supports its customers to solve their specific challenges with AVX ONE CLM, the most advanced certificate lifecycle management (CLM) solution, with powerful, flexible, and extendable automation capabilities.



1. End-to-End CLM Automation

AVX ONE CLM is designed to automate all CLM operations from start to finish. It can handle every step of the certificate lifecycle—from generating CSRs and issuing certificates to the critical “last mile” of binding the certificate to the appropriate application or endpoint. It can even automate the intricate steps in between, such as pre and post validation checks. Unlike any other CLM solutions in the market, which often require manual intervention for certificate binding, AVX ONE CLM ensures this step is fully automated too, eliminating any gaps or errors.

Here’s an example: With real-time monitoring, AVX ONE CLM continuously tracks certificates for their expiry and keeps you informed about their expiry status through an intuitive dashboard. When a certificate is about to expire, AVX ONE CLM takes charge. It identifies the expiring certificate and promptly notifies its owner via a built-in alerting system. It then executes the entire renewal process automatically. From generating the key pair and CSR to submitting it to the appropriate Certificate Authority (CA), retrieving the renewed certificate, installing it, and binding it to the correct endpoint, every step is seamlessly managed. Each of these steps is governed by policy, which is automatically enforced to maintain consistency, standardization, and compliance.

This extent of automation ensures the new certificate is fully configured and ready to use, eliminating the risk of outages caused by expired certificates. More importantly, the end-to-end automation makes the system crypto-agile to adapt to sudden changes and new requirements.

In addition to automating lifecycle operations, AVX ONE CLM conducts compliance checks against predefined policies and criteria. If a rogue certificate is detected, it will automatically be flagged or if a provisioning issue was to occur, it can perform automatic rollbacks, ensuring your cryptographic infrastructure remains secure and aligned with organizational standards.

The full-spectrum automation of AVX ONE CLM simplifies the complex process of managing certificate lifecycles at scale, helping boost productivity and mitigate security weaknesses and outages.

2. Automation Workflows

Automation workflows are a smarter alternative to manual approaches in certificate lifecycle management. AVX ONE CLM automation workflows are second to none, designed to deliver complete visibility, robust automation, and full control—critical elements for achieving crypto-agility. They streamline repetitive certificate tasks, ensuring every certificate action is performed with precision and speed. With automation handling critical processes, the risk of downtime and vulnerabilities drops dramatically, and your IT teams can focus on what really matters.

With AVX ONE CLM, you get the flexibility to approach automation your way: either choose from a library of existing workflows (out-of-the-box) or design custom workflows tailored to your unique needs.

- **Out-Of-the-Box (OOB) CLM Workflows**

  AVX ONE CLM offers an extensive catalog of pre-built automation workflows. These ready-to-use workflows are purposefully designed to simplify and streamline the many steps involved in certificate lifecycle management. They're ready to use right out of the box and can also be shared across teams to support common use cases, ensuring consistent and efficient operations across the organization.

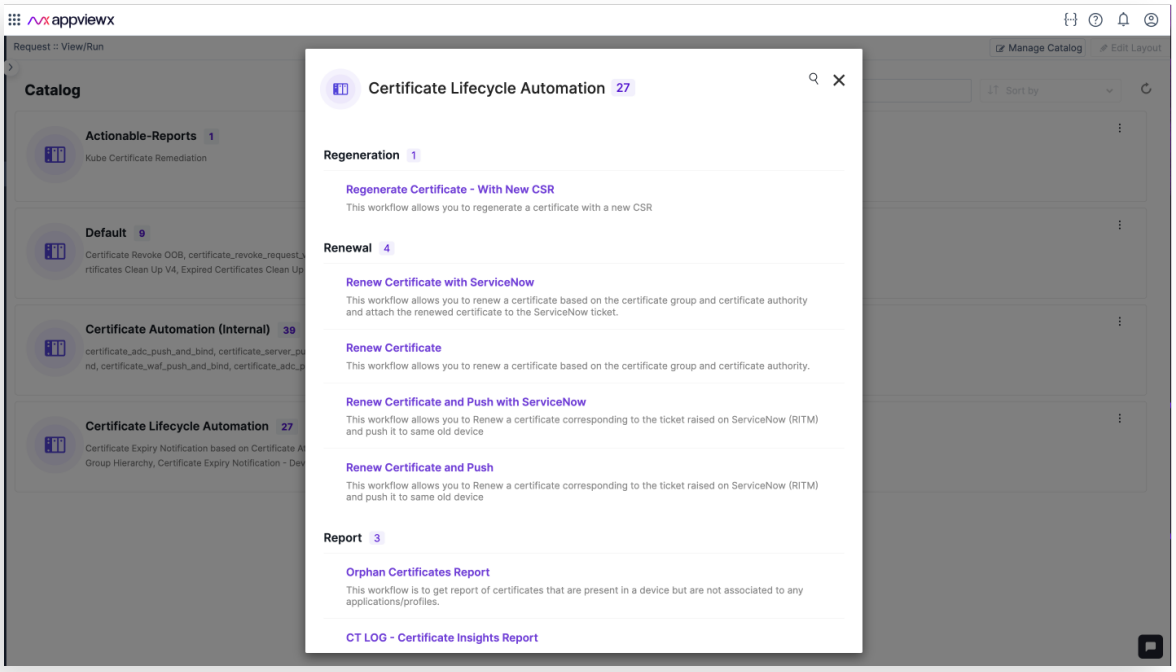
  Here's how simple it is to use Out-of-the-box Workflows:

  1. Select an automation workflow from the Workflow Catalog. Common examples include:

     a. ***Auto-Regenerating a Certificate***

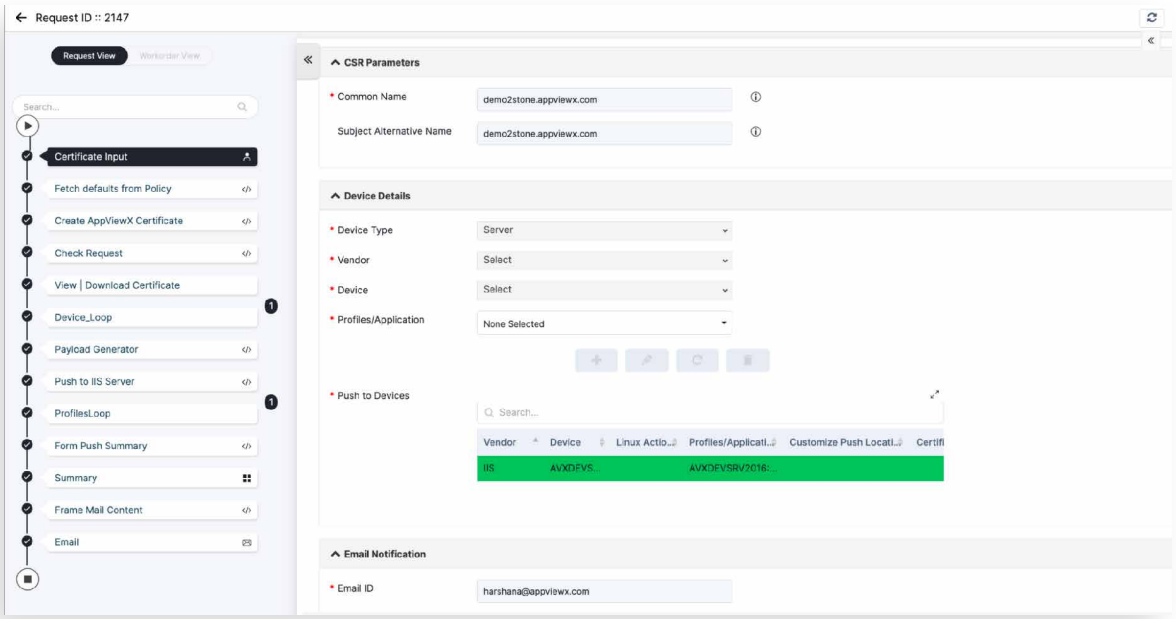
     b. ***Auto-Renewal***

     c. ***Critical Certificate Alerts/Notifications***



Out-of-the-box Workflow Catalog

2. Self-service users can initiate and monitor the automation workflow as it is processed through this interface



Automation Workflow in Process - Self-Service User View
Workflow Type: Automated Certificate Enrollment

- ## Custom CLM Workflows

While the AVX ONE CLM out-of-the-box automation workflows address most standard enterprise use cases, we understand the need for customized and advanced automation. Basic, rigid workflows from other vendors that are more like workstops don't cut it. That's why AVX ONE CLM offers customizable automation through a powerful visual workflow builder. Using this tool, you can design workflows tailored specifically to your organization's requirements. Our dedicated Professional Services (PS) team can help you design or provide training modules to help create custom workflows with ease. In fact, one out of every three AppViewX customers chooses to build custom workflows.

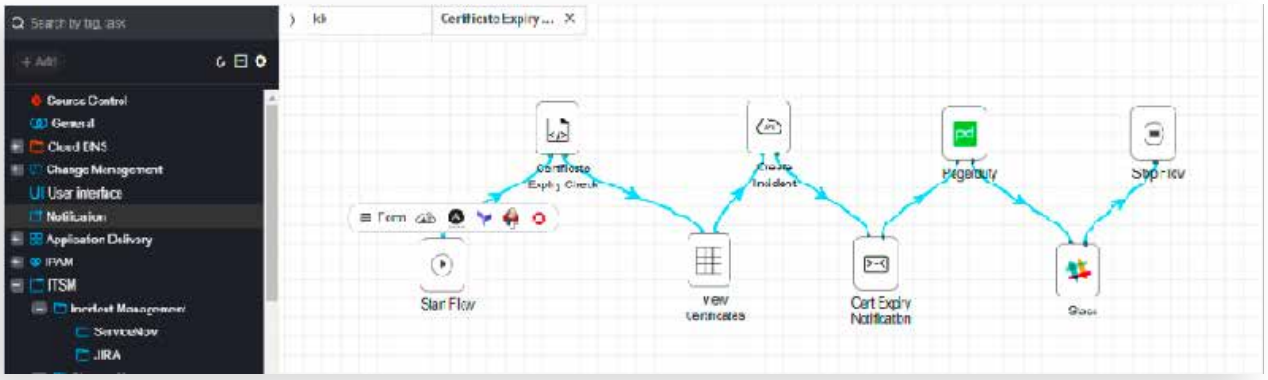
With these intelligent workflows, you can configure any number of actions, triggers, and approval processes. You can implement one-click approvals and renewals, or fully automate the entire renewal and provisioning process as zero-touch, without any manual intervention. Additionally, these workflows are designed to integrate seamlessly with your ITSM, DevOps, and other security and IT tools, allowing you to invoke workflows via API for maximum flexibility and efficiency.

Below is an overview of the Custom Workflows feature:

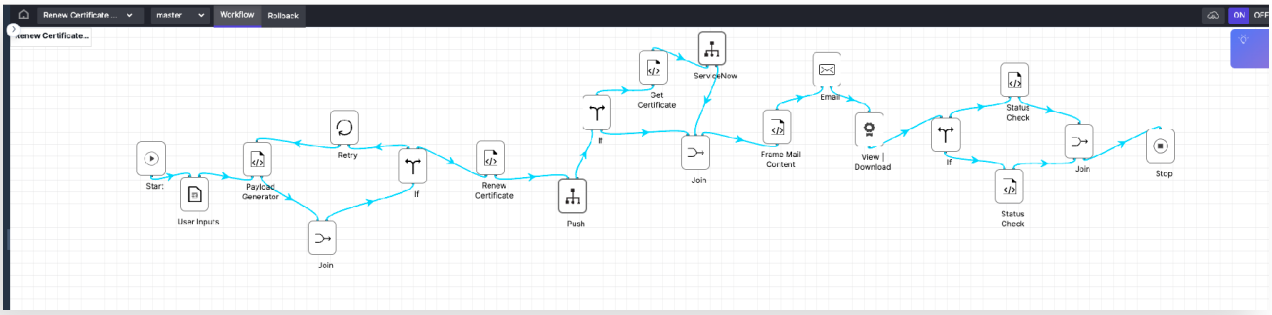
Administrators can access the visual workflow canvas, to clone, customize, or modify a workflow. They also have the option to build their own workflow using the simple drag and drop feature.

Examples:

1. A simple Custom Certificate Expiry Notification Workflow - Admin Canvas View



2. An advanced Custom Certificate Renewal Workflow - Admin Canvas View



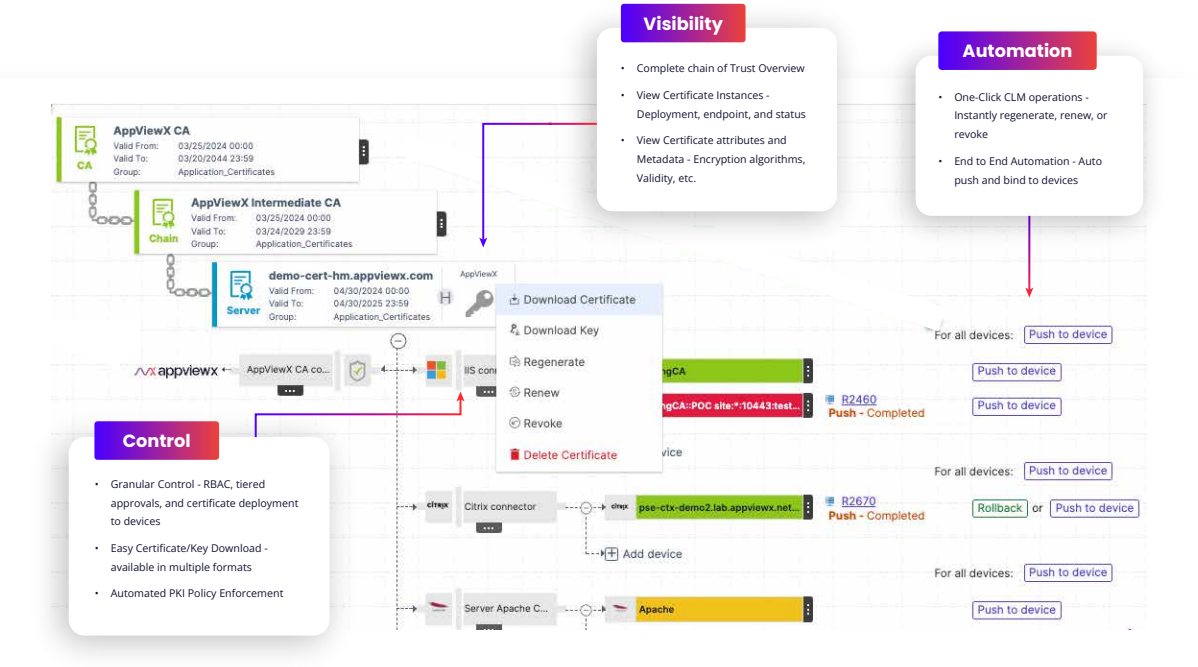
3. Closed-Loop Automation View

To bring automation full circle, AVX ONE CLM offers the industry's only closed-loop automation view. This powerful feature simplifies the entire certificate lifecycle process, bringing crypto-agility—visibility, automation, and control—into a single, unified screen.

- **Visibility**
  View all critical details for a given certificate, including the chain of trust, all instances where the certificate is deployed (including all associated endpoints), certificate attributes and metadata, such as encryption algorithms and validity. You can also see the flow of automation and how actions are triggered.

- **Automation**
  Seamlessly initiate automation workflows for essential tasks like certificate regeneration, renewal, revocation, rollback or pushing to the end device.

- **Control**
  PKI policy with RBAC (role-based access control) and tiered approval mechanisms is automatically enforced for certificate actions. Monitor and control automation progress with live status updates and receive confirmation upon successful completion. Easily download keys or certificates in multiple formats with a single click.



4. Integrated Certificate Lifecycle Management (CLM Ecosystem)

Certificate lifecycle Management typically spans across various vendors, endpoints, Certificate Authorities (CAs), and cloud environments, creating a complex network that requires seamless integration, consistent provisioning methods, and advanced automation.

To meet these demands, AVX ONE CLM offers a centralized, integrated solution for end-to-end certificate lifecycle management.

- **CA-agnostic CLM**

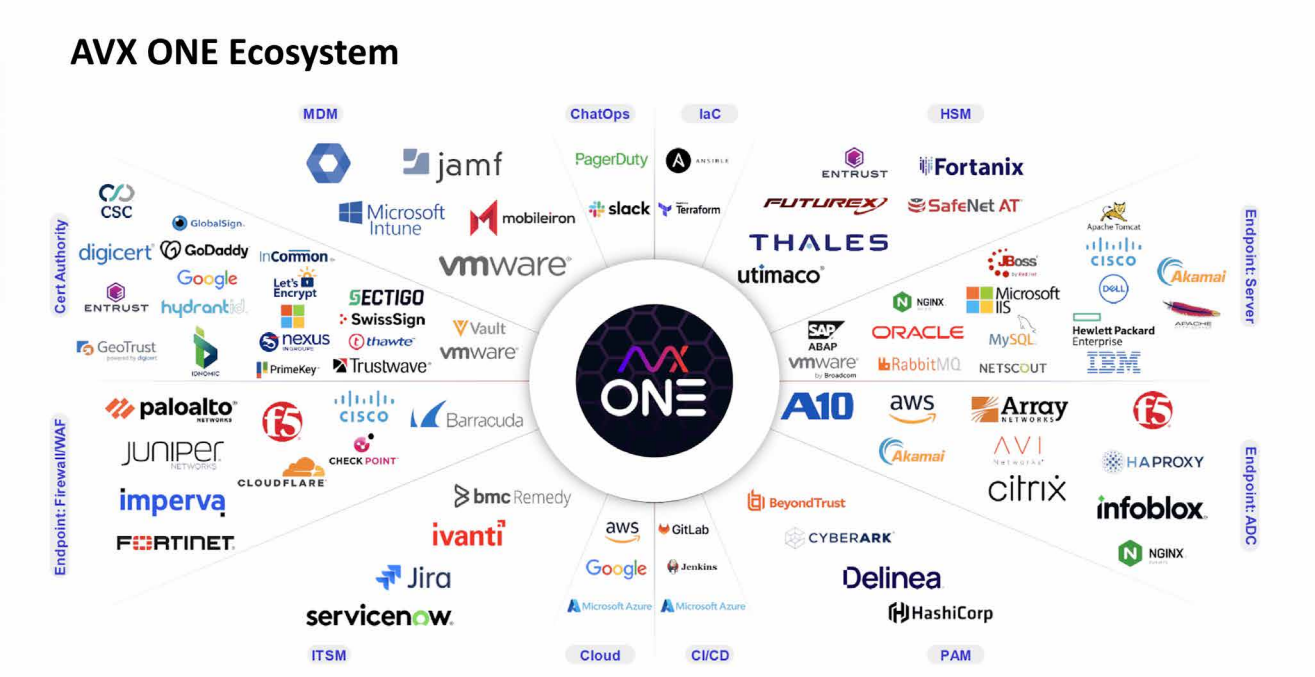
  AVX ONE CLM is CA-agnostic, meaning it lets you manage certificates from any public and private Certificate Authorities (CAs) in one centralized platform. AVX ONE CLM's seamless integration with all major public and private CAs enables the multi-CA strategy and enhances CA agility, making it easy to switch between CAs or diversify your CA providers as needed. Using AVX ONE CLM's unique CA-switch feature, you can seamlessly switch CAs and migrate certificates in just 5 simple steps. In simplifying certificate management across CAs, AVX ONE CLM enhances your overall crypto-agility, helping you maintain a resilient cryptographic infrastructure.

- **Extensive Vendor Integrations and APIs**

AVX ONE CLM offers seamless API-based integrations with a wide range of tools and services, including DevOps toolchains, SIEM systems, and MDM solutions, ensuring end-to-end automation across your infrastructure.

To further streamline operations, AVX ONE CLM integrates with ITSM, CMDB, and ChatOps tools, automating repetitive ticketing and governance processes to reduce manual effort and improve efficiency.

These out-of-the box integrations with vendors help handle certificate enrollment for all end points.



- **Auto-Enrollment Protocol Support**

For automated certificate enrollment, AVX ONE CLM supports all major auto-enrollment protocols, including ACME, EST, SCEP, Native Windows Auto-enrollment, and Microsoft Intune. This makes it easier for DevOps teams and IoT environments to issue and manage certificates at scale efficiently.

- ## Multi-Cloud Support

  Managing certificates across hybrid and multi-cloud environments can be challenging due to the unique identity and security requirements of each cloud platform. AVX ONE CLM simplifies this process by providing seamless integration with major cloud service providers, including AWS, Azure, and Google Cloud Platform (GCP).

  AVX ONE CLM enables comprehensive discovery, visibility, and lifecycle management of certificates across all accounts and services within AWS, Azure, and GCP environments. For federated AWS accounts, it extends certificate management to services across all linked accounts, streamlining operations at scale.

  AVX ONE CLM's in-built integrations with all major certificate authorities, application delivery infrastructure devices such as load balancers, containers and web servers, simplifies certificate onboarding and complete automation of certificate-related processes

- ## Agentless Automation

  AVX ONE CLM provides robust agentless automation capabilities, eliminating the need to deploy additional software agents on individual endpoint devices. By leveraging API-driven workflows, secure communication protocols, a cloud-native architecture, and extensive pre-built integrations, AVX ONE CLM helps manage certificates directly on endpoints, servers, devices, applications, workloads, cloud services and more. This comprehensive approach allows AppViewX to provide more extensive agentless functionality than many of its competitors, who may rely solely on agents. With agentless automation, AVX ONE CLM ensures faster deployments, reduced overhead, and seamless certificate operations.

  AppViewX also offers agent-based capabilities for deeper system-level access, more complex integrations, or specific environments, delivering adaptability and efficiency in your certificate lifecycle management strategy.

Key Business Benefits of AVX ONE CLM Automation

1. **Eliminate Outages and Security Risks**
   End-to-end automation of certificate processes ensures every certificate is renewed on time and rogue or non-compliant certificates are proactively detected and resolved. This eliminates the risk of costly outages and security vulnerabilities.

2. **Improve SLAs with Faster Service Delivery**
   By removing manual processes, automation accelerates certificate issuance, renewal, and provisioning—reducing errors and delays. This ensures faster service delivery, helping consistently meet SLAs.

3. **Reduce IT Workload, Boost Productivity**
   Monitor and control automation progress with live status updates and receive confirmation upon successful completion.

4. **Ensure Continuous Compliance**
   Centralized certificate operations across diverse hybrid and multi-cloud environments, reduces complexity and security gaps, ensuring compliance with industry best practices, security standards, and regulatory mandates.

5. **Achieve True Crypto-Agility**
   Seamlessly adapt to evolving security requirements, whether transitioning to 90-day (proposed by Google) or 47-day (proposed by Apple) certificates or preparing for post-quantum cryptography (PQC). Future-proof your business against emerging threats with flexible and resilient cryptographic strategies.

AVX ONE CLM - Flexible Consumption Models

AVX ONE CLM can either be consumed as a service or deployed as a hosted solution or on-premises. 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 lifecycle 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.

Security simplified with AppViewX

AppViewX is trusted by the world's leading global organizations to ensure application availability, security and compliance with centralized visibility and control of public key infrastructure (PKI) and application delivery services across complex hybrid multi-cloud environments. The AppViewX Platform enables self-service automation and orchestration for NetOps, DevOps, SecOps and application teams to quickly and easily translate business requirements into automation workflows that improve agility, harden security, enforce compliance, eliminate errors, and reduce cost.

Make visibility the cornerstone of your protection mechanism.

https://www.appviewx.com/live-demo/

AppViewX Inc.,

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+1 (212) 951 1146