appviewX

The CISO's Guide to Certificate Lifecycle Management (CLM)

www.appviewx.com

Contents

1. Introduction

In the modern IT environment, data, applications, and devices are no longer bound by the confines of corporate premises or data centers. They are distributed across multiple private and public clouds and the edge. With network perimeters fading away, traditional security frameworks will no longer function the way they used to, thereby putting enterprise data at risk.

Moreover, as organizations tread their paths to digital transformation, some are struggling as they move their legacy solutions to the cloud. The increasing number of regulations and strict compliance standards do not make the situation easy either.

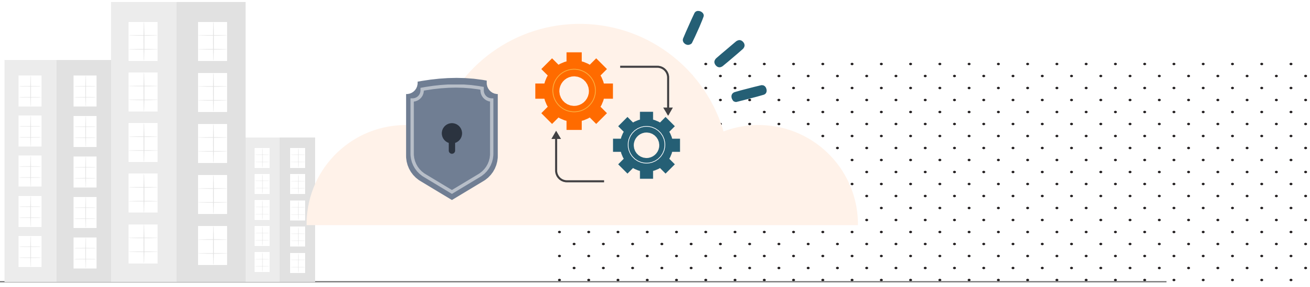
Gartner's Top Security and Risk Management Trends 2021 states that the cybersecurity mesh approach will support over half of digital access control requests. 45% of organizations worldwide will have experienced attacks on their software supply chains, while 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments

There has been a rapid increase in ransomware attacks over the past few years. Recent cyberattacks that have used ransomware as their attack vector include attacks perpetrated against the Colonial Pipeline, Steamship Authority of Massachusetts, JBS (the world's largest meatpacker), the Washington DC Metropolitan Police Department and the Federal Bureau of Investigation.

These attacks had serious consequences on business including financial losses due to shutdown of critical infrastructure, increased cost of goods/services and loss of money due to having to pay the ransom to the hackers and worse.

How do you bridge security gaps to fortify digital transformation so that there is no impact on revenue and business growth?

According to Forbes, "Despite all the warnings and high-profile breaches that state of readiness for most when it comes to cybersecurity is dismal. The need for better cyber-hygiene is evident from using stronger passwords, patching software, employing multi-factor authentication and many other important security steps."



2. The Importance of Managing Digital Certificates and Keys

Digital certificates serve as proofs for a machine's authenticity on a network and help establish and extend trust during communication. These certificates help validate machines' identities and enable them to securely communicate with other devices and applications on the network through encrypted channels.

With valuable data continuously being exchanged between applications in cloud environments, containers, IoT, and mobile devices, it is important for organizations to secure this machine-to-machine communication. This is achieved by protecting and diligently managing digital certificates. Digital certificates are used as identities for machines and are provided by certificate authorities (CAs).

As the requirement for certificates grows – especially certificates that need to be trusted within the organization, enterprises have to set up their internal public key infrastructure (PKI) so that private CAs can be created internally.

Technically creating a CA and signing a certificate is very simple. If it is being done for local testing, anybody can sign the certificate without much effort. However, when the certificates provided by CA's are used in production, there is more to it. Digital certificates, which serve as virtual identities for both hardware and software entities connected to the internet, can make or break a network system.

PKI is a framework that enables the encryption of public keys and includes their affiliated crypto-mechanisms. The purpose of any PKI setup is to manage keys and certificates associated with it, thereby creating a highly secure network environment for use by applications and hardware. X.509 certificates and public keys form the cornerstone of PKI, acting as the mechanism through which cryptography can be established for an endpoint.

Ecuador's largest private bank Banco Pichincha suffered a cyberattack that disrupted operations and took the ATM and online banking portal offline

Tech giant Microsoft fixed several Windows 11 features failing to load after an expired certificate was discovered

A recent GoDaddy data breach exposed the data of 1.2 million customers

Since enterprises now manage thousands of certificates regularly in their network infrastructure, these must be monitored, tracked, and renewed on time to avoid expensive application outages. However, the maintenance required is not the only challenge posed by the growing number of certificates – security is also a significant concern.

Hackers compromised the Federal Bureau of Investigation's external email system on November 13, 2021.

The trust they represent can be misused by cybercriminals for phishing, making them a potential target for theft. This fuels the need for efficiently managing these SSL/TLS certificates and their keys. However, it extends beyond SSL/TLS certificates to include certificates that involve people, devices, and IoT systems. At the same time, considering an enterprise's certificate volumes and issuance velocity is significant.

Through strong authentication and authorization mechanisms, digital certificates help verify all devices, applications, and workloads regardless of where they are, ensuring secure machine-to-machine communication. In doing so, they help build a cybersecurity model that is multi-layered, transparent, location-independent, and, more importantly, based on zero-trust, the bedrock of digital security.

This guide is designed to provide CISOs with an insight into three of the key pieces of certificate lifecycle management. The guide also focuses on the role automation plays in an organization's cybersecurity strategy and on their path towards digital transformation.

- *Simplifying certificate ownership and approval for efficient certificate management*
- *Seamless integration of certificate management with other enterprise solutions*
- *Real-time discovery, visibility and monitoring of digital certificates*

"As the number of devices increases — and continues to grow — establishing an enterprise-wide strategy for managing machine identities, certificates and secrets will enable the organization to better secure digital transformation."

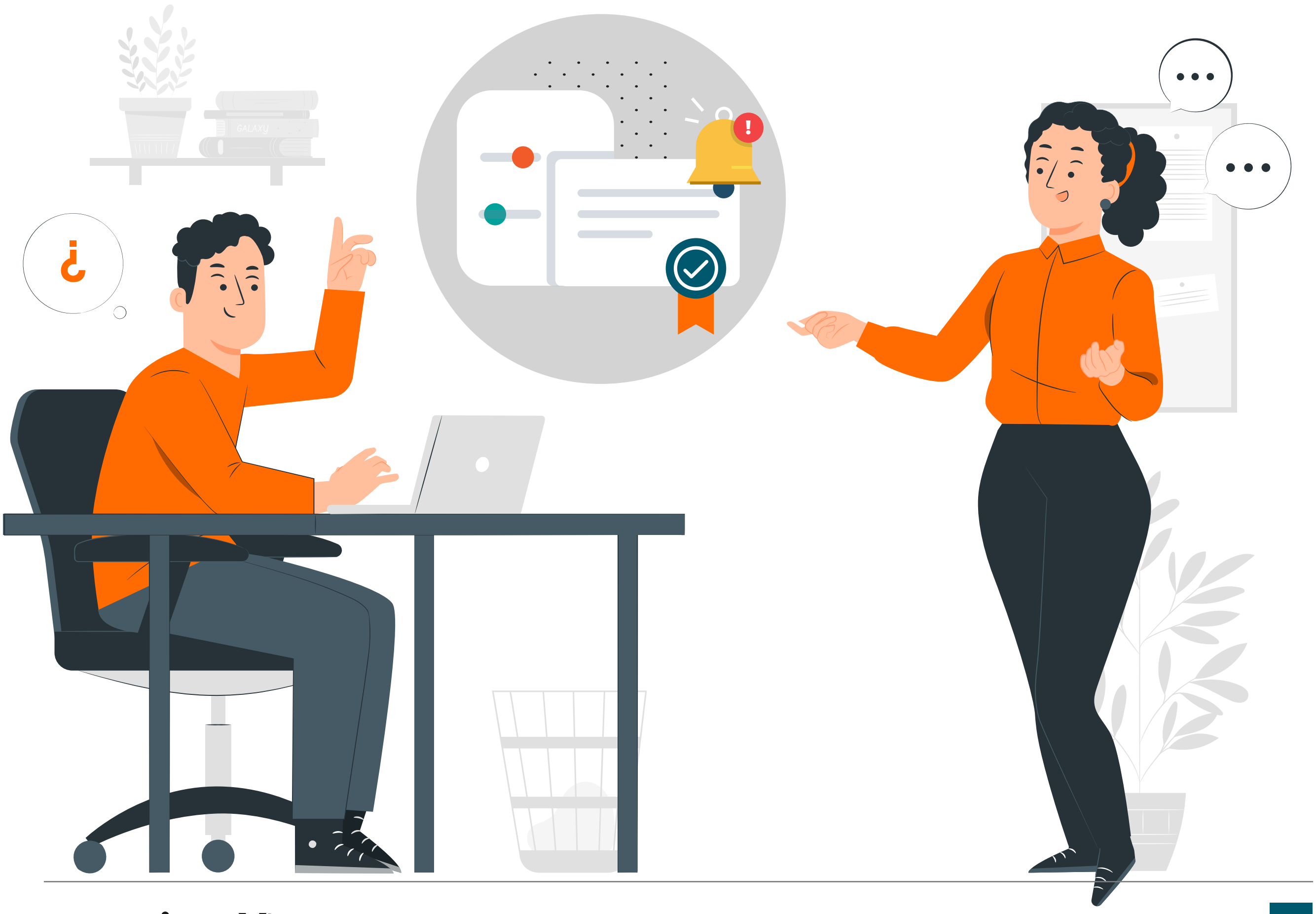
- Gartner Top Security and Risk Trends for 2021

3. Key Challenges faced by Companies with Managing Digital Certificates

Identity authentication is critical in today's digital world and identity can be much more than security alone. Hence, many organizations are looking at broader business benefits by investing in new identity sources, biometrics, and advanced analytics to ward off potential cybersecurity threats.

Some of the key challenges faced by companies include:

- **Colossal increase in data:** Large volumes of sensitive and private financial data
- **Need for seamless integration:** Integration with the existing system helps simplify complex business processes
- **Demand for enhanced security:** Twin benefits of authentication, as well as encryption, secure potentially sensitive documents from unauthorized access and identity thefts
- **Compliance:** Various government mandates and standards require organizations to ensure protection from phishing, malware, and other advanced attacks



4. Public Key Infrastructure (PKI) and Certificate Management

Gone are the days when installing necessary SSL certificates on websites and servers and renewing them once every few years would be enough. Today, PKI protects nearly every internet-facing system (and its back-end servers), software programs (in the form of code-signing certificates), and communication in general. There have been well-documented occurrences of PKI being the weak link that resulted in a data breach.

- **Cloud Applications:** With the emergence of cloud-based apps, multicloud deployment, and container-based deployment, the need to secure the hosting infrastructure and individual consumer endpoints has become paramount.
- **Internet of Things (IoT):** Not only are IoT deployments numerous in terms of individually connected endpoints, but several applications of IoT also hold sensitive data that should be protected at all by PKI, as the vanguard.
- **DevOps:** PKI and DevOps have never been compatible – DevOps exemplifies agility, while PKI has traditionally been a slow, manual exercise. However, certificates need to be rapidly deployed to protect outgoing code, applications, and communication lines in general.
- **Remote Work:** As an entirely remote workforce slowly becomes the norm, the existence of valid, constantly updated PKI on organizational systems not only makes remote access secure, it also ensures that employees' digital assets remain secure by enabling constant updates.

When a network's PKI is compromised, it instantly renders affected entities on the network invalid in the watchful eyes of the rest of the internet. They are assumed to be (and often are) unsafe to interact with and effectively boycotted until the vulnerability is resolved. This seemingly insignificant occurrence has potentially huge ramifications.

Certificate-related issues are almost synonymous with PKI infractions. A certificate that has **expired, compromised, or gone rogue** is the definition of a security lapse. It accompanies the possibility of **application downtime, outages, or even data breaches,** which could set victims back by million dollars in damages.

5. What constitutes improper certificate management?

We have compiled a checklist that will help you evaluate if your certificate management strategy has room for improvement:

	YES	NO
■ Does your certificate management practice have an audit trail?	◉	○
■ Can any individual in your organization request new certificates?	◉	○
■ Does your PKI team have role-based access control (RBAC) for certificate handling processes?	◉	○
■ Do you have documented visibility into the certificate chain across environments?	◉	○
■ Are your private keys stored on encrypted hardware security modules (HSM)s?	◉	○
■ Are your systems up-to-date on the latest cryptographic standards?	◉	○
■ Do you have an automated tool to discover, monitor, renew, and revoke certificates?	◉	○

If you answered ‘no’ to any of these questions, then you are at risk of becoming a potential victim of an outage!

Certificate outages can affect your business in a multitude of ways:

- Customer disconnect and opportunity losses
- Brand damage
- Legal fines and compliance restructuring
- Customer reconciliation
- Drop in productivity

6. **The Solution**

6.1. Simplifying certificate ownership and approval for efficient certificate management

One of the crucial aspects of certificate lifecycle management is delegating the management responsibility of certificates and keys, in other words, assigning certificate owners and approvers. The underlying intent of establishing an ownership and approval process is to ensure that only authorized personnel are allowed to make changes to the certificate infrastructure. This process eliminates the existence of undocumented or unapproved certificates with weak security standards, thereby mitigating the risk of a data breach.

Properly assigning certificate owners and escalations, designing an approval workflow, and creating a simplified certificate enrollment process are pivotal to successfully implementing a standardized certificate management system.

However, organizations employing manual processes store certificate ownership information in excel spreadsheets and databases along with other certificates and key-related information. These cursory approaches make establishing ownership and enforcing accountability for certificate actions a significant challenge. As the organization's digital footprint increases, the number of digital certificates to be managed can run into thousands. Manually tracking assigned owners and approvers for thousands of interlinked certificates via spreadsheets becomes plain unreasonable and, not to mention, highly error-prone.

Here’s how certificate ownership dilemmas can kill your security posture and affect your bottom line revenue

- In a typical enterprise public key infrastructure (PKI) setup, there are many stakeholders involved in the development, deployment, and management of a single application. Based on the different stages of the application lifecycle, multiple certificate groups are created and allowed to manage certificates independently. When multiple stakeholders are involved, poor collaboration and ambiguous ownership mapping lead to unknown or undocumented certificates being provisioned.

  When working with manual processes, tracking and monitoring these multiple groups and their actions becomes a huge challenge. The inability to regulate the access and prevent unauthorized actions inadvertently creates auditing issues, certificate expirations, outages, and security vulnerabilities.

- Digital certificates must be continuously monitored for renewals to avoid expiry and application outages. In a manual management premise, when a certificate is due for renewal, renewal requests are raised via email, and more often than not, these requests are buried among other service inquiries in an owner’s inbox. Missed requests often lead to certificate expiry and result in unnecessary outages that not only impact business revenue but leave the security door ajar for bad actors.

  In the event of a certificate owner changing position or quitting the company, certificate ownership is not updated and left to linger in ambiguity. When this orphaned certificate expires or is compromised, certificate teams struggle to ascertain the rightful owner to initiate renewals and revocations. Not having this critical piece of information delays incident response, risks data exposure and leads to unplanned application downtime.

  Another reason for worry is change in root ownership. Change in root ownership happens when one company sells off its CA division to another company, mostly due to a shift in focus. The impact is relatively less for CAs with root and intermediate certificates already available in the trust stores. But, for enterprises with pinned intermediate or root certificates, there’ll be huge service disruptions due to certificate trust. There’ll be an even higher impact for CAs that’ve spun off as a separate entity and are trying to change the root CA abruptly. Apart from just certificate expiries, enterprises using certificates from deprecated roots or intermediates can also suffer severe disruptions.

How should you respond?

- Assess the certificates within the discovered inventory. Group and prioritize them according to the organization's requirements. For example, replace weak certificates on mission-critical and public-facing applications before updating certificates on internal servers.

- Establish well-defined roles in the PKI management team with an ownership hierarchy. Each level in the hierarchy should be a part of an approval chain that allows the delegation and validation of ownership.

  Develop a management process that helps enforce role-based access control. For example, a super administrator will be able to request, enroll, and push certificates to their endpoints, while an administrator will only be able to request certificates – they would have to require the super admin’s approval before taking any further actions on it. Restricting the level of access for users and groups based on requirements helps prevent unauthorized certificate actions, bolstering the security posture.

- Enforce strict policies for use and generation of certificates and keys - such as recommended cryptographic techniques, hashing algorithms, key lengths, CAs, and workflows – consistently across the infrastructure to validate and eliminate non-compliant certificates. Mandate network-level changes to be approved by authorized personnel only.

- Simplify the process of adding new certificate owners by allowing existing owners to transfer the ownership before changing positions or moving out of the company or by assigning ownership for the entire certificate group.

- Create an audit trail system that logs every action taken by stakeholders in the hierarchy, along with a timestamp. Make sure critical events are automatically reported back to the respective certificate teams. Audit logs are immensely useful for determining the cause of certificate-related issues and for detecting policy violations.

- Set up an automated alerting and reporting mechanism that sends periodic reports and notifications on expiry, validity, and compliance status of certificates to the corresponding owners. This helps with in-time renewals and proactive resolution of certificate issues.

6.2. Seamless integration of certificate management with other enterprise solutions

In a typical IT operations premise, enterprises use various solutions for authentication, authorization, monitoring, ITSM (IT Service Management), and SIEM (Security Information and Event Management). A certificate management solution is required to integrate with these enterprise solutions to simplify and secure operations.

The true power of automation can only be realized when a certificate lifecycle management system tightly integrates with other existing enterprise solutions.

Here's how a siloed CLM can affect your IT operations efficiency

- When certificate management operates in silos, IT operations face the challenge of a grinding long-drawn process that involves manually raising certificate requests, procuring them from CAs, and pushing them to the devices using another IT solution. The disconnect stemming from the lack of integration creates serious delays in the certificate lifecycle process. Also, too many pit stops in the lifecycle increase operational complexity, thereby introducing security vulnerabilities in the IT operations systems.

- Managing certificates in distributed cloud environments starts with holistic visibility and discovery of all certificates installed across various endpoints in the network. Visibility is the cornerstone of any protection mechanism. Yet, most enterprises still have little to no visibility into their certificate infrastructure. Most of the information that ensures full visibility (such as the number of certificates in use, their locations, their expiration dates, and their ownership details) are either improperly documented or not documented at all when managed manually in spreadsheets. Even when they are documented, the high risk of human error affects the accuracy of the inventory.

Legacy tools often fail to discover certificates in distributed cloud environments, as they don't integrate with enterprise network scanners. Scanning involves discovering all the certificates that are installed across various endpoints in an organization's network. Every scan records key details of certificates like their locations, health, types, days to expiry, their positions in the chain of trust, etc. They provide insights into the security map of a network infrastructure and help detect major flaws.

- As far as control and visibility are concerned, mobile devices still pose a serious threat to enterprise security. Since mobile devices leverage digital certificates for authentication and security, it is essential to closely monitor and manage these certificates. This requires CLM platforms to integrate with mobile device managers (MDM). Lack of integration makes monitoring certificates for expiry, issuing new certificates, and updating weak certificates across mobile devices extremely challenging.

How should you respond?

- Choose a certificate lifecycle automation solution that has pre-built integrations with third-party systems. This integration allows IT operations teams to access simple automation workflows from third-party systems for self-servicing certificate requests, therefore standardizing certificate management. For example, integration with ITSM tools such as ServiceNow and BMC Remedy, allows teams to design manual ITSM tasks, such as creating a ticket, pushing a configuration, and closing a ticket, directly into an automation workflow, which drastically accelerates the entire process.

- Choose a certificate management solution that can seamlessly integrate with existing enterprise scanners in the network. This integration allows the CLM solution to penetrate deeply into the enterprise network and discover all certificates in hybrid network infrastructures, procured from multi-vendors and on an on-demand basis. The integration also eliminates the complexity of running multiple scanners for certificate discovery. Brownie points if the solution allows enterprises to customize the intensity of scans for uninterrupted discovery. The ability to discover all certificates provides enterprises a holistic view of the chain of trust and installation location.

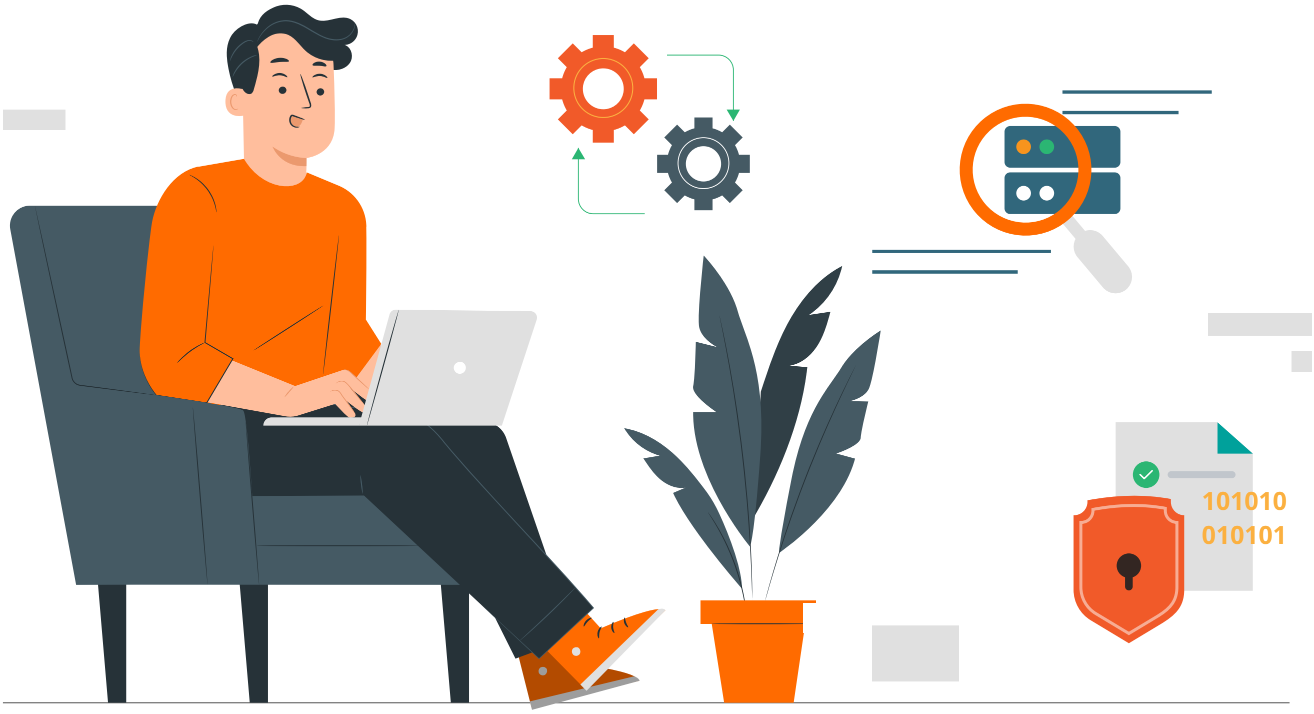
- Choose a certificate lifecycle automation solution that integrates with MDMs and enterprise mobility management (EMM) systems for simplified and secure certificate management. This helps discover certificates from each device group within the MDM, monitor them for expiry, leverage both internal and external CA for issuing new certificates, and push these certificates back to the device group efficiently.

6.3. Real-time discovery, visibility, and monitoring of certificates

From a load balancer to a cloud application to mobile devices, every entity on the network requires digital certificates. In a typical IT environment, multiple teams such as security, networking, and DevOps are involved in the development, governance, and maintenance of the network infrastructure. These teams have the flexibility of procuring and provisioning certificates independently to facilitate uninterrupted operations.

When multiple teams manage certificates, enforcing a uniform PKI policy becomes challenging. Ad-hoc processes are error-prone and non-compliant, and often lead to variations in cryptographic standards. The security risk is amplified when PKI teams rely on manual processes for discovering and monitoring certificates. Spreadsheets and legacy monitoring tools do not offer real-time, top-down visibility of certificates distributed in multi-cloud environments. This increases the probability of orphaned certificates becoming weak links.

The problem of discovery, visibility, and monitoring of certificates is more pronounced when it comes to DevOps and containerized environments. The fast-changing nature of these environments has reduced the validity of digital certificates from years to a few hours. This means certificates are now renewed and provisioned more frequently, and therefore must be closely governed to avoid security lapses. If encrypted communication is not properly orchestrated and managed—the very advantages of DevOps and containers such as agility and ease of deployment—can become the greatest vulnerabilities.



6.4. Certificate Management in DevOps and containerized environments

As organizations move towards infrastructure-as-a-code culture that is rife with rapid release cycles and continuous integration/ continuous delivery (CI/CD) practices, speed is always the top priority. This need for speed has inadvertently made it difficult for security teams to shift left and bake security right into the DevOps lifecycle. As DevOps grows increasingly multi-faceted with cloud deployments, containers, microservices, and several other open-source management tools—the risk of a cyberattack increases multifold. Mitigating this risk requires DevOps to align with cybersecurity.

One of the pivotal and time-tested security measures enforced to secure the CI/CD pipeline is digital certificates. These certificates add a much-needed layer of security for DevOps by authenticating and securing all digital communication. Implementing a well-documented, policy-based, compliant certificate infrastructure for applications used in DevOps toolchains and containerized environments is key to making the most out of speed and agility, without compromising on application security.

However, many organizations employ manual processes for certificate management. The inefficiency and complexity of these processes create a host of challenges for the DevOps teams as they try to balance rapid development timelines with secure certificate management practices.

Here's how manual certificate management can kill your DevOps agility and your security posture

- The DevOps environments today are overrun with new web servers, virtual machines, and containers that are constantly being spun up and down in a matter of hours. This has substantially increased the use of digital certificates. In a conventional development pipeline, procuring trusted certificates can take days. Ticketing systems that are required to move the request from one point to another are typically scattered, which further delays the certificate issuance process. Given the fleeting lifespans of virtual machines and containers, issuing certificates cannot be a delayed process as it breaks the application delivery speed.

  Because speed is critical, DevOps teams often tend to steer clear of speed breakers. This means taking shortcuts to certificate generation and provisioning. One of the most commonly used hacks by DevOps in this context is to procure certificates from CAs of their choice or issuing self-signed certificates, which causes inconsistencies in certificate management and puts security at high risk.

- With the number of digital certificates increasing substantially, the manual process of monitoring, allocation, expiration, and binding of thousands of certificates across the organization can become a dreaded chore for DevOps. The burgeoning volume and chaos of manual requests clouds visibility. Tracking and monitoring certificates for expiry becomes difficult and are neglected. The problem is further exacerbated by the lack of consistent communication with the CA. Together, this leads to frequent certificate expirations and DevOps outages—whose consequences are no less catastrophic for organizations.

How should you respond?

- Choose a certificate lifecycle automation solution that tightly and seamlessly integrates with your DevOps tools such as Puppet, Chef, Ansible, Terraform, and Saltstack. This way, you can rest assured that every new application or update is secured with an X.509 certificate. As DevOps requires certificates to be deployed rapidly for uninterrupted operations, an integrated CLM will allow DevOps teams to request and install certificates right from the CI/CD pipeline.

- Automate certificate lifecycle operations in the DevOps environment. This allows teams to order certificates from any supported CA, push issued certificates to associated applications, renew and revoke existing certificates, and delete unused certificates—all from their preferred DevOps tool.

- Use automated workflows to enable self-servicing for certificate generation and enrollment. These predefined workflows allow DevOps teams to procure and provision certificates without any manual intervention. An automated solution automatically provisions newly issued certificates and associates them with necessary SSL profiles on end-servers, wherever they may reside. This process accelerates certificate enrollments while also ensuring strict policy compliance.

  Adopting automation also helps DevOps gain complete and holistic visibility of the certificate infrastructure. This gives them the ability to identify the entire chain of trust, including the issuing CA and the endpoint where the certificate resides.

- Employ a CLM solution that supports container-based platforms and integrates with dedicated container management tools. Containerized applications and workloads sometimes use certificates with a lifespan of a few hours. Having an integrated CLM provides an efficient and reliable mechanism for deploying certificates and keys for applications hosted in a container infrastructure.

7. Step into the agile world of cloud with automated certificate lifecycle management

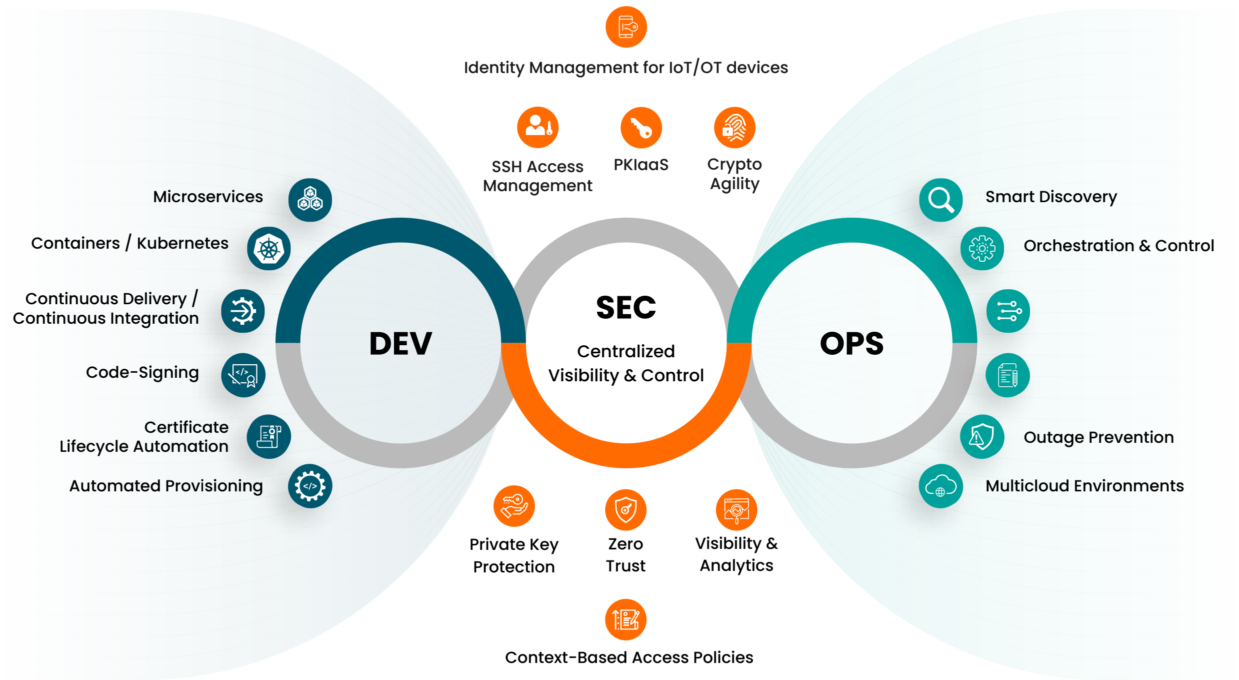
The AppViewX Next-Gen Machine Identity Automation Platform is purpose-built for orchestrating and governing digital identities – digital certificates and keys – of machines – devices, workloads, applications, containers, and the Internet of Things. The AppViewX Platform quickly and easily translates business requirements into automation workflows that improve agility, enforce compliance, eliminate errors, and reduce cost.

AppViewX CERT+ is a turnkey solution for all enterprise public key infrastructure (PKI) needs. With AppViewX CERT+, enterprises can quickly set up their internal root certifying authority (CA) as well as issuing CAs without having to upfront invest in costly hardware or complicated processes, or cumbersome PKI operations. Certificate lifecycle management (CLM) in CERT+ simplifies all certificate operations between CA and the applications where certificates are used.

> *"AppViewX CERT+ has delivered the solution we needed to greatly improve the management of our certificate lifecycle. Since implementing AppViewX, we have not had a single certificate related outage and our certificate turnaround time has been greatly reduced. "*
> *-Paul French (Assistant Director), DMAC*
> *- Middleware Operations Manager, The Australian Bureau of Statistics.*

AppViewX is revolutionizing the way NetOps and DevSecOps teams deliver certificate lifecycle management solutions to enterprise IT. The AppViewX Platform quickly and easily translates business requirements into automation workflows that improve agility, enforce compliance, eliminate errors, and reduce cost. The platform works hand in glove with AppViewX CERT+, providing a more comprehensive approach for enterprises to scale their machine identity management.

How the AppViewX Platform Revolutionizes DevSecOps Practices



7.1. Context-aware and state-aware

Automation in CERT+ is 'smart.' Before running an automation workflow, the solution first checks the device's state, performance, capacity, etc., and proceeds only after getting a green light. This way, it prevents the all-too-common problem of automation collisions - a scenario where a device gets more requests than it can handle from various other devices and tools and eventually crashes. CERT+ here acts as a master-orchestrator - it can regulate and forward requests from other tools as well, such as a vulnerability-scanning tool like Rapid7 or a configuration management tool like Ansible, through REST API integrations.

7.2. Policy-based orchestration

CERT+ automates certificate management based on policies laid down by the enterprise, the CA, and industry regulations. PKI administrators can group certificates based on their type, use-case, criticality, etc., and apply a different policy for each certificate group. Policy-based automation takes care of certificate lifecycle tasks such as time-bound certificate renewals, key rotation, access privileges, and compliance audits.

7.3. DevOps-friendly

DevOps requires certificate lifecycle management to be integrated into CI/CD pipelines so that every new application or update will be secured with an appropriate X.509 certificate. Another requirement for DevOps is speed - certificates need to be deployed almost instantaneously for testing and production. CERT+ integrates with popular DevOps tools, such as Jenkins, enabling DevOps teams to request and install certificates right from the CI/CD pipeline. CERT+ also ensures that obsolete certificates (such as internal certificates used for testing) are destroyed automatically to prevent their misuse.

7.4. Support for containers and multicloud

Containerized applications and workloads may have ephemeral certificates with a lifespan of a few hours. Many times container applications use self-signing CAs within the Kubernetes cluster for ease and speed of certificate enrollment. AppViewX provides a Kubernetes controller as an integration point between CERT+ and Kubernetes. Any application running in the Kubernetes cluster can leverage this external signer for routing certificate signing requests (CSR) to the corporate CA. Typically, the service mesh solutions like Istio are configured to use this signer as the service mesh takes care of SSL offload. CSRs flowing through AppViewX CERT+ go through the central control policies defined by PKI administrators and ensure high security standards.

The Next-Gen Machine Identity Automation Platform from AppViewX consolidates its security automation solutions for certificates, keys, IoT security and SSH access management across multicloud environments. The platform enables zero-trust, making the entire system more flexible, adaptable, efficient and agile. It is available as a service and can be deployed in the public cloud, private cloud or on-prem environments. The platform works hand in glove with AppViewX CERT+, providing a more comprehensive approach for enterprises to scale their machine identity management.

> *"AppViewX has a good concept of managing the lifecycle of PKI certificates and has gone to great lengths to ensure adaptability and integration. Automation is embedded in the tool to ensure we succeed in our goals." -* ***Lawrence Ly, Senior Platform Specialist, AXA Life Japan.***

Security simplified with AppViewX

Trusted by one out of every five Fortune 100 companies, AppViewX CERT+ powered by enterprise-grade automation helps with smart discovery, visibility into security standards, and centralized management of certificates and keys across hybrid multi-cloud environments.

Make visibility the cornerstone of your protection mechanism.

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