appviewX

The CISO's Handbook for Certificate Management

PART 1:

# CREATING A SECURE CRYPTOGRAPHIC LANDSCAPE

Three key takeaways for the establishment of an effective certificate management system.

www.appviewx.com

# Building a secure certificate infrastructure has long-term pay-offs.

CISOs need to ensure that the necessary processes to do so are firmly established within their firm's security organizations.

## Maximize Visibility

Environment-wide scanning systems to locate and inventory certificates.

## Define Trust Structures

Compartmentalized PKI functions for maintenance and management.

## Accelerate Response

Mechanisms to expedite vulnerability or threat resolution.

# Improper certificate management is associated with several potentially devastating risks – from application downtime to data breaches.

Certificate-related outages usually stem from a few persistent cases of mismanagement, like expiration or invalidity. Even the simplest of errors have large impacts – the cost of network outages caused by expiring certificates tops out at US$ 15 Million.

It's important to note that most such events can be circumvented by simply using a certificate management system, which prevents them from occurring in the first place. By streamlining and automating the certificate lifecycle, the possibility of error is almost completely eliminated, rendering businesses safe from PKI-related anomalies.

CISOs, being responsible for the cryptographic wellbeing and security of their organization, have to take a top-down approach to implementing a defined system for PKI management. A good way to start would be by:

- Identifying the manual, error-prone certificate processes
- Determining if automation is a viable alternative to those processes
- Deploying certificate management systems to automate

# The CISO's handbook is geared towards implementing decisive PKI changes. The 'Evaluate, Formalize, Resolve' framework is built for agility and rapid results.

In this handbook, we'll cover the three initial steps technology leaders can immediately take towards implementing certificate management to realize transformational changes in their operational efficiencies and cryptographic agility with respect to PKI teams.

We'll also provide pointers on how you can use a certificate management tool to simplify adherence to these guidelines. The tool we'll use as an example for each action item will be AppViewX CERT+, a full-cycle, cross-channel certificate management platform.

## Evaluate

The certificate infrastructure for flaws, efficiency bottlenecks, and blind spots.

## Formalize

Build a trust structure that maximizes PKI agility and documents processes.

## Resolve

Vulnerable cryptographic mechanisms and potential threats to your network's security.

1

# Evaluate the certificate infrastructure for weak links

Improper certificate management has significant business-wide impacts on organization, resulting in system downtime and outages. The inability of a user to access a website due to a certificate issue is the most common symptom, with the prognosis being disappointed customers and lost business.

Statistically, certificate expiry is the most common issue that businesses grapple with. Manual PKI management is a prime contributor to these problems, and does not permit administrators to deal with unknown certificates outside their purview. Furthermore, there is no mechanism for renewal, revocation, or provisioning, leaving these processes vulnerable to manual error and negligence.

## How should CISOs respond?

- Employ scanning tools to locate and inventory all certificates on the network
- Use certificate management tools to automate renewal, revocation, and provisioning processes.
- Identify all PKI attributes, cryptographic algorithms, and CA providers on discovery to minimize downtime in case of outages.

# How can AppViewX help?

AppViewX CERT+ helps teams streamline certificate operations and thereby hedge against risk in the event of an issuer compromise, critical vulnerability exposure, or suspected compromise.

- It scans networks to detect all the certificates on it, regardless of Certificate Authority or endpoint.
- It automatically inventories the discovered certificates and permits grouping by several criteria.
- Appends relevant PKI attributes to the inventory records of the certificate repository.
- Allows for automation of tasks like renewals, revocations, and pushing certificates to endpoints.

2

# Formalize the Certificate and PKI Trust Structure

Internet-facing systems are multifaceted and gestalt, consisting of several internal and external applications working together in unison. For two online entities to interact, both of them must first determine each other's established trust by ensuring that they are valid and meet encryption protocol standards, and this is done by verifying the certificates on both sides of the transaction. However, the absence of a defined PKI management strategy in most organizations results in a scattered trust chain, creating the possibility of an incomplete verification process. This increases the chances of the communication channel becoming insecure and vulnerable to breach.

In addition, the disintegrated nature of the trust chain makes it difficult for teams to deal with events such as compromised CAs, attempts to tamper with the certificates, phishing attacks, or digitally signed malware. There are several risks associated with deprecated or weak cipher mechanisms as well. It is important for security and risk leaders to understand these risks and plan for contingencies by structuring the management process and accelerating response times.

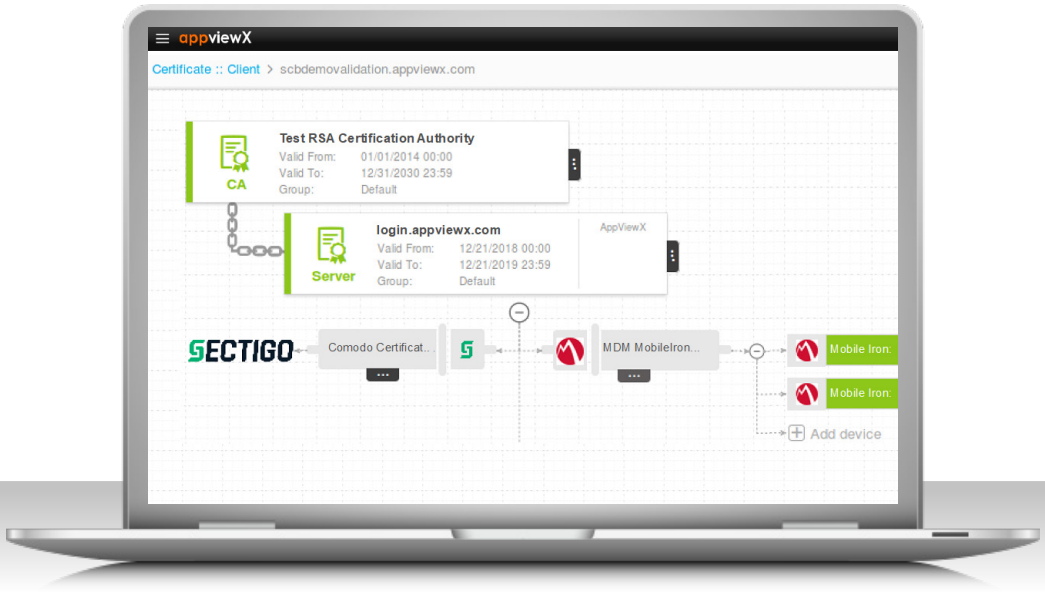
## How should CISOs respond?

- Formalize the certificate trust chain by using a management system to define stage-by-stage processes, and establish multi-level control.
- Enforce policies across the system to eliminate the possibility of operational errors (eg: avoiding wildcard instances, ensuring valid chain structures, enforcing encryption policies).
- Understand the internal processes that concern quick removal and replacement of root certificates from servers or applications.
- Ensure that strong cipher mechanisms are in place.

# How can AppViewX help?

As a full-fledged certificate management system, AppViewX CERT+ creates clearly delineated processes that helps administrators visualize the certificate trust chain and precision-engineer workflows for agility.

- Access visual representations of certificate chains that assist in validation of root and intermediate certificates.
- Single-window certificate operation capabilities (renewal, revocation, enrolment, provisioning)
- Create and enforce policy across the system for a range of criteria.
- Grant granular role-based access to allow personnel to self-service whenever necessary, minus the issue of clearance.



3

# Resolve Vulnerable Certificate Cryptographic Mechanisms

Though PKI security rely on x.509 certificates, x.509 certificates rely on the underlying cryptographic mechanisms and standards to ensure that they are capable of operating alongside the newest technology, or to enable advanced threat-deterrence capabilities. These crypto-algorithms are continuously evolving (such as the deprecation of SHA-1 and the advent of SHA-2).

Certificate Authorities update the certificates they offer to the latest algorithms, and CISOs have to stress upon a few variables where their certificate management strategies are concerned. There are a handful of critical questions CISOs should be asking their PKI teams. Are all certificates in the system updated to the latest standards? Are there any known vulnerabilities with the CA? Are the cryptographic primitives in compliance with mandated standards? Does the certificate meet enterprise policy?

## How should CISOs respond?

- Create directives for certificate operations and management to enforce crypto-agility and align with the cybersecurity incident response plan.
- Use certificate management systems to track, locate, identify, and renew or replace certificates that are faulty, corrupted, or out-of-compliance.
- Continuously update certificates to ensure that cryptography techniques, hashing algorithms, and key lengths are always at their most powerful.

## How can AppViewX help?

The aforementioned certificate operation automation and policy definition capabilities of the platform come in handy whilst ensuring the safety of cryptographic mechanisms.

- Leverage definable automation workflows to arrange for renewals, revocations, and replacement of certificates in bulk, by CA, or by business unit.
- Monitor the status of certificates on dynamic dashboards, and get alerted when a certificate expires or becomes vulnerable.
- Generate compliance reports that continuously validate the certificate and key repository based on organizational policy.

## Building a secure cryptographic landscape is a top priority for CISOs across the globe.

Get started by implementing certificate management within your organization. To learn more about how AppViewX CERT+ can help you and your team, visit our website, or sign up for a demo by clicking on the button below.

Register for Demo

### About AppViewX

AppViewX is revolutionizing the way DevSecOps and NetOps teams deliver services to enterprise IT. The AppViewX platform is a modular, low-code software application that enables the automation and orchestration of enterprise network infrastructure and certificate management using an intuitive, context-aware visual workflow. It is built to rapidly enable users to implement cryptto-agility, enforce compliance, eliminate errors, and reduce cost. AppViewX is headquartered in New York City with additional offices in the US, UK, and India. To know more, visit **www.appviewx.com** or **info@appviewx.com**