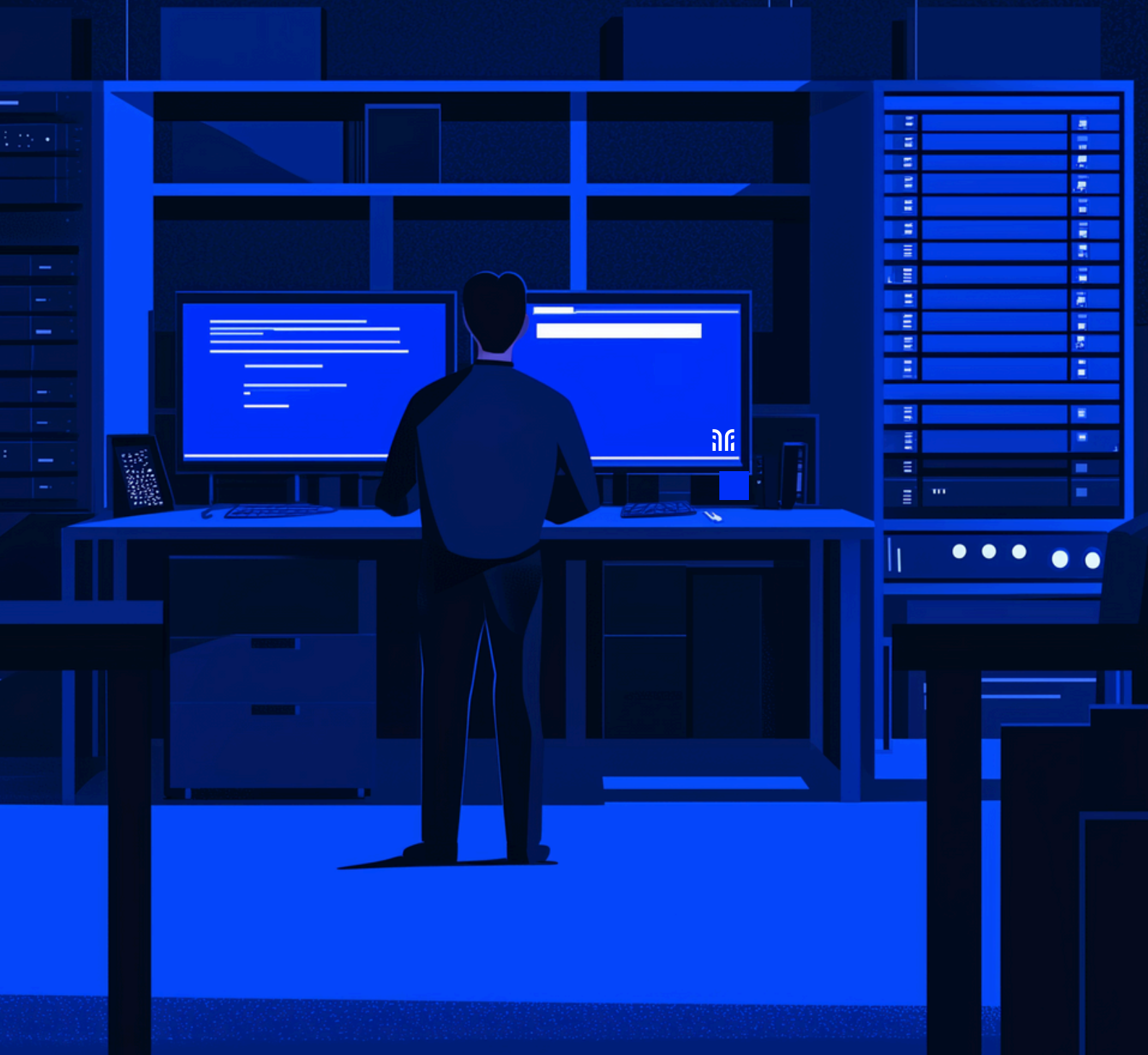
EVERTRUST

Whitepaper

Certificate Inventory Management



The Importance of Certificate Inventory Management

Understanding the importance of have a certificate
Certificates are a fundamental component of secure communications, authentication and encryption in today's technology universe.

They are essential for SSL/TLS, code signing, and user authentication and their efficient management of these certificates ensures the security of digital communications and data.

This document is intended to serve as a guide for organizations to improve their certificate management methods by addressing the challenges of tracking and maintaining these digital assets because effective certificate management is closely related to the overall security of an organization.

Since certificates are the foundation of secure communication channels, ensuring that they are properly managed - tracking their lifecycle, preventing their expiration and avoiding misconfigurations leads to preventing security breaches as unmanaged or expired certificates can lead to vulnerabilities, leaving systems exposed to potential cyberattacks. Therefore, solid management is not only a matter of operational consistency, but a central element of an overall cybersecurity strategy.

Certificates have also an impact in theses cases

Cost Optimization

Unused or duplicate certificates can generate unnecessary costs. By monitoring certificates and their usage, organizations can identify opportunities for consolidation and cost reduction.

Operational Continuity

Certificates are vital to ensure uninterrupted operation of digital services. When certificates suddenly expire, services can become inaccessible, resulting in downtime and potential financial loss. A well-managed inventory helps avoid these disruptions by ensuring continuity of operations.

Security and Compliance

Effective certificate inventory management is key to organizational integrity and compliance, as expired or forged certificates can lead to security breaches and regulatory breaches. Maintaining an adequate inventory helps prevent these risks.

A security policy for certificates is essential under the RGS Ordinance (Ordinance No. 2005-1516), which links legal constraints and trust in digital exchanges :

Legal Constraints: Mandates specific digital security requirements (electronic identification, confidentiality, signatures) to protect information systems and secure interactions.

Trust in Exchanges: Ensures the security of electronic exchanges by requiring security certification and compliance with strict security measures, promoting digital trust between authorities and users.

Best Practices for Certificate Inventory Management

Automate Discovery

Employ automated tools to detect and catalog all certificates on the organization's network, including public and private keys, allowing for real-time updates and centralized visibility.

Centralized Certificate Repository

Maintain a centralized repository for certificate storage and management. This ensures easy access and effective tracking (reporting and compliance auditing).

Certificate Lifecycle Management

Implement processes for certificate provisioning, renewal and maintenance. Automate certificate renewals to avoid certificate expiration.

Regular Auditing and Monitoring

Frequently audit certificate inventory to identify expired, false or non-compliant certificates. Implement real-time monitoring for immediate problem detection.

Role-Based Access Control

Limit access to certificate management tools and repositories to authorized personnel only.

Tools and Technologies for Certificate Inventory Management

Explore a range of tools and technologies designed to optimize CIM:

1. Certificate Management Platforms:
Comprehensive solutions for certificate lifecycle management, automation, and reporting.

2. Certificate detection tools:
Automated tools that locate certificates throughout the network.

3. PKI (Public Key Infrastructure):
System Infrastructure for managing digital certificates, keys, and authentication.

4. Monitoring and Alerting Systems:
Real-time monitoring solutions to promptly detect and respond to certificate-related issues.

The mains actors in Certificate Inventory

The CISO (Chief Information Security Officer)

Who they are?

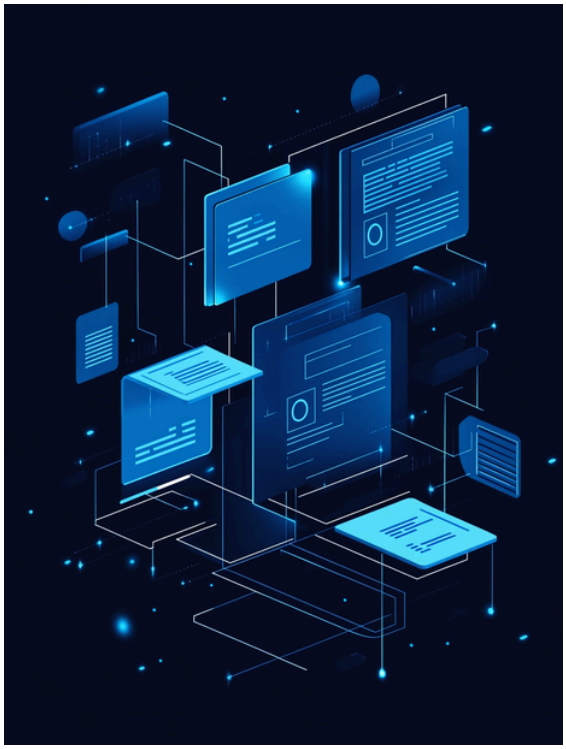
- Highly skilled senior executives responsible for protecting an organization's information technology and assets. They require both business and technical skills in addition to financial and project management training.

Why are they important?

- The CISO is critically important in safeguarding information assets and ensuring regulatory compliance in the current business environment. The importance of this role evolved it to the status of a senior executive, often reporting directly to the board of directors.

What are their main responsibilities?

- The CISO's role involves tasks are developing cybersecurity strategies, responding to incidents, managing security technologies, ensuring regulatory compliance and protecting proprietary and customer data.

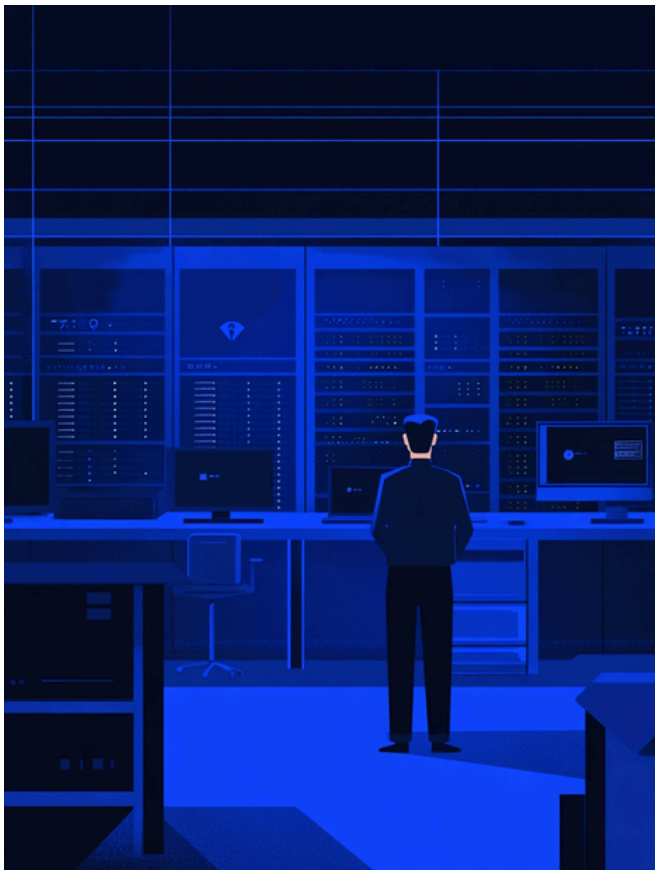


The mains actors in Certificate Inventory

The CISSP (Certified Information Systems Security Professional)

What is a CISSP?

- Worldwide recognized information security certification provided by the International Information Systems Security Certification Consortium (ISC2).



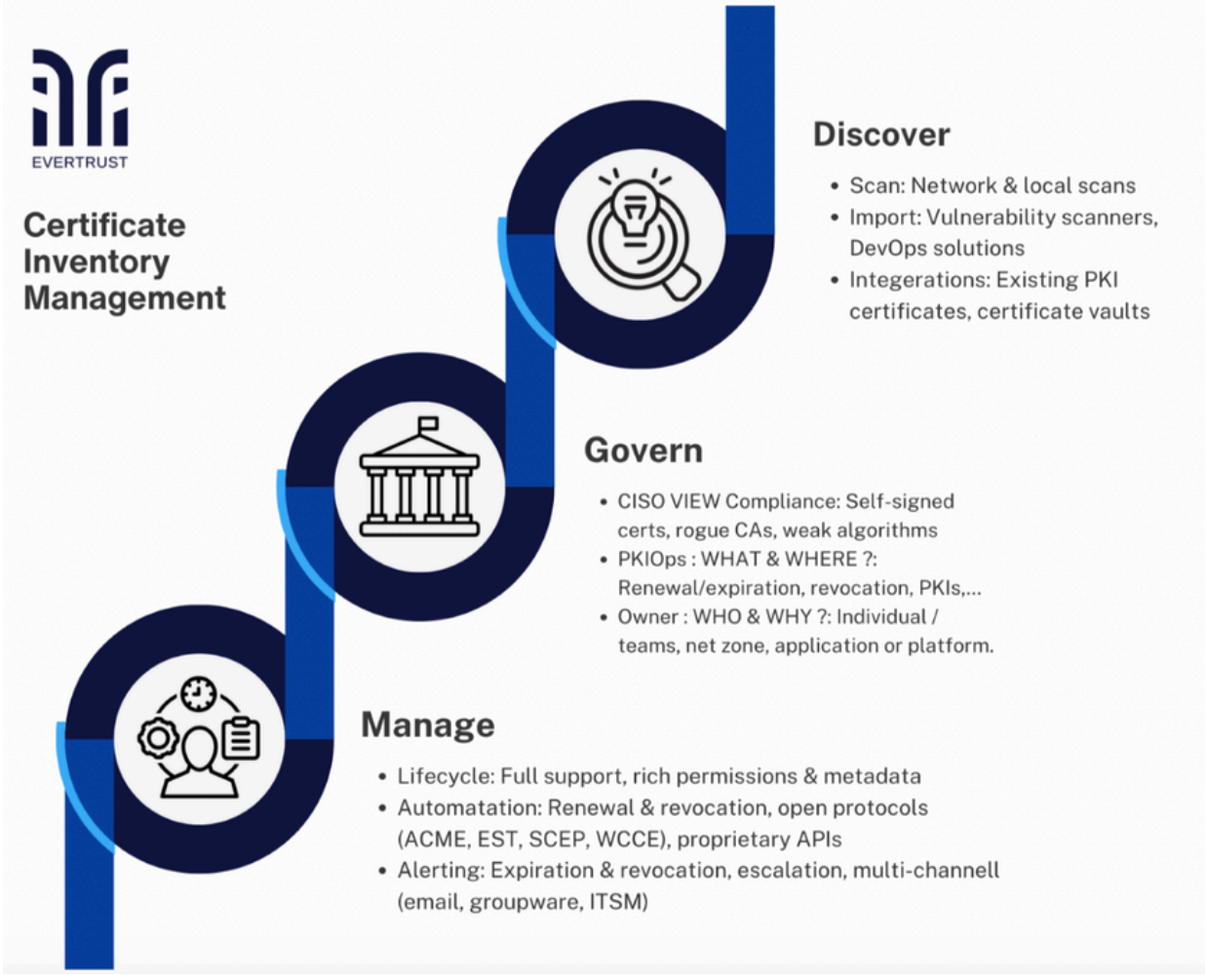
What are the requirements for this position?

- You must fulfill the CISSP Code of Ethics and background check, have passed the CISSP exam (a highly valued certification equivalent to advanced academic degrees) and have the qualifications endorsed by another certified professional.
- Typically, their knowledge and skills cover topics such as: Identity and Access Management (IAM), Security operations and risk management, asset, communications or network security and in software development as well as security testing evaluation. They also hold certifications like: CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP.

You can't manage
What you can't see

As is well known, the manual techniques currently used by most organizations are not suited to the large number of certificates they contain, and these certificates exceed their scalability limits.

Take control of your organization's certificates by proactively establishing a CLM practice that can help you inventory them and maintain actionable data about them. Don't let a certificate whose expiration date has slipped through the cracks cause business disruption.



Steps to manage and inventory certificates

The importance of a Certificate Lifecycle Management

CLM is a certificate discovery, inventory and storage process that enables centralized management of the certificate lifecycle. It provides centralized control in a decentralized environment and implements management workflows, automation, ownership tracking and delegated administration.

Giving you visibility of your certificates by **inventorying** them, maintaining **up-to-date information** about them and implementing **expiration alerts.**

Records **ownership information**, details about the **entities using the certificates**, their **locations** and, of course, **expiration dates.**

Ensure **continuous operation** in **high-volume certificate** use cases by implementing **automated certificate lifecycle management.**

Comprehensive capabilities such as **network and local scans,** vulnerable **point scanner imports** and **integration** with **existing PKI certificates** and establishing a **CLM practice**

Ensures **compliance**, PKI operations **efficiency and proper ownership tracking,** while **automating lifecycle management** and **alerting processes** to **avoid** potential **business disruptions**.

Certificate inventory management is a critical component of an organization's cybersecurity strategy. Neglecting it can lead to security breaches, operational disruptions and financial losses. By adopting best practices and leveraging available technology tools, organizations can strengthen their security posture, ensure uninterrupted operations and optimize costs in an increasingly critical digital environment.

EVERTRUST

Whitepaper

Certificate Inventory Management