Link to outline

How to Pick the Right Certificate Manager for Your Organization's Growth

Public key infrastructure (PKI) and certificate management underpin enterprise security. They're responsible for secure communications, authenticating users and devices and maintaining the integrity of digital transactions.

Selecting the right certificate manager lays the foundation for your organization's growth and scalability.

However, not all certificate managers are created equal. The chosen certificate manager should align with the organization's specific needs, infrastructure and security requirements. Hence, your choice directly affects your organization's ability to manage certificates effectively, mitigate risks and streamline operations.

This article will guide you through key considerations for choosing a certificate manager. It also identifies what features to look for, such as:

- Comprehensive visibility
- Lifecycle automation
- Ecosystem integration
- Policy governance

In each section, we've included a list of relevant questions to ask vendors during the evaluation process.

Visibility and deployment

Effective certificate management begins with visibility: you can't manage what you can't see. While you may be aware of many certificates, certificates issued outside standard processes tend to remain unnoticed.

Finding these rogue certificates is particularly challenging. Generally, they're dispersed across platforms such as servers, load balancers, firewalls, containers and multi-cloud environments. This wide distribution complicates the tracking and management process, making it necessary to employ robust discovery tools.

According to our PKI & Digital Trust Report, organizations typically use an average of seven different certificate authorities (CAs) across their operations. This underscores the need for a single comprehensive discovery tool that can locate all certificates, regardless of where they reside or where they were issued from.

To address this, opt for a tool that offers continuous discovery, capable of identifying all existing certificates regardless of their location or issuance origin. The ideal certificate manager should provide various discovery mechanisms and manage these certificates centrally through a universal hub.

When evaluating potential solutions, consider the following questions:

- Can the vendor discover and manage every certificate, including those *not* issued through its platform?
- Does the solution require significant changes to firewall rules and port configurations when deployed in environments with multiple network segments or cloud services?
- Does the solution inventory and manage the root of trust certificates on network endpoints?

Monitoring and reporting

Once you've established a complete inventory of your certificates, the next step is to actively monitor them for expiration, compliance and usage. Monitoring ensures you address potential issues before they lead to disruptions or vulnerabilities.

Access to a dashboard and basic reporting capabilities is just the beginning. **To effectively manage your certificates, you need a certificate manager with a highly customizable interface.** The added flexibility allows you to prioritize certificates based on business importance or applications and take swift action when needed.

Grouping certificates and tagging them with business or application-relevant data expands management capabilities. Choosing a tool that supports configurable metadata gives you more efficient certificate organization and tracking.

The following features make sure your certificate management process is both comprehensive and adaptable to evolving needs:

- Does the solution offer customizable and clickable dashboards that give the insights you need?
- Are there any limitations on the format or number of metadata fields you can use?
- Can you revoke issued certificates directly from the console?

Lifecycle Automation

On average, organizations manage an astonishing 81,139 internally trusted certificates, according to the PKI & Digital Trust Report. With this many certificates, handling the entire lifecycle of each one—from issuance to revocation—becomes overwhelming. This leads to missed expirations and subsequent outages.

To mitigate these risks, a certificate manager should offer lifecycle automation. **Automated renewal and provisioning directly to end-devices eliminates expired certificates, preventing costly downtimes.**

A simplified enrollment process encourages widespread adoption of digital certificates across your organization. Check if the vendor provides an extensible workflow engine capable of handling thousands of certificate requests and integrating seamlessly with existing IT service management (ITSM) workflows.

Additionally, the tool should offer crypto-agility at scale, allowing you to integrate with multiple vendors or smoothly transition from one CA to another. This capability is important as cryptographic standards evolve, particularly in response to the challenges posed by post-quantum computing.

When evaluating lifecycle automation solutions, consider the following questions:

- Can the solution manage certificates that are already in place or deployed through other processes?
- In the event of a CA compromise or algorithm deprecation, how quickly can the solution re-issue certificates (potentially tens or hundreds of thousands) from a new CA?
- Does the solution integrate with ITSM systems for request workflows and incident reporting?

Ecosystem integration

Your certificate manager will need to integrate with a variety of systems, so you'll want to understand *how* it administers these integrations.

Any certificate management tool should support basic protocols such as ACME, SCEP, Windows auto-enrollment and others. These protocols are fundamental for providing smooth and secure certificate operations across different environments.

However, certain use cases require special attention. For instance, if you have a DevOps function, it's important to check if the vendor supports API-driven integrations that work seamlessly within your existing workflows and toolsets, such as code signing.

IoT and mobile device management systems present their own complexities and require a vendor that can handle the scale and intricacies of these ecosystems. Similarly, if you are utilizing cloud Infrastructure as a Service (IaaS), be sure that your certificate manager handles the typical certificate lifecycle functions directly within cloud workloads and integrates with cloud key vaults.
By addressing the following questions, you'll ensure the chosen certificate manager integrates well into your existing ecosystem:

- Does the vendor sup
- port the industry-standard protocols your applications will need?

- Can the solution integrate with your target systems, such as network equipment, web servers, key vaults, mobile devices, cloud, and containerized platforms?
- Does the vendor provide a framework to build custom connectors when needed?

Policy and governance

Keys and certificates must be protected to prevent unauthorized access. **If a single user issues a rogue or non-compliant certificate, it can expose your organization to significant risk.**

To avoid unauthorized use, implement access controls and policy guardrails within the certificate management system. The certificate manager should include an intelligent policy engine that enforces certificate policies so that only compliant certificates are issued. This maintains the integrity and security of your certificate infrastructure.

Moreover, having clear audit logs allows for tracking certificates and user-related activities. The certificate manager should provide a comprehensive audit trail, enabling you to monitor and review actions taken within the system. This transparency ensures accountability and regulatory compliance.

To be sure the chosen certificate management system is equipped to enforce policies and provide the necessary governance, consider the following questions:

- Does the solution allow you to configure private key storage and retention policies?
- Does the solution require private keys to be stored within the system, or can they be generated remotely on the device?
- Does the solution integrate with popular privileged access management (PAM) and hardware security module (HSM) providers?

Conclusion

Asking questions and focusing on key features narrows down your options by disqualifying certificate management systems that don't fit your needs.

Whatever solution you choose, be sure it offers comprehensive visibility, lifecycle automation, ecosystem integration and robust policy governance.

For additional guidance, including a list of potential pitfalls to avoid and more expert insights, check out our certificate lifecycle automation buyer's guide. This buyer's guide will help you find and choose the right certificate manager for your processes and growth.