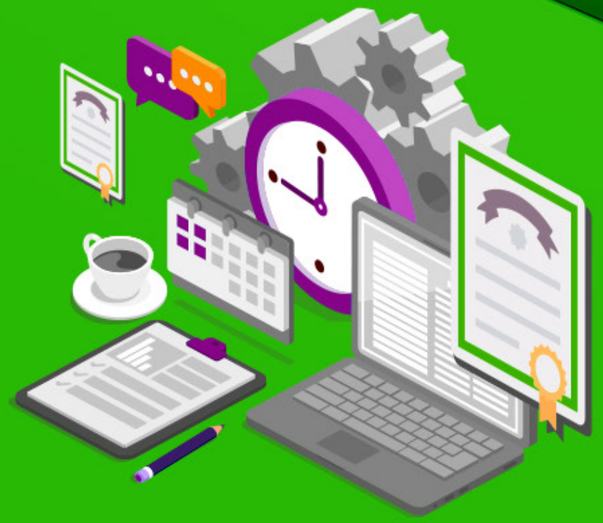
BUYER'S GUIDE

Certificate Lifecycle Automation

Practical advice for choosing your first (or next) solution

KEYFACTOR



Chances are you're in the market for a certificate lifecycle automation solution because the task of managing hundreds or thousands of certificates manually just isn't viable.

Maybe you've failed an audit or experienced one too many outages. Or maybe your existing solution just cannot scale with the needs of your business. In any case, you're in the right place.

What's inside

This buyer's guide is designed to help you choose the right certificate management solution for your organization. It identifies core capabilities needed to effectively manage certificates in large-scale, complex and multi-vendor environments. It also contains important questions to ask vendors and key insights from PKI experts.

Table of contents

Introduction

Today's enterprises face serious challenges with certificates.

Enterprises create more connections every day. The shift to containers, multi-cloud, mobile and IoT platforms has introduced significant new challenges for PKI and security teams, as increased network exposure has led to a Critical Trust Gap.

Keeping pace with the rapid rise in connectivity means using more keys and digital certificates to secure those connections. With the number of certificates growing exponentially, increasing numbers of devices, and shorter expiration periods, organizations need to rely on automation.

MANUAL SPREADSHEETS

Spreadsheet-based tracking only works for a limited certificate count. Manually keeping track of thousands of certificates just isn't feasible. It also doesn't account for unknown certificates, leaving organizations exposed to high risk of outages.

BASIC CA SOLUTIONS

CA-provided tools are a step up from spreadsheets, but these solutions aren't effective in complex, multi-vendor environments. Lack of automation and limited cross-platform support make these tools unfit for most enterprises.

OPEN-SOURCE TOOLS

Open-source CA tools and protocols are free and flexible, but they do not provide centralized visibility and control across all CAs and certificates that enterprises need to sufficiently prevent outages and ensure compliance.

THE SOLUTION: CERTIFICATE LIFECYCLE AUTOMATION

Certificate lifecycle automation - also known as X.509 certificate management - enables enterprises to proactively discover, manage, and automate the lifecycle of keys and digital certificate across their environment. There are many tools and approaches, but some are more effective than others to meet your specific needs.

Finding a solution that is easy to deploy, easy to manage, and can cost effectively protect your business is critical. To help you find the right fit, we've put together this practical buyer's guide.

"X.509 certificate management tools arm organizations with critical insight, automation and management capabilities when dealing with digital certificates."

Gartner

"Technology Insights for X.509 Certificate Management"

David Mahdi, David Collinson, October 2019

Where to Start

There are many tools on the market today, but some are more effective than others for the scale and complexity of your environment. The real difference between vendors is less about their offered capabilities and more about how they implement them.

That's why it is critical that your teams drill into use cases – and how they are implemented – before deciding on a solution. Start with these three guiding principles:

EVERY CERTIFICATE MATTERS

There are no second-class certificates. The vendor you select shouldn't force you to pick and choose which certificates to manage due to cost or complexity. A well-architected solution should make it easy and affordable to manage *every* certificate across your environment without exception. Why? Because It's not the certificates you know about that will cause your next outage – it's the ones you don't – and incomplete inventory or oversight will leave you exposed to risk.

FROM ANYWHERE, TO ANYWHERE

Multi-cloud is the new norm – as is the adoption of mobile and IoT devices. Any solution must be able to support the distributed, dynamic nature of infrastructure today. Choose a vendor that allows users to issue certificates from anywhere, to anywhere, while giving you complete visibility and control. That means any certificate (public or private), any CA, and any device or platform. It also means being able to deploy how and where you need to – whether on-prem, in the cloud, or hybrid and containerized environments.

ORCHESTRATION, NOT MIDDLEWARE

The architecture of a platform has significant impacts on ease of use and deployment. Avoid "middleware" solutions that sit between CAs and end-devices. These solutions require you to issue all certificates through their platform to fully manage them. Instead, look for modular, loosely coupled solutions that act as a certificate orchestrator, not a transaction pipeline or bottleneck.

WHY MANAGE EVERY CERTIFICATE?

Most vendors and organizations hyper focus on SSL certificates used for Internet-facing or internal applications, but this is a shrinking fraction of the certificate landscape. Cloud services, containers, services meshes all use machine-to-machine communications that rely on client authentication certificates. A large number of outages – such as the recent Microsoft Teams outage – are not caused by expired SSL server certificates, but by a failure to track web service client authentication certificates.

Core Capabilities

Now we'll look at the core capabilities of certificate lifecycle automation solutions in more detail. Within each area, you'll find a list of questions for vendors to help you drill down into how they implement the capabilities and why that's important.

“By 2022, organizations that leverage X.509 certificate management tools will suffer 90% fewer certificate-related issues and will spend half the time managing these issues, compared with organizations that use spreadsheet-based management methods.”

Gartner

“Technology Insights for X.509 Certificate Management”

David Mahdi, David Collinson, October 2019

Continuous discovery & inventory

Discovery is the foundation of every certificate management solution. After all, you can't manage what you can't see. But certificates don't live in just one place; they're distributed across web servers, load balancers, firewalls, containers and multi-cloud.

Most vendors rely primarily on the network for discovery, but this doesn't provide a complete picture. A solution should offer multiple mechanisms to discover certificates, regardless of where they reside or where they were issued from.

WHAT TO LOOK FOR

CA Synchronization

Real-time synchronization with any CA for complete visibility of all certificates issued.

Certificate discovery starts at the source. The solution you choose should continuously synchronize inventory from both internal and public CAs. This ensures that every certificate is identified, regardless of how it was issued. Without real-time visibility into CA issuance, you're left exposed to rogue certificates not issued through standard processes or left undetected in network scans.

Network-Based Discovery

Distributed SSL/TLS certificate discovery across IP ranges and subnets.

Next, you'll need to discover where certificates live. Most vendors offer built-in SSL/TLS discovery, but the real difference is in implementation. Scanning across networks from one location is highly disruptive and often non-compliant. Look for solutions that offer flexible tools that can be deployed to different network segments or cloud environments.

Low-Level Discovery

Direct inventory of key and certificate stores (and roots of trust) on network endpoints.

If a certificate isn't bound to an IP or port, it won't show up in network discovery. More integrated solutions use agent-based or agentless methods to inventory key and certificate stores. Roots of trust inventory is critical as well, because it allows you to find or remove rogue root certificates, or add a new root of trust.

ASK VENDORS

- Is the vendor able to discover and manage every certificate, even 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 root of trust certificates on network endpoints?
- Can the solution discover and inventory certificates issued via EMM/MDM and IaaS platforms?

"Ensure that the discovery mechanisms are sufficient for the organization. Network-based discovery tools should be considered boilerplate functionality."

Gartner

"Solution Comparison for PKI"

Erik Wahlstrom, Paul Rabinovich, April 2019

Real-time monitoring & reporting

Discovery and monitoring work together to give you actionable intelligence over your certificate landscape. Once you've pulled in a complete inventory, you'll need to effectively organize and monitor certificates for availability and compliance.

The solution you choose should help you simplify certificate inventory, identify vulnerabilities or pending expirations, and take action to remediate risks quickly.

ASK VENDORS

- Does the solution offer customizable and clickable dashboards?
- Does the vendor have limitations on the format or number of metadata you can use?
- Does the solution allow you to revoke issued certificates directly from the console?
- Does the solution allow you to export audit logs or integrate with security information and event management (SIEM) providers?

WHAT TO LOOK FOR

Intuitive Dashboards

An intuitive dashboard provides an at-a-glance review and drill-down functionality to take action quickly.

Dashboards should be configurable to prioritize what matters most to specific users. Users should also be able to drill down to specific certificates or groups from the dashboard to view more details or take action on any identified vulnerabilities.

Automated Alerting & Notification

Automated alerts are triggered when certificates are near expiration or out of compliance.

Most vendors offer a basic form of functionality for reporting and alerting. Look for a solution that allows you to set up notifications and escalation paths that meet your specific needs. It should also enable you to leverage pre-defined templates and fields to simplify email notifications to certificate owners.

Configurable Groups & Metadata

Allows admins to group certificates and tag them with meaningful data to manage them effectively.

Not every certificate found in discovery needs to be managed individually. The solution should allow you to group certificates and tag them with custom attributes, such as contact or billing information. Ask the vendor if there are any limits to the format or number of metadata fields that you can use.

Reporting & Search Engine

Allows users to customize and run scheduled reports, as well as search and revoke certificates quickly.

Organizations face increasing scrutiny around the use and management of keys and certificates. To keep pace with audit requirements, look for solutions that offer pre-built and customizable reports and the ability to quickly search and revoke certificates directly from the console – regardless of where they live.

Lifecycle management

As certificate counts rise from hundreds to thousands, it's become much harder to manage them effectively. This is only compounded by changing industry standards and shrinking certificate validity.

Automation is the answer. An effective solution will enable your team to automate certificates across large, complex, and multi-vendor environments - all without getting in the way of existing business processes.

ASK VENDORS

- Can the solution manage certificates 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 IT service management (ITSM) systems for request workflows and incident reporting?

WHAT TO LOOK FOR

Multi-Platform Self-Service

Self-service interfaces for users to request security-approved certificates from any device or platform.

A single web-based enrollment portal isn't flexible enough for today's users. A solution should provide multiple self-service interfaces to allow users to enroll for certificates directly from their mobile device, computer, or web-based portal.

Extensible Workflow Engine

Workflows to define certificate owners and approval structure for issuance and renewal.

Properly assigning certificate owners, designing approval workflows, and creating a simple enrollment process is critical to successful adoption. The solution should offer a built-in workflow engine capable of handling thousands of certificate requests, or integrate with existing ITSM workflows.

End-to-End Automation

Automated renewal and provisioning of certificates directly to end-devices.

Automation allows you to minimize human intervention and reduce the risk of outages. Make sure the solution can automate the entire lifecycle. It should be able to submit a CSR, retrieve the issued certificate, push it to target devices, and bind it automatically.

Crypto-Agility (at Scale)

Flexibility to issue (or renew) thousands of certificates from any CA.

Don't get locked into a single CA provider. Look for a CA-agnostic solution that gives the agility to rotate, replace and revoke all impacted keys and certificates or renew them from a new CA. Don't take a vendor's word for it; ask them to prove incident response at scale.

“Establish consistent PKI management processes and leverage certificate management tools to manage and monitor certificates. Match up out-of-the-box discovery and automated certificate life cycle management functionality of the platforms to your specific needs."

Gartner

“Solution Comparison for PKI”

Erik Wahlstrom, Paul Rabinovich, April 2019

Ecosystem integration

Industry analysts' guidance for certificate lifecycle solutions focuses first on visibility and compliance, then on ease of management and integrations.

When looking at integrations and APIs, think about how they will fit your specific use case. It's one thing to offer "out-of-the-box" integrations, but it's quite another to make them work in your environment.

ASK VENDORS

- Does the vendor support 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?
- Does the vendor offer a solution to secure code signing keys across dispersed development teams?

WHAT TO LOOK FOR

DevOps Integrations

API-driven integrations with container orchestration frameworks, key vaults, and CI/CD tools.

Fast-moving DevOps teams use keys and certificates, often outside enterprise security requirements. The solution should provide flexible API-driven integrations that fit within existing workflows and toolsets – including code signing – to provide the security team with visibility and control while minimizing disruption to developers.

Protocol Support

Support for industry-standard protocols to automate certificate provisioning and enrollment.

Make sure the solution supports the protocols your applications will need, such as Windows auto-enrollment, ACME, SCEP and others. These protocols extend visibility and control of certificates across hundreds of open-source clients and existing infrastructure.

IoT & Mobile Integrations

Integrations with mobile and IoT devices and connected device management systems.

Identity and authentication are critical for IoT and mobile devices. Look for vendors that can handle the complexity and scale of these ecosystems. The solution should integrate with devices and connected platforms via SDKs, APIs, agents, and KMIP support.

Multi-Cloud Support

Discovery and management of keys and certificates issued from cloud IaaS providers.

Extensibility into multi-cloud operations is necessary to ensure that all certificates are compliant and up to date. The solution should be able to issue, renew, revoke and push certificates to cloud workloads, as well as integrate directly with cloud key vaults and certificate management tools.

Policy & governance

Keys and certificates are critical infrastructure that must be protected, but security teams struggle to prevent users from issuing rogue or non-compliant certificates and protect private keys from compromise.

An important element in certificate lifecycle automation is to implement policy guardrails, access controls, and extensive auditability of every event.

ASK VENDORS

- 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?
- How does the solution allow you to define role-based access permissions?
- Can you get a complete audit trail of all configuration changes, user activities, and certificate lifecycle events?

WHAT TO LOOK FOR

Granular Role-Based Access

Assign certificate owners and platform permissions via users and groups from your identity provider.

Any tool that you choose must provide your team with role-based access to certificates and limit the operations they can perform within the platform. Look for solutions that use a least-privileged access model with granular permissions for roles and individual users.

Flexible Private Key Generation

Provides flexibility to generate and store keys on end-devices, within the platform, or with an HSM.

Private keys are a gateway to critical data and connections. On-device key generation should be used whenever possible to reduce the risk associated with keeping multiple keys within the platform. If keys are stored in the platform, they must be encrypted and protected by an HSM.

Intelligent Policy Engine

Enforces certificate policies and provides an audit trail of all certificate and user-related activities.

Despite tight controls, there are still possibilities where unauthorized actions can break compliance. A solution must be able to enforce certificate issuance policies and audit every user action, configuration change, and certificate lifecycle event to prevent or detect and remediate issues.

PAM Integration

Retrieves device credentials from password vaults for authentication to network devices.

To perform sensitive renewal, replacement and re-key operations, certificate automation solutions need privileged access to network devices. If you're using a password or secrets vault, you'll need a solution that can retrieve credentials automatically from the vault.

"Look for flexible key generation (server and device-side generation), plug-in integrations and support for building your own connectors when needed."

Gartner

"Solution Comparison for PKI"

Erik Wahlstrom, Paul Rabinovich, April 2019

What to avoid

Far too many companies purchase a certificate lifecycle automation solution, only to find out that the proof of concept doesn't translate to a production-ready deployment. Here are some practical tips and considerations from our PKI experts to help you avoid selecting a solution that isn't the right fit for your organization.

1

Tip #1: Don't Get Locked In

Tools provided by your current SSL/TLS provider are a helpful starting point, but enterprises with large and complex certificate landscapes require more flexibility. Don't get locked into CA-provided solutions that issue and manage certificates from only their CAs. The CA and certificate landscape changes fast, and you'll need the flexibility to adapt and expand as your enterprise evolves.

2

Tip #2: Don't Rely on Let's Encrypt Alone

Don't rely on Let's Encrypt to solve all of your PKI requirements. Let's Encrypt makes sense in some scenarios, but every certificate issued still needs to be centrally managed to gain visibility and ensure compliance with enterprise security policies. Make sure that you have an automated and enforceable management framework across all CAs.

3

Tip #3: Avoid "Low-Code" Frustration

Low-code solutions are intended to minimize complexity and custom-coding requirements. The notion of less code, less work is a promising offer, but sometimes the tools built to save time create frustrations down the line. PKI often involves unexpected curveballs and configurations that don't mesh well with a cookie-cutter approach. A solution should be customizable, flexible and scalable to meet your needs today and into the future.

4

Tip #4: Beware of "Middleware"

Avoid middleware architectures that sit between CAs and end-devices. These vendors can only manage certificates issued by their platform, meaning you can't manage certificates already in your environment. Deploying the solution will require you to re-issue every certificate and re-engineer existing workflows through their solution, which is not only highly disruptive, it's also fraught with risk.

Consider PKI as-a-Service

It's rare that an organization has unlimited security resources, time, and budget. For nearly everyone else, constraints are a constant reality – especially when it comes to public key infrastructure (PKI).

There is much more to PKI than just managing digital certificates; there's the backend hardware, software, licensing, revocation infrastructure, policies and procedures, security controls, and of course, the maintenance frustration.

Those with the right skills and expertise to run a PKI are hard to find, and even harder to keep. If your organization lacks the resources or expertise to run PKI effectively and support all of your use cases, consider a managed PKI as-a-Service (PKIaaS) solution.

ASK YOURSELF

- Does the organization have sufficient skills and depth in personnel to maintain PKI?
- Is running PKI in-house worth the ongoing costs and maintenance requirements?
- How much does it cost the organization to deploy and run PKI in-house?

BEST PRACTICE:

Choose a Platform That Does it All

Make things easier for yourself and choose a solution that combines PKIaaS and certificate lifecycle automation into a single cloud-based platform. In addition to managing certificates, this will allow you to:

- Reduce hardware and software costs
- Spend less time on backend maintenance tasks
- Improve availability, scalability and security
- Get a privately-rooted, cloud-hosted PKI

WHAT DOES PKI SUCCESS LOOK LIKE?

Watch our webcast on "Why PKI in the Cloud: Fastest Way to Mitigate Risk and Lower Costs."

WATCH NOW

38% of organizations say they don't have sufficient IT and security staff dedicated to their PKI.

Keyfactor-Ponemon Institute

The Impact of Unsecured Digital Identities, 2020 Report

Finding the Right Fit

Finding the right vendor to work with is just as important as the functionality of the product itself. Knowing that you have the right platform, people, and deployment model to support your specific business needs will ensure successful adoption.

Deployment Flexibility

The ability to quickly deploy and scale an implementation that is aligned with your current technology stack is critical. The greatest flexibility comes from solutions that can easily be deployed on premise, in the cloud, delivered as-a-service, or with a hosted PKI.

Platform Architecture

PKI is inherently complex. A modern, holistic approach to PKI and certificate management must be simple, modular and distributable. The vendor should allow you to deploy components throughout your network segments and cloud infrastructure without significant configuration requirements..

Responsive Support

This one might sound obvious, but knowing you have access to PKI expertise is invaluable. Look for a vendor that can ramp up your team quickly, align resources, and set milestones for success. Inquire about 24x7 support, initial response times, customer satisfaction and retention scores, and references.

Depth in Expertise

PKI isn't just about technology, it's about finding the level of expertise to complete your project on time and in the right way. Look for vendors that don't just develop software, but also have hands-on experience in deploying and running PKI in line with best practices, they should also have hands-on experience with PKI.

Scalable Licensing

When evaluating vendors, be sure that the licensing model is flexible and scalable. Some vendors charge per-certificate, or per certificate instance, rather than in bundles or packages that align with your certificate count. Licensing options should help you affordably manage every certificate today and as your business needs grow with a predictable cost structure.

Product Innovation

Rapid time-to-value is important. However, equally important is how the product will adapt and support emerging industry trends, such as IoT and quantum computing. Ask the vendor about their vision and mission for the product. Inquire about future product releases that will benefit you and your business.

5 Questions to Answer Before Evaluating Certificate Lifecycle Automation Solutions.

Once you've defined your solution requirements, it's time to prepare to evaluate potential products.
There are 5 questions you should be able to answer before you start.

1. What is the timeframe for the evaluation? What is the urgency for product selection based on evaluation?
2. What are the specific use cases or business requirements – both existing and future – that the solution must address?
3. How much can your organization invest in properly evaluating solutions against these requirements?
4. What are the criteria required for different users groups within the organization (e.g., PKI admins, developers, security analysts, network admins, endpoint users)?
5. What are the systems and applications within the organization that rely on the use of digital certificates (i.e., web servers, load balancers, firewalls, devices, containers, etc.)?

Next Steps

Choosing the right certificate lifecycle automation solution has never been more important to the security and continuity of your business. Letting your use cases, team skillsets, resource constraints, and risk exposure guide your selection is the best way to achieve sustainable, scalable success.

CERTIFICATE LIFECYCLE AUTOMATION

Only a limited number of certificates can be managed manually using a spreadsheet, but this process isn't scalable. It also only accounts for known certificates, leaving organizations with gaps in visibility.

Learn more >

PKI AS-A-SERVICE

CA-provided tools are a step up from spreadsheets, but they will not address complex, multi-vendor environments and only offer limited discovery and management capabilities in comparison to full lifecycle management tools.

Learn more >

WHAT ABOUT SSH KEYS?

If you're looking for SSH key management, we've got you covered. Keyfactor can provide flexible modules to extend management capabilities across all of your cryptographic assets, including symmetric and SSH keys. Contact us for more information.

EVALUATE KEYFACTOR NOW

Do you want to learn more about how complete PKI as-a-Service and certificate lifecycle automation can help improve your security posture?

SPEAK TO AN EXPERT

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security, IT and InfoSec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

Learn more at www.keyfactor.com.

- +1.216.785.2990
- www.keyfactor.com

Keyfactor Headquarters

6150 Oak Tree Blvd., Suite 200 Independence, OH 44131