KEYFACTOR

Buyer's Guide:

Certificate Lifecycle Automation

Practical advice for choosing your first (or next) solution

Why you're here

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

Maybe you've failed an audit or experienced 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 will help you choose the right certificate management solution for your organization. It identifies core capabilities to effectively manage certificates in large-scale, complex, and multi-vendor environments. It also contains essential questions to ask vendors and critical insights from PKI experts.

Table of contents

Here's the situation

Today's enterprises face serious challenges with certificates

Machine identities, such as X.509 certificates, have always been challenging for security teams. Enterprises lack visibility of where keys and certificates reside, making it much harder to manage them effectively and avoid costly outages or application failures.

The shift to cloud, containerization, mobile, and IoT devices brings thousands more certificates into the mix. Meanwhile, security teams often struggle to manage these certificates using an inefficient patchwork of spreadsheets, homegrown tools, and CA interfaces that fail to provide the visibility and automation needed to keep pace.

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, exposing organizations to a high risk of outages.

CA vendor tools

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

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

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 certificates across their environment. Many tools and approaches exist, but some are more effective than others to meet your specific needs.

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

Where to start

Many tools are on the market today, but some are more effective than others for the scale and complexity of your environment. The fundamental 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 managing every certificate across your environment easy and affordable 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 expose you to risk.

Deployment flexibility is key

Any solution must 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), CA, and device or platform. It also means being able to deploy how and where you need to — as a software appliance, as a service, or combined with a fully managed PKI.

Orchestration, not middleware

A platform's architecture significantly impacts 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 manage them fully. Instead, look for modular, loosely coupled solutions that act as certificate orchestrators, not transaction pipelines or bottlenecks.

Why manage every certificate?

Most vendors and organizations hyper-focus on certificates used for SSL/TLS endpoints on the network. However, this is only a fraction of the certificates in your environment. Cloud services, containers, and service meshes all use machine-to-machine communications that rely on client authentication certificates. Many outages are not caused by expired SSL server certificates but by failure to track 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 determine how they implement the capabilities and why that's important.

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 environments.

Some vendors rely heavily on the network for discovery, which requires complex set-up and firewall configuration and 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.

Ask vendors

- Can the vendor discover and manage every certificate, even those not issued through its platform?
- Does the solution require significant firewall rules and port configuration changes 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?
- Can the solution discover and inventory certificates issued via EMM/MDM and IaaS platforms?

What to look for:

CA synchronization

Real-time inventory of CA databases.

Certificate discovery starts at the source. Your chosen solution should continuously synchronize inventory from internal and public CAs. This ensures that every certificate is identified, regardless of how it was issued. Vendors that rely only on network-based certificate discovery typically require resource-intensive scanning agents and do not offer real-time visibility of certificates at the CA level.

Network-based discovery

Scalable SSL/TLS discovery across IPs 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 can be finely tuned to your network operations and deployed modularly across different network segments or cloud environments.

Low-level discovery

Application and device-level inventory.

If a certificate isn't bound to an IP or port, it won't appear in a network scan. More integrated solutions use agent-based or agentless methods to inventory key and certificate stores. It's also important to inventory trust stores and have the ability to remove or add a new root of trust quickly.

Real-time monitoring & reporting

Discovery and monitoring work together to give you actionable intelligence on your certificates. Once you've pulled in a complete inventory, you'll need to actively monitor them for expiration, compliance, and usage.

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:

Alerts and workflows

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.

Single pane of glass

An intuitive dashboard provides an at-a-glance view 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 particular certificates or groups from the dashboard to view more details or take action on any identified vulnerabilities.

Configurable metadata

Allows admins to group certificates and tag them with business or application-relevant 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 you can use.

Intuitive reporting

Allows users to customize and run scheduled reports and 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.

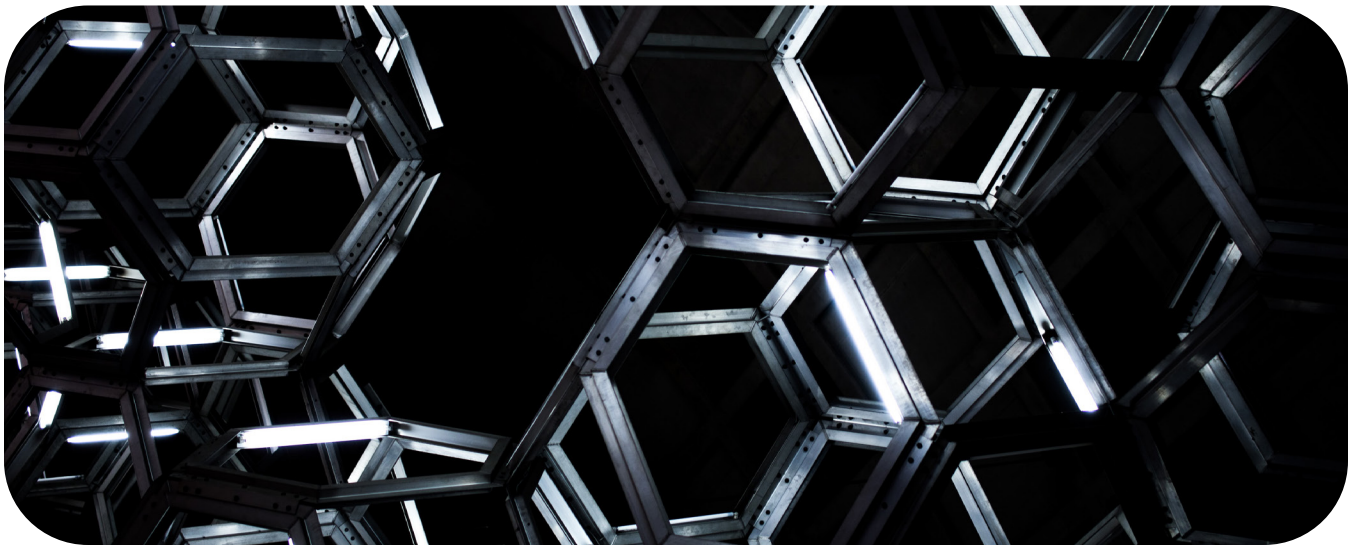
Lifecycle automation

As certificate counts rise from hundreds to thousands, managing them becomes more challenging. This is only compounded by changing industry standards and shorter SSL/TLS certificate lifespans.

Automation is key. A practical solution should enable your team to automate the deployment and lifecycle of certificates across large, complex, and multi-vendor environments — 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 case 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:

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 vendor solution. The ability to integrate with multiple CA vendors, or migrate from one CA to another quickly, is essential to ensure business continuity and support for current and future requirements.

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 integrating with existing ITSM workflows.

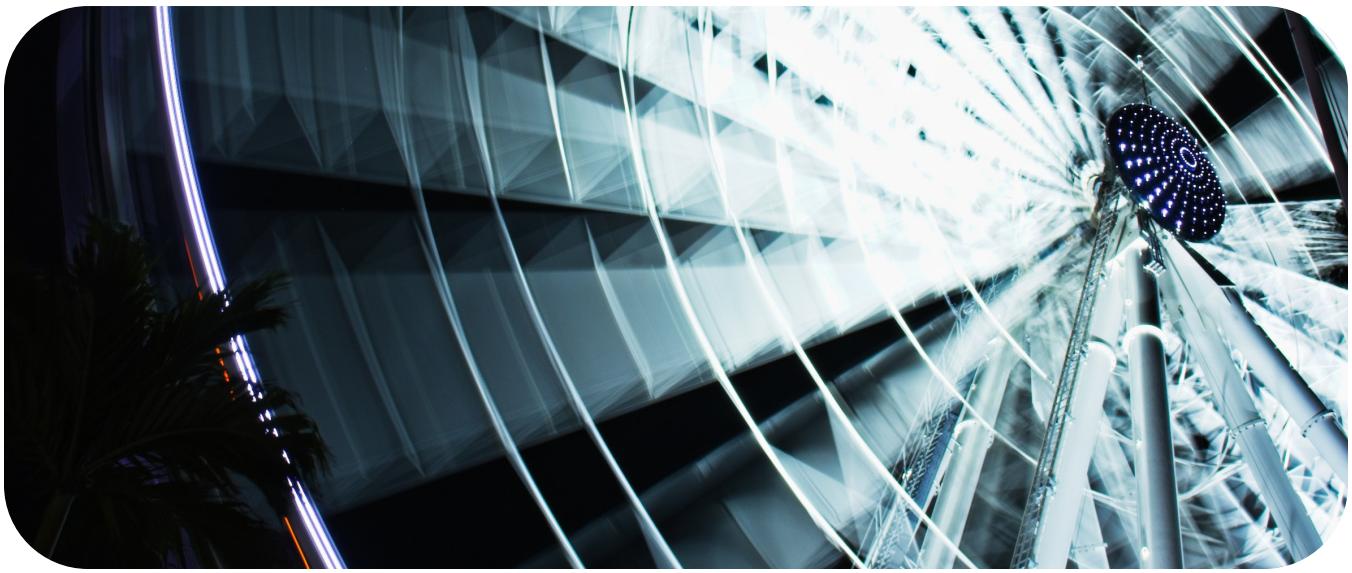
Ecosystem integration

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 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:

Protocol support

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

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

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 give the security team visibility and control while minimizing disruption to developers.

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 and 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 essential element in certificate lifecycle automation is implementing 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:

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 of 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.

Granular role-based access

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

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

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 to retrieve credentials automatically.

What to avoid

Far too many companies purchase a certificate lifecycle automation solution only to discover 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.

01 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.

02 Don't confuse protocol with platform

Don't rely on protocols like ACME to be a replacement for certificate management. While these and other protocols (SCEP, EST, Autoenrollment) do a decent job of issuing and, in some cases renewing certificates, they are not a complete certificate management solution. Total lifecycle management includes critical operations like revocation, automated endpoint configuration to bind the certificates, and root of trust management.

03 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.

04 Think about your environment

Don't get locked into an on-prem solution that won't scale with your organization's requirements. Most companies have embraced the cloud in some shape or form. Consider the platform architecture and the flexibility needed to support your environment, whether your organization is just starting in the cloud, running a hybrid, or all in on multi-cloud. Modern CLM solutions should offer the flexibility to deploy however and wherever you need them, including SaaS-delivered models.

Deployment options

Keyfactor offers the flexibility to deploy or migrate certificate management (and PKI) wherever you need it. On-premise, in the cloud, as a service, or combined with fully managed PKI – pick the option that best fits your organization's needs.

On-premise [Self-hosted]: Some organizations still want to host their certificate infrastructure, and in this case, your CLM should support on-premise support.

CLAaaS [Hybrid]: Many organizations have an eye on moving significant assets to the cloud. However, in many cases, existing infrastructure remains on-premise, like legacy PKI. In this case, or cases of a complete migration to the cloud, organizations need the ability to run parts (or all of the CLM infrastructure) in the cloud while still managing on-premise assets.

PKIaaS [Cloud]: When the goal is to move to the cloud, PKIaaS combined with CLAaaS is a great solution to remove the operational burden of running this unique but critical infrastructure.

Learn more about Keyfactor's flexible deployment options →

Expert insight: Two key areas to consider when it comes to platform architecture

- **Modular:** CLM can mean different things depending on the organization, and you might not know precisely how the end-state looks when you begin. Therefore, it is essential to look for products that enable you to implement them modularly. It's vital that each organization set its priorities to address any risk — and for that, there is not a "one size fits all" approach. Taking a modular approach allows maximum flexibility and the ability to shift based on the organization's needs.
- **Scalable:** As the saying goes, you don't know what you don't know. The reality is most organizations have no idea exactly how many certificates they have. Therefore, asking an organization to commit to a product or licensing agreement based on a number of certificates only results in one outcome — surprises. Likewise, it's unlikely you can predict the total number of certificates your organization may have in future. It could be a few thousand more than you have today, but it could just as easily be millions more. It's important to consider future growth and scale alongside cost certainty.

What about your 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 maintenance frustration.

Those with the right skills and expertise to run a PKI are hard to find and keep. If your organization lacks the resources or expertise to run PKI effectively and support 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?

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

Finding the right fit

Finding the right vendor to work with is just as important as the product's functionality. 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 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

Scalable licensing

When evaluating vendors, ensure 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.

Depth in expertise

PKI isn't just about technology; it's about finding the level of expertise to complete your project on time and correctly. 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.

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.

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.

Product innovation

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

Five 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 five questions you should be able to answer before you start.

01 **What is the timeframe for the evaluation? What is the urgency for product selection based on evaluation?**

02 **What are the specific use cases or business requirements — both existing and future — that the solution must address?**

03 **How much can your organization invest in properly evaluating solutions against these requirements?**

04 **What criteria are required for different user groups within the organization (e.g., PKI admins, developers, security analysts, network admins, endpoint users)?**

05 **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 critical 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. Still, they will not address complex, multi-vendor environments and only offer limited discovery and management capabilities compared to complete lifecycle management tools.

Learn more ↗

Evaluate Keyfactor now

Do you want to learn more about how certificate lifecycle automation and modernized PKI can help improve your security posture?

Speak to an expert ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)