KEYFACTOR

EBOOK

# How Investing in Certificate Automation Protects Your Business & Bottom Line

Plus, get a curated list of key questions to build a strong business case and highlight specific benefits for your organization

# Table of contents

# Executive Summary

As we rely more on digital services, managing machine identities and certificates by hand is becoming inefficient and costly. Automating certificate lifecycle management is a smart choice to avoid expensive outages, **strengthen security posture**, and prepare for future challenges like quantum computing.

**It all comes down to digital trust.** With the rapid growth of machine identities and the impending arrival of quantum computing, innovation and cybersecurity must go hand in hand. Mismanaged certificates can lead to serious financial losses and reputation damage.

Availability is key in cybersecurity. Outages go beyond lost revenue – they can damage customer confidence and lead to compliance issues. When certificate management is inadequate, it hampers the effectiveness of your security, IT, and infrastructure teams, increases the risk of breaches, and creates unnecessary reliance on outdated tools or vendors.

As you read through this ebook, keep in mind that it's designed to help you build a compelling business case to present to your executives. The content in this eBook will help you explore the projected cost savings, improved security, and operational efficiency that will provide both immediate and long-term benefits for your company.

# Introduction

With automation, your team can focus on higher-value tasks. In the 2024 PKI & Digital Trust Report, we uncovered the impact of investing in certificate lifecycle automation (CLA).

As your business expands its digital operations, automating certificate management becomes essential. This investment not only reduces the risk and business disruption caused by outages, it also allows security teams to focus on what matters most, not tedious certificate-related tasks that consume hours of their day.

Here we'll cover the financial insights we've learned. Investing in CLA isn't just a technical necessity — it's smart business.

# Assessing Where You Are Today

Whether you're managing certificates through manual processes or relying on more sophisticated automation tools, our digital trust report found that the choice of tool impacts how well your infrastructure supports your organization's security, compliance, and business continuity.

There are three key stops on the journey to fully automated, scalable certificate lifecycle management. We've broken them down so you can identify the needs and trade-offs unique to your organization and circumstances.

38%

of organizations manage PKI with a patchwork of homegrown solutions: open-source tools, spreadsheets, and manual processes.

## Homegrown solutions

Many businesses have small IT and security budgets and rely on the ingenuity of infosec professionals to create a certificate lifecycle program with open-source, homegrown, and low-cost tools like spreadsheets. If their organizational risk is relatively low and their certificate landscape isn't complex, these solutions may sustain the organization for some time.

While such patchwork solutions may appear cost-friendly, they come with a few challenges and maintenance overhead.

- They fall short of providing critical information, such as certificate ownership, workflow processes, and key storage information.
- Because these systems are heavily manual, they invite human error and misconfigurations that may lead to an outage or breach.
- When the staff members who create this system retire or move on, new and remaining staff will likely have a difficult time continuing and managing this system.
- Manual spreadsheets and database tracking only show you the certificates you know about, but it's the unmanaged and undiscovered certificates that most often cause disruptive outages.

Even if the company isn't experiencing significant growth, certificate volume will likely grow as it adopts new technologies like cloud, developer tooling, and AI solutions. Emerging regulations like PCI-DSS or HIPAA and factors like shrinking certificate lifespans will only compound the challenge of maintaining a brittle, patchwork certificate management system.

## Prepare for the next stop on the CLA journey:

The first step to improvement is moving away from manual processes. Begin by implementing basic automation for certificate discovery, revocation, and renewal. Look for solutions that give your team better visibility into the certificate landscape and centralize management.

## Vendor-Supported Solutions

Tools provided by your SSL/TLS certificate provider can help provide some visibility into certificates, while supporting basic protocols. They often provide basic lifecycle automation and can be more easily integrated into other platforms and services. Updates and support are more reliable compared to the homegrown maturity phase.

However, this stage still comes with a few problems:

- SSL/TLS provided tools lead to a fragmented view of your certificate landscape. Juggling multiple dashboards and interfaces between your internal PKI, public CA, and other CA tools creates complexity. The average company has 7 different PKI and CA tools in use, making it impossible to manage with a solution that only covers a few.

- SSL/TLS vendor tools support protocols like ACME and SCEP, but offer limited automation capabilities, making it difficult to integrate with their applications and automate critical processes like certificate provisioning and installation.

- SSL/TLS vendor provided tools can help you simplify management of some certificates, but they don't fully support other SSL/TLS providers, meaning you're locked into a single vendor.

Vendor-supported solutions give your team a toolkit actually designed for managing certificate lifecycles. However, some organizations find that while such tools lower complexity, they don't solve the root causes of certificate issues, especially at scale.

**30%**

of organizations rely on tools provided by certificate vendors.

### Prepare for the next stop on the CLA journey:

Move beyond vendor-specific tools to adopt a centralized certificate lifecycle management platform that spans across all CAs. This will give you complete visibility and control over your entire certificate environment, reducing complexity and operational risk. Unify certificate management under one platform to streamline workflows, reduce human error, and manage every certificate proactively regardless of its source.

## Dedicated Certificate Lifecycle Management

Organizations that have implemented a dedicated solution are able to handle discovery, issuance, renewal and revocation across all environments. At this level, your team is no longer in reactive mode; instead, they're empowered with automation and real-time visibility into every certificate in use through a universal hub. Outages and compliance errors are rare, and your PKI infrastructure is resilient and scalable for the future.

As a result, your organization appears trustworthy, secure, and highly reliable. Customers and partners can count on your infrastructure, and you're seen as a leader in security best practices. With a robust CLA system in place, you're not only protecting current operations but planning and preparing for emerging threats like post-quantum cryptography.

100% visibility

You can't secure what you can't see.

How to stay ahead:

To remain at the forefront of CLA, it's critical to continue investing in automation and crypto-agility. Stay proactive by conducting regular audits of your cryptographic assets, expanding automation into new areas like IoT device management, and preparing your infrastructure for post-quantum security standards.

# The Outage Problem

The solution you choose is a determining factor in the likelihood of costly outages. Improved certificate lifecycle management capabilities reduce the risk of certificate-related incidents and operational fallout.

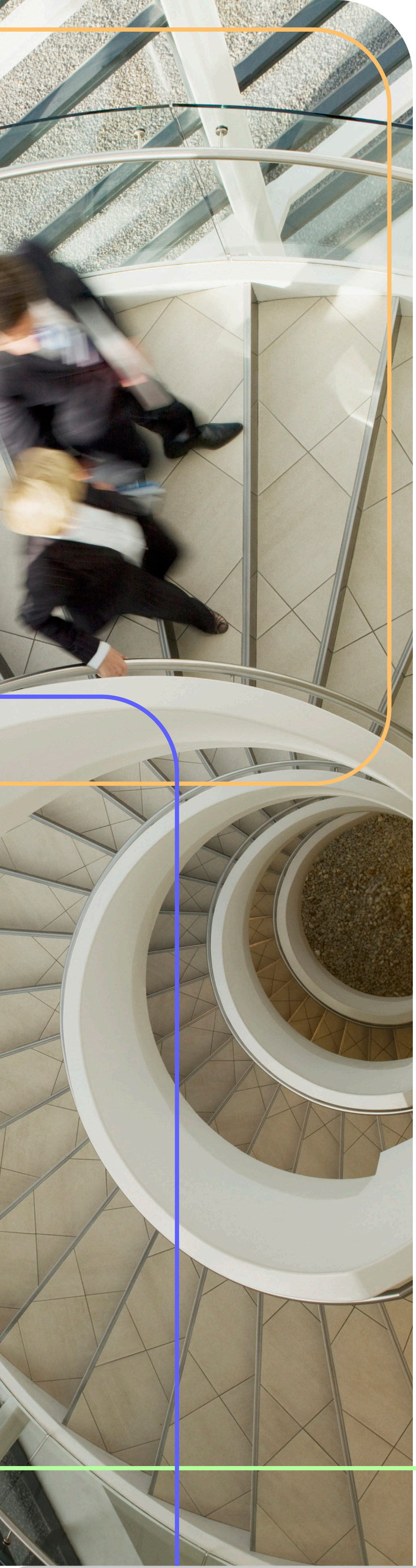
Organizations managing certificates with spreadsheets or homegrown tools are far more vulnerable to outages. When certificates expire, critical systems can go offline, damaging your business and risking security. The more certificates you have, the harder they are to track manually, and the more likely it is that one will slip through the cracks.

According to the PKI and Digital Trust Report, organizations with a dedicated CLA tool were 3 times more likely to experience no outages than organizations relying on spreadsheets, and 2 times more likely than organizations using homegrown solutions.

The math is clear: without automation, outages are inevitable. Manual processes introduce delays, increase the risk of errors, and overwhelm teams as the number of certificates grows. Investing in a dedicated CLA solution improves efficiency and reduces the risk of costly outages that damage your business's reputation and bottom line.

Because of all these risks, it's important to build your business case and protect your organization's bottom line. We've included a set of questions at the end of this guide so you can show a breakdown of benefits to your company, addressing current issues and potential financial gains.

By presenting the business case, you can clearly justify the investment in certificate lifecycle automation. Almost anyone who looks at your template will see that the projected cost savings, increased security, and operational efficiency make this a smart investment, securing both immediate and long-term benefits.



# The Hidden Costs of Free Tools

Relying on homegrown solutions, spreadsheets, and disparate vendor tools comes with hidden costs that extend far beyond operational inefficiencies. From increased workload on your team to revenue lost from service disruptions, the price you pay for underdeveloped certificate lifecycle management adds up quickly. The more certificates you have, the harder they are to track manually, and the more likely it is that one will slip through the cracks.

## Increased operational burden

According to the PKI & Digital Trust Report, 84% of organizations using homegrown solutions experienced a significant operational burden in 2024. This number is trending upwards: 60% in 2021, 70% in 2022, and 72% in 2023. The operational burden results from the constant manual tasks needed to manage certificates, troubleshoot outages, and ensure compliance – all without the help of automation.

## More certificate outages

For organizations relying on spreadsheets, 61% reported multiple incidents where expired certificates caused outages. Those using slightly more sophisticated solutions didn't fare much better, with 57% experiencing outages. These outages aren't just inconvenient – they're avoidable, costly, and frustrating for everyone involved.

When certificates expire, critical systems can go down, affecting everything from internal applications to customer-facing services. Outages result in lost productivity, lost revenue, and a damaged reputation. In an age marked by the necessity for digital trust, such outages can make customers and partners think twice before trusting your organization with their business.

## Institutional knowledge gaps and business continuity risks

In organizations using a combination of tools held together by digital string and chewing gum, one or two champion team members may have built and understand the system. But what happens when they leave? The hidden costs of free or patchwork certificate management solutions include institutional knowledge, if new hires are left trying to untangle a web of scripts, spreadsheets, and manual processes with little to no documentation.

## Time lost and salaries wasted

On average, it takes a dedicated team 2.6 hours to identify the root cause of a certificate-related outage and another 2.7 hours to remediate it. That's more than five hours spent responding to a single incident. Compound that by the average number of staff members involved in resolving an outage - eight - and you are left with 40 hours of lost productivity across the organization.

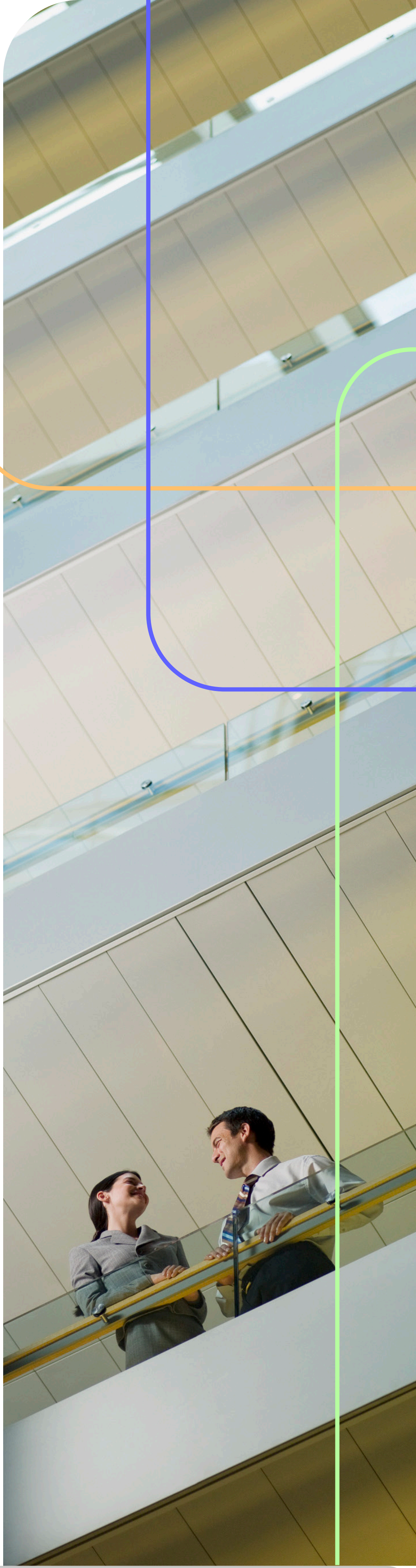
## Impact on productivity and outage downtime

Certificate-related outages have a cascading effect on your entire organization. When internal applications go down, employees are left without the tools they need to do their jobs. If external applications are affected, the consequences reach even further – customers and partners may be unable to access critical services, leading to lost revenue and damaged relationships.

## The costs of a security incident

In the past 24 months, organizations experienced an average of three incidents where a breach or security-related incident occurred due to lost or stolen keys or certs.

The cost of a breach can be immeasurable. Forensic investigations, remediation efforts, and ongoing monitoring all require significant resources, and that's before you take the potential fines and penalties for compliance violations into account. The reputational damage of a security breach outstrips the inconvenience of a minor outage, leading to lost customers and long-term brand harm.



# Achieve Digital Trust

Outages don't happen in a vacuum. When certificates expire and systems go down, the ripple effect spreads throughout your organization and beyond. To avoid these risks and build a foundation of digital trust, invest in automated certificate lifecycle management. Digital trust is more than a technical achievement—it's the assurance your business operates securely and reliably, providing confidence to employees, customers, and stakeholders alike.

Organizations that automate certificate lifecycle management see a significant reduction in outages, operational strain, and security incidents.

## Here's how investing in certificate management helps build digital trust:

### ☑ Centralized visibility and discovery

Instead of relying on scattered open-source tools or spreadsheets, your team has a comprehensive view of all certificates across departments and applications. This complete visibility means fewer missed renewals, reduced risk of outages, and better ability to track certificate lifecycles. No certificate goes unnoticed, providing peace of mind to IT and security teams.

### ☑ Automated issuance and lifecycle management

Automation is key to minimizing human error and running certificate management smoothly. Automated issuance, renewal, and revocation take the manual burden off your team, allowing certificates to be issued consistently and on time without relying on constant oversight.

### ☑ Fewer — or zero — outages

With centralized management and automation in place, the likelihood of certificate-related outages drops dramatically. As mentioned above, organizations with a dedicated CLA tool were 3 times more likely to experience zero outages over those relying on spreadsheets or homegrown solutions. Taking certificate failures off the table means you can focus on growth and innovation without the looming threat of unexpected downtime.

### ☑ Free up staff for higher-priority tasks

Manual certificate management is time-consuming and inefficient, tying up valuable staff resources. Automating repetitive tasks reduces the pressure on your workforce and allows them to focus on the areas where their expertise matters most. Proactive staff improve your security posture, drive innovation, and respond to emerging threats quickly.

### ☑ Address skill shortages with access to expertise

By implementing automated tools and solutions for certificate management or employing vendor services like PKI-as-a-Service, organizations can also tap into external expertise through vendor support and integrated best practices. This helps bridge the gap in cybersecurity talent and reduces the pressure on your team to handle everything internally.

### ☑ Prepare for post-quantum cryptography

Organizations must start now to prepare for quantum computing. An automated, scalable PKI solution for certificate management equips your organization with crypto-agility, allowing you to quickly pivot and implement quantum-resistant algorithms.

## The Bottom Line

The path to digital trust begins with reducing risk, automating critical processes, and equipping your organization to handle future challenges.

# Key Benefits of CLA

As digital services continue to grow, it's essential to prioritize working smarter, not harder — especially as your organization gears up for future challenges like quantum computing.

**To build a compelling business case for certificate lifecycle automation, it's crucial to articulate the financial and operational benefits.**

To help you outline the value of certificate lifecycle automation, consider the following questions as your "cheat sheet." By addressing these points, you'll be well-equipped to present automation as a strategic investment that prepares your organization for the future.

## Improved Team Efficiency

BENEFIT:

CLA frees IT and security teams from manual tasks, allowing them to focus on strategic projects.

### Questions to Ask

- What are the average costs of a security breach, including forensic investigations, remediation, and fines?
- How often do expired or mismanaged certificates contribute to security?
- What is the estimated savings from reducing compliance fines or avoiding security breaches?

## Improved Security Posture

BENEFIT:

CLA mitigates risks tied to expiring or compromised certificates, reducing breach likelihood and compliance risks.

### Questions to Ask

- What are the average costs of a security breach, including forensic investigations, remediation, and fines?
- How often do expired or mismanaged certificates contribute to security?
- What are the estimated savings from reducing compliance fines or avoiding security breaches?

## Crypto-Agility and Future-Proofing

BENEFIT:

CLA enables crypto-agility, allowing readiness for post-quantum cryptography and emerging threats.

### Questions to Ask

- Have we prepared for quantum-based threats like "harvest now, decrypt later" (i.e., is current data at risk based on the bad guys stealing data now)?
- What are the estimated costs of potential data exposure from quantum-related breaches?
- What would be the business value of positioning our organization as a leader in quantum-readiness?

## Cost Savings

BENEFIT:

CLA reduces the need for external vendors and improves operational efficiency, cutting daily productivity losses.

### Questions to Ask

- How much time do non-PKI experts, such as application owners, spend managing certificates?
- What errors or delays commonly arise from manual certificate management, and how do they impact productivity?
- Could automation help us redirect resources to core business activities? What would be the estimated cost savings?
- What specific inefficiencies or duplicated efforts could CLA eliminate in our current processes?

# Learn more

See how achieving a dynamic state with certificate lifecycle automation can help keep your certificates and keys more secure with less effort:

Request a demo of Keyfactor Command now.

Request a demo ↗

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)