SECTIGO®

# 47-Day

## survival guide

Let’s put an end to manual certificate management

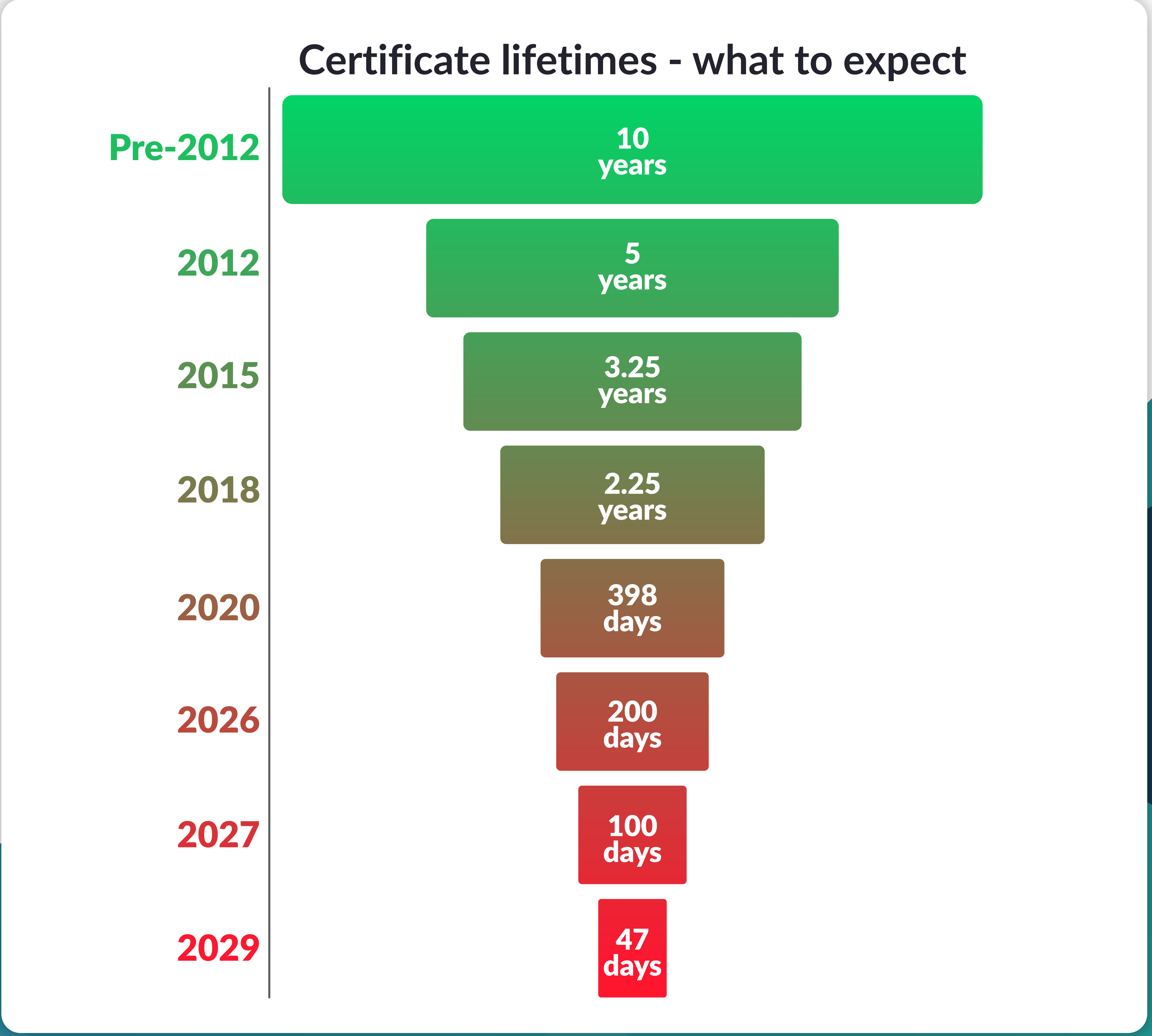
# Introduction to short certificate lifespans

For the past few years, the maximum term for a public SSL/TLS certificates has continued to shrink, dropping from three years, to two, to one. This trend is set to continue, as the largest browsers are advocating for even shorter digital certificate lifespans in the future.

On March, 3, 2023, Google's "Moving Forward, Together" roadmap laid out its intention to further reduce TLS certificate maximum validity from 398 to 90 days. Google shared: "Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes."

In January 2025, Apple submitted an official ballot to the CA/Browser Forum proposing a gradual reduction of the maximum SSL/TLS certificate lifespan to 47 days by 2029.
As of April 11, 2025, the 47-day ballot proposed by Apple, and sponsored by Sectigo, has passed. Organizations need to be prepared now for the changes to come.

So, what does this mean for your cybersecurity?


Certificate lifetimes - what to expect

The road to shorter certificates is now clear: organizations must prepare now to ensure that their business stays secure and agile in the face of changing regulations. There's no reason not to get ahead of certificate management. This is a call to action for organizations to automate now, ensuring they are ready for the challenges and are not left scrambling when these shorter lifespans start going into effect.

Sectigo supports shortening certificate lifecycles to uphold the integrity of the WebPKI ecosystem and enhance security for all customers. As the only CA to endorse this ballot - alongside Chrome, Mozilla, and Apple - we are proud to advocate for a phased transition to shorter lifecycles.

Ultimately, this is a major change in policy that will have serious ramifications for organizations unable to automate the issuance and lifecycle management of digital certificates.

We are fully prepared for this new era, and we want you to be ready too, which is why we created this 47-day certificate readiness plan for your organization.

**There's no reason not to get ahead of certificate management.**

# Why do we need shorter certificate lifespans?

398 days (the current maximum term allowed by the CA/Browser Forum Baseline Requirements and by various major root programs) is a long time for a compromised certificate to exist. After all, the longer a certificate remains valid, the more likely the risk of it becoming compromised.

Shorter certificate lifespans help reduce the risk of cybercriminals exploiting outdated certificates that may be overlooked when companies close, employees leave, organizations merge, domain names are sold or transferred, or businesses undergo rebranding.

When certificates are improperly issued or compromised, mass revocation is necessary but can be a complex process and damaging to businesses. Shorter certificate lifecycles, which minimize exposure time, reduce risks associated with compromised certificates, and ensure more frequent validation of certificate integrity and security practices.

The change will enable the agility required to transition the ecosystem to quantum-resistant algorithms, helping enterprises secure their sensitive data against potential future threats using quantum computers. This proactive approach, known as cryptoagility, ensures that organizations can quickly adapt their cryptographic systems to evolving threats and advancements, maintaining robust security regardless of shifts in technology or attack methods.

# 47-day TLS marks the end of the manual management era

47-day TLS is essentially an 88% reduction in maximum term.

But what this means for businesses relying on manual certificate lifecycle management is:

12x more work
12x more certificates
12x higher risk of missing a renewal

| Timeline | Max. TLS term | Renewal frequency |
|---|---|---|
| 3/15/26 | 200 days | 2x |
| 3/15/27 | 100 days | 4-5x |
| 3/15/29 | 47 days | 12x |

With certificates needing renewal every 47 days, as opposed to the current 398-day term, businesses will need to renew all their public certificates every month, as opposed to every year (this includes accounting for a two-week grace period to avoid outages if issues arise during renewal). It's easy to understand how this number can quickly blow up if an organization has a lot of certificates.

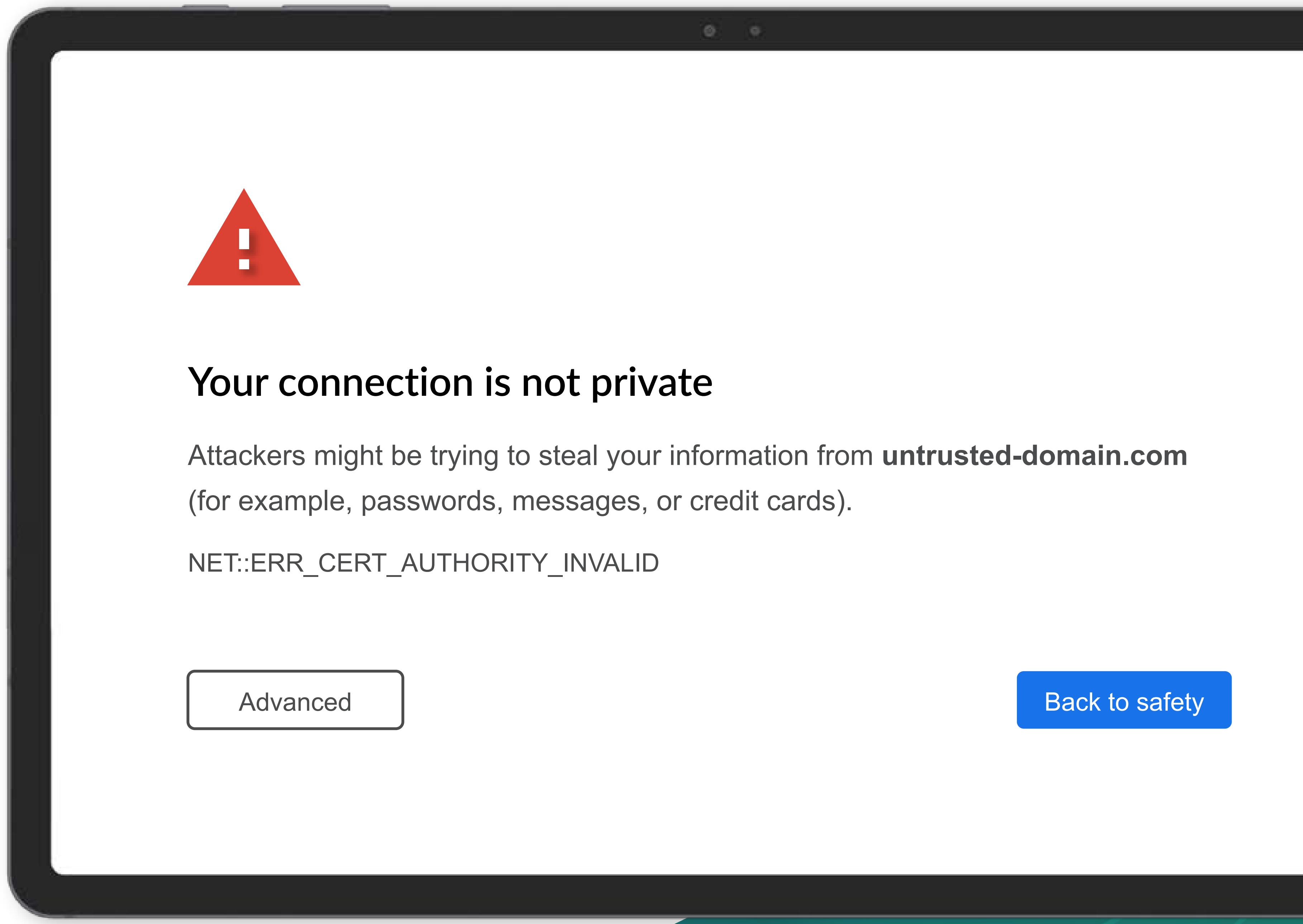
This increase in certificates will likely overwhelm IT teams handling manual management, leading to a higher risk of outages and breaches, reputational damage and loss of revenue. Managing certificates manually will become practically impossible under 47-day TLS, as it demands constant planning, multiple validations, and precise handling of certificate issuance and expiration tracking. Organizations will need to adopt automated solutions to maintain digital trust and avoid operational risks.

# What happens if no action is taken

Public digital certificates play a crucial role in keeping websites secure and accessible for customers. They verify a website's identity and encrypt communications, protecting users' data. However, when a certificate expire and is not renewed on time it will trigger a browser warning informing users that their connection is no longer private, causing them to leave assuming (rightly so) that the site is unsafe.

These warnings not only drive customers away but also damage a business's reputation. Many users never return after encountering such issues, leading to long-term revenue loss. The financial impact can be severe, with businesses losing both immediate sales and future revenue as customer trust deteriorates.

But this is just the tip of the iceberg. A missed certificate renewal can also lead to outages, data breaches, service disruptions, and costly non-compliance fines.



Your connection is not private

Attackers might be trying to steal your information from **untrusted-domain.com** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

# It’s time to automate!

Google and Apple's upcoming reduction in TLS certificate lifespan will significantly impact organizations that cannot leverage automation for managing the increased volume of digital certificates. Google's “Moving Forward, Together” roadmap heavily promotes the use of automation to:

- Increase agility
- Enable stability
- Enhance security
- Promote ecosystem simplicity

Automation is essential for handling frequent updates and certificate replacements required by shorter TLS lifespans. It minimizes human error, reduces downtime, and allows IT teams to seamlessly generate, deploy, and monitor certificates across systems. Automated processes ensure timely renewals, preventing security risks from expired or misconfigured certificates.

## Now is the time to act.

To maintain digital trust, organizations must scale their automation of certificate lifecycle management or face potential outages, breaches, and downtime. Google has provided ample warning, making it clear that preparation is critical. By adopting automated Certificate Lifecycle Management (CLM) systems, businesses can avoid chaos and unnecessary costs.

## How will your organization manage the switch to shorter TLS? Don’t worry.

Sectigo is offering a Certificate as a Service model for all public certificates, and you will not only save money, but be able to sleep easy knowing all your certificates are being managed effectively and automatically.

**Every certificate should be a managed certificate**

# What’s a "Certificate as a Service" model?

The "Certificate as a Service" model, (CaaS), streamlines certificate lifecycle management to meet the demands of shorter 47-day TLS cycles. In this model, renewals are automated and scheduled monthly, consistently on the same date, forming part of a broader Certificate Lifecycle Management (CLM) program that keeps certificates current, reducing expirations, outages, and compliance risks.

With this model, organizations can easily adapt to shorter certificate validity periods. The automated approach ensures continuous operations by reducing human error and the risk of service disruptions. Additionally, centralized visibility and control over certificates enhance compliance and reduce operational overhead by preventing unexpected certificate issues. Your organization will not need to be concerned about staff taking leave, holidays or summer breaks; with the CaaS model the automation will ensure absolute digital trust and certificate management without reliance on manual management.

This model aligns with the longstanding tradition of certificate management processes where beginning the renewal process starts well before the expiry date and allows for total prevention of last-minute technical glitches and preventable outages due to expired certificates. It is the optimal way to manage digital infrastructure, providing:

- A proactive, planned approach to digital trust
- Benefits of automation
- Enhanced security for the entire organization
- Cryptographic agility

*Sectigo’s "set it and forget it" CaaS model fully automates the certificate lifecycle process, eliminating the need for constant manual intervention. This seamless, hassle-free management of 47-day certificates reduces expiration and service disruption risks, allowing organizations to focus on core operations with confidence that their digital security remains robust, compliant, and free from additional operational burdens.*

# 47-day checklist

The time to prepare for 47-day certificate lifespans is now. To ensure your organization’s preparedness, follow this checklist.

## Step 1: Awareness & Discovery

Raise awareness within your organization about the shift to 47-day certificate lifespans. Ensure your team and leaders understand the implications and the need for frequent certificate renewals. Identify the key stakeholders (sysadmins, network admins, IT architects, engineers) responsible for managing public certificates.

To drive awareness:

- Conduct workshops or training on the impact of 47-day certificates and timely renewals.
- Send regular educational emails to teams and leadership.
- Share resources from trusted publications to help different departments understand the impact on business operations.

Simultaneously, perform a comprehensive **discovery of all SSL/TLS certificates** across your digital infrastructure. This process is crucial to identify and track all certificates, preventing unmonitored or rogue certificates that could cause service outages or security vulnerabilities.

- Gaining full visibility into the entire certificate landscape is essential to ensure that no certificates are missed, expired, or left vulnerable.

### Discovery process:

With Sectigo Certificate Manager (SCM): Scan your external and internal public certificates and always find all of your certificates, providing the visibility needed to manage certificates effectively.

Without SCM: Use tools like Certificate Transparency logs (e.g., https://crt.sh/) or third-party applications (Netcraft, Qualys) to scan certificates.

# Step 2: Vendor technology inventory

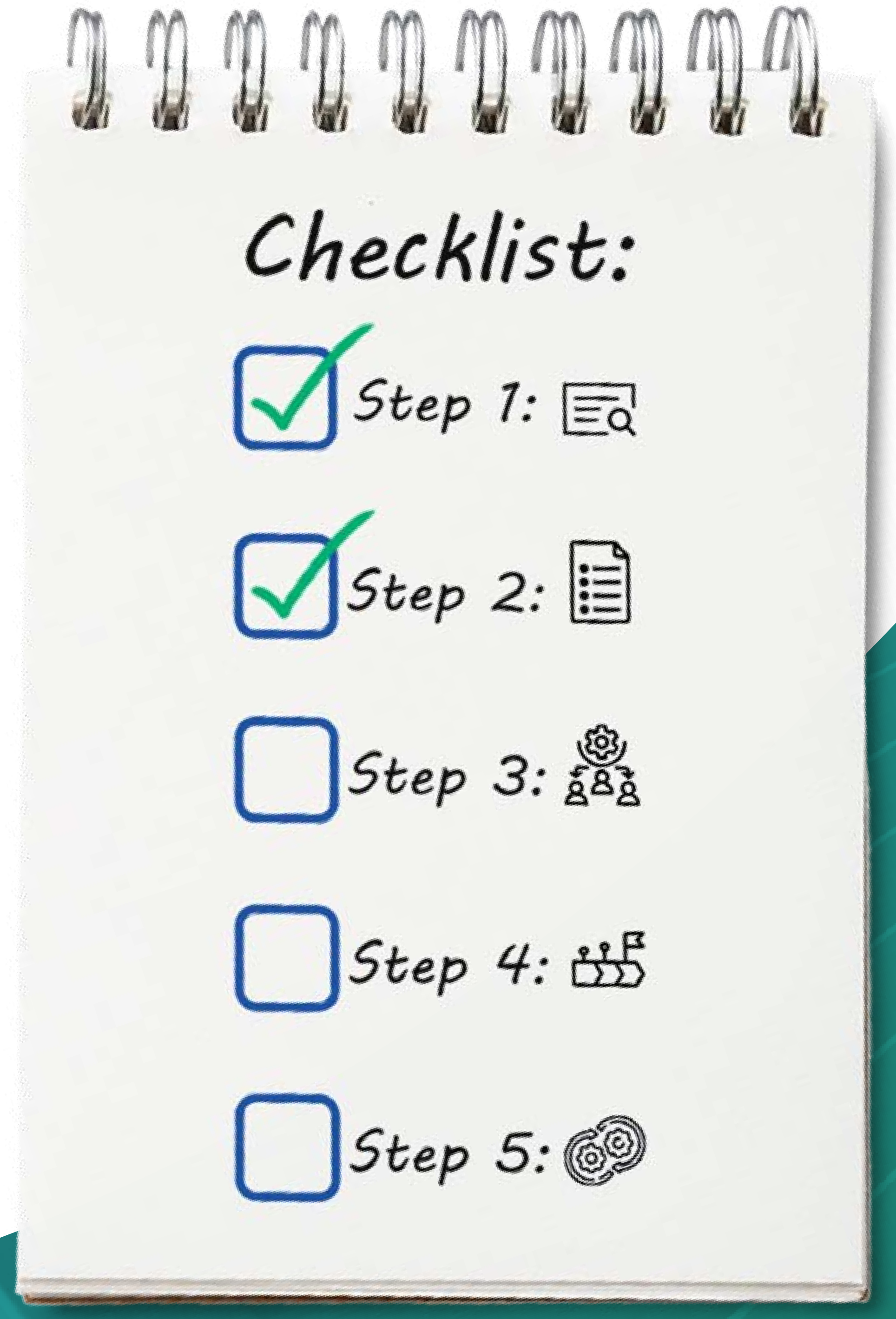
After discovering your certificates, the next step is to compile a thorough inventory of vendor technologies that rely on SSL/TLS certificates within your IT environment. This inventory helps you prioritize systems and applications based on criticality, ensuring that all key systems are accounted for in your certificate management strategy.

By identifying which technologies depend on certificates:

- You can better prepare for renewal cycles.
- You will be able to avoid disruptions to essential services.

See below for an example of what this could look like:

| Technology | Application | IP | Certificate | Notes |
|---|---|---|---|---|
| Amazon | ACM | xxx.xxx.xxx.xxx | slideshow.contoso.com | Application hosting |
| Apache | Apache | xxx.xxx.xxx.xxx | promo.contoso.com | Promotion website |
| Kubernetes | Kubernetes | xxx.xxx.xxx.xxx | payments.contoso.com | Kubernetes for payments |
| F5 | BIG-IP | xxx.xxx.xxx.xxx | germany.contoso.com | Load Balancer for Germany |
| Cisco | ASA | xxx.xxx.xxx.xxx | vpn.contoso.com | SSL VPN access |



# Step 3: Automation mapping

The Automatic Certificate Management Environment (ACME) is the preferred automation protocol for public certificate issuance and management. Google highlights ACME as core to the automation of digital certificate lifecycles and lays out the benefits of automation in the context of shorter certificate lifespans. These include increased resilience and agility, which can help organizations more easily transition to quantum-resistant algorithms.

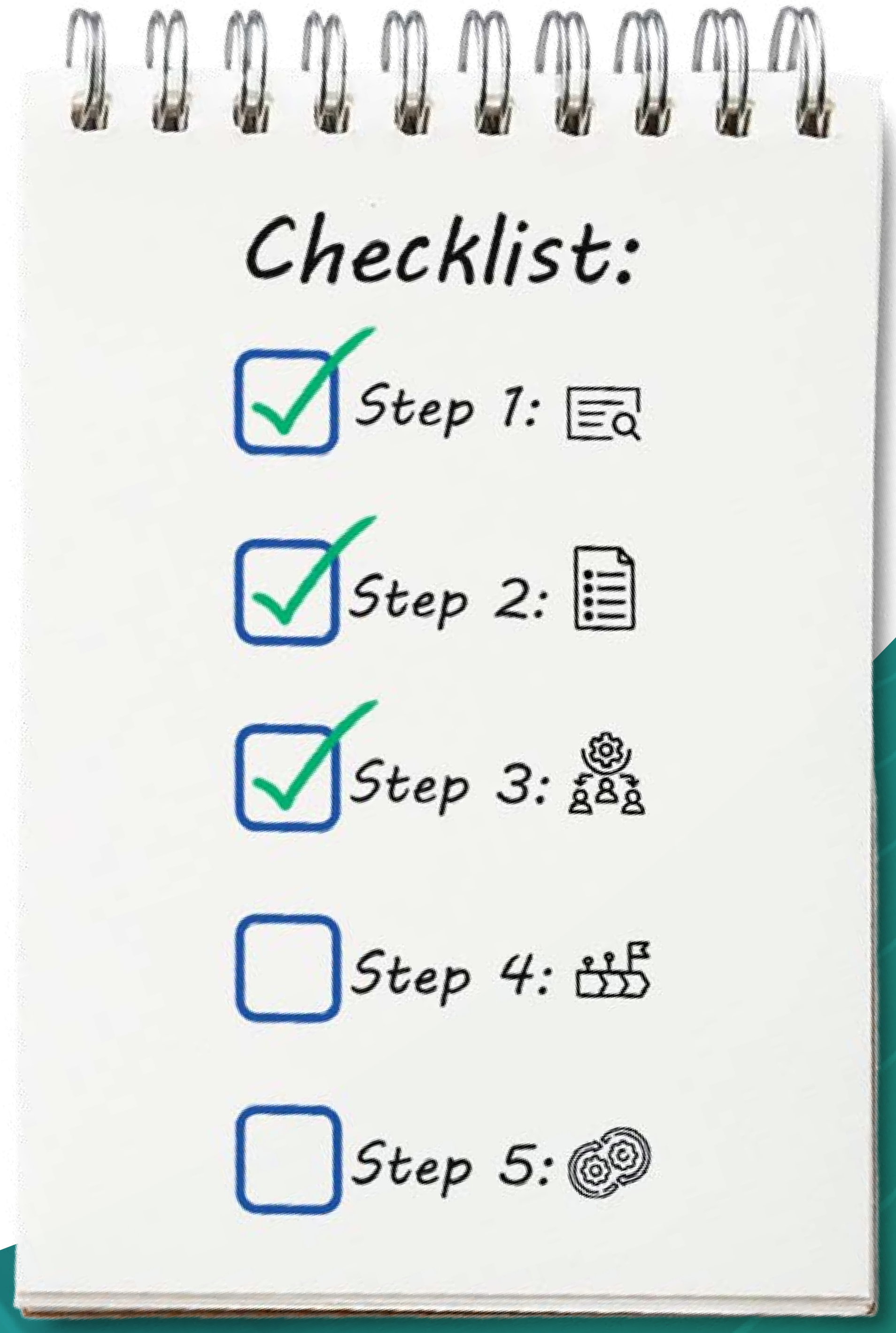
**Source a list of ACME clients for SSL/TLS certificate automation and map the available automation to the technology inventory you created in step three.**

Use SCM to collate a list of ACME clients which are known to integrate well with SCM. See below for a list of example ACME compatible technologies you can use with SCM.

**Note:** From ACME to SCEP, EST, its REST API and its network agent, Sectigo ensures seamless integration with diverse systems and workflows, enabling comprehensive automation across various environments. However, there will always be some technologies that cannot be fully automated.

## ACME clients for SSL/TLS certificate automation

| | | | |
|---|---|---|---|
| kubernetes | f5 | NGINX | HAPROXY |
| A10 | aws | Google Cloud | Kong |
| Microsoft IIS | paloalto NETWORKS | APACHE | node JS |



Checklist:

☑ Step 1:

☑ Step 2:

☑ Step 3:

□ Step 4:

□ Step 5:

# Step 4: Rollout plan

Developing a comprehensive rollout plan for the adoption of 47-day public certificate issuance will begin by a business setting clear objectives and identifying the resources, requirements, and priorities needed for a smooth transition.

You will need to determine which systems and certificates will be impacted and ensure that the appropriate automation tools are in place to manage frequent renewals.

To guarantee success:

- Set the objective
- Establish timelines
- Assign responsibilities
- Allocate necessary resources (such as software, personnel, and processes)

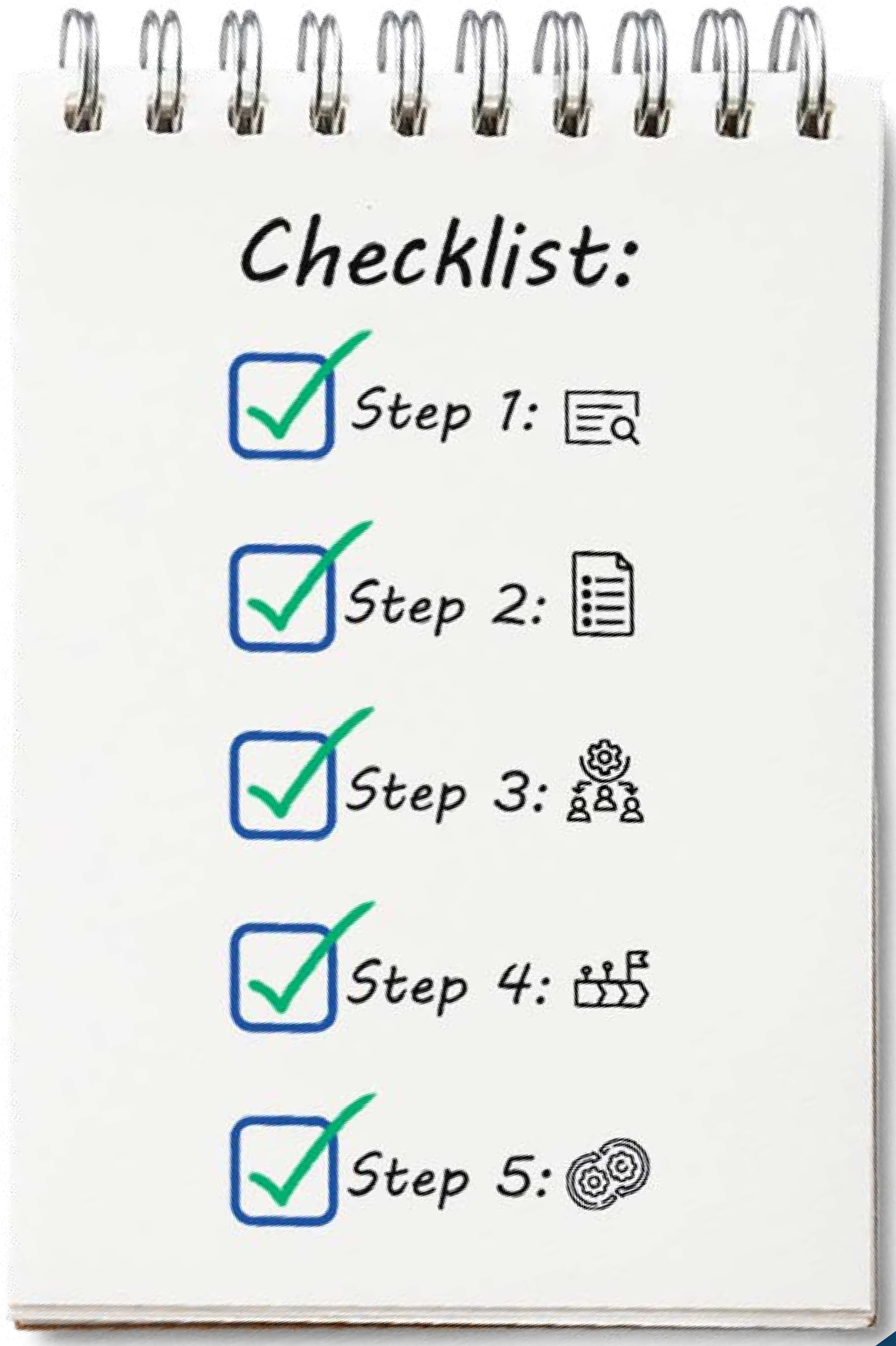
By creating structured processes and a detailed timeline, organizations can effectively manage the switch to 47-day TLS certificates without operational disruptions.

## Step 5: Crypto agility

Once all previous steps have been completed, organizations should solidify their readiness by creating a Cryptographic Center of Excellence (CCoE). For larger enterprises, this is essential to ensure crypto agility remains a priority across all departments, with active involvement from the C-suite to ensure buy-in of strategies and processes. The transition to 47-day certificates is just the beginning; businesses need to reassess how they manage certificates. Sectigo's "Certificates as a Service" model could then be adopted, whereby certificates are automated and continuously renewed, making the process seamless regardless of the certificate's validity period.

By embracing automation, organizations can establish rolling, ephemeral operations that ensure long-term security and agility, setting the foundation for continuous cryptographic readiness.

- Establish a dedicated team within the CCoE to oversee cryptographic policies, certificate management, and compliance.
- Regularly review and update cryptographic protocols and technologies to ensure alignment with evolving security standards and industry best practices.



# SCM can prepare your organization for 47-day TLS

Sectigo Certificate Manager (SCM) is the most robust CA agnostic CLM platform on the market. SCM is purpose built to continuously automate the lifecycles of all digital certificates within an ecosystem, regardless of their type or origin.

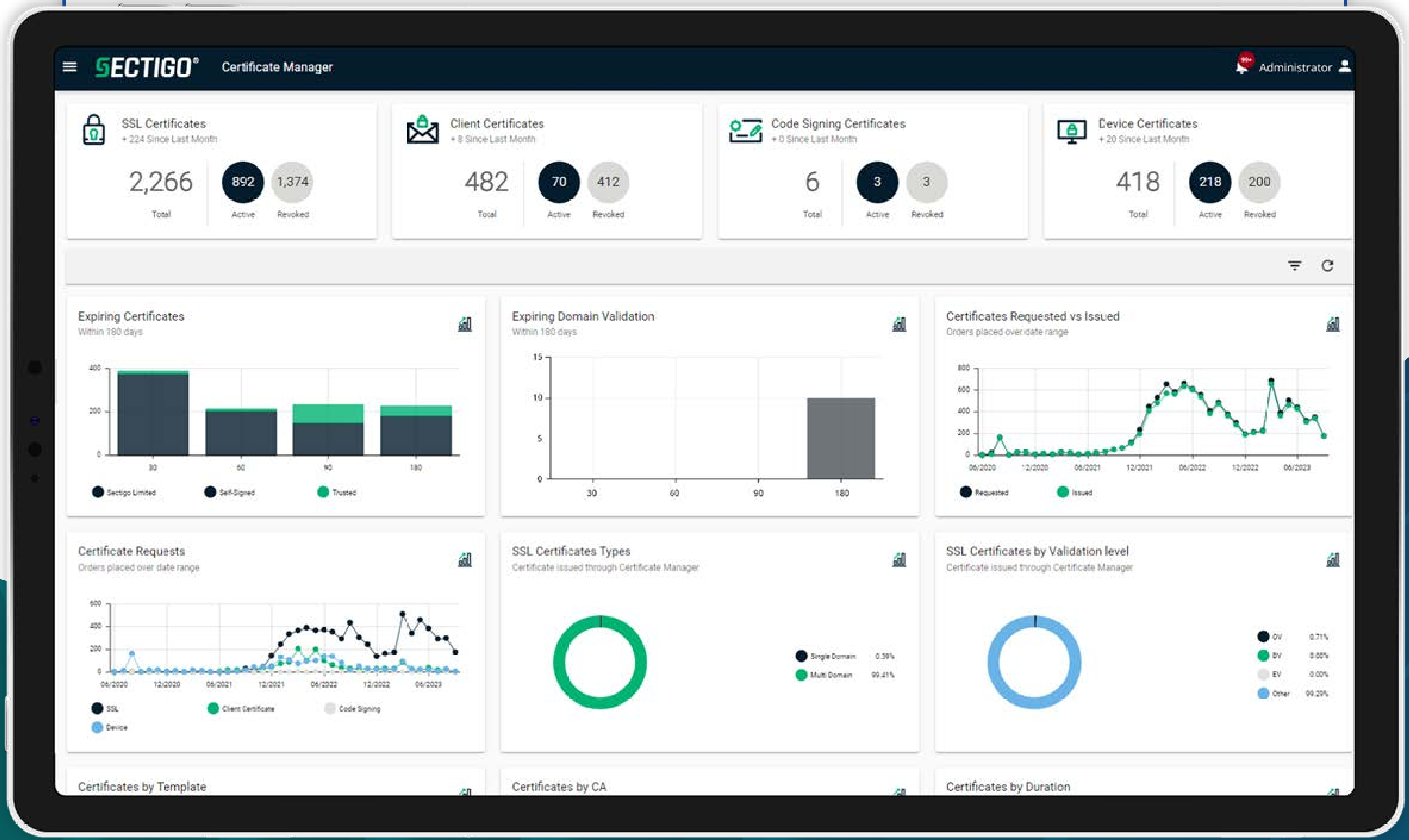
SCM is open and interoperable. At a time when IT teams are increasingly looking to consolidate the number of vendors in the tech-stack, SCM integrates with a broad set of technology vendors and can automate the issuance and management of Sectigo digital certificates, as well as those originating from other public and private CAs.

**Do you have some concerns about how your organization will manage the switch to 47-day TLS? Don't worry. Sectigo can help!**

## Sectigo offers **ACME automation** for all public certificates

**Want to see ACME certificate automation in action?**

Schedule a demo today, or find out more here:
[https://www.sectigo.com/47-day-ssl](https://www.sectigo.com/47-day-ssl)



# About SECTIGO®

Sectigo is the most innovative provider of certificate lifecycle management (CLM), delivering comprehensive solutions that secure human and machine identities for the world's largest brands. Sectigo's automated, cloud-native CLM platform issues and manages digital certificates across all certificate authorities (CAs) to simplify and improve security protocols within the enterprise. Sectigo is one of the largest, longest-standing, and most reputable CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust.

Talk to Us