SECTIGO®

90-Day TLS

An implementation guide

Introduction to short certificate lifespans

398 Days » **90** Days

In recent years the maximum term for a public TLS (also called SSL) certificate has dropped from three years to two to one.

On March, 3, 2023, Google's "Moving Forward, Together" roadmap laid out Google's intention to further reduce TLS certificate maximum validity from 398 to 90 days. Here Google notes: "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."

There is no specific timing announced for this change - but there's a very good chance 90-day validity periods will come into effect **by the end of 2024.**

This major change in policy has serious ramifications for organizations unable to automate the issuance and lifecycle management of digital certificates.

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 can help prevent cybercriminals from exploiting old certificates that are "left behind" as companies close their businesses, merge with other organizations, sell or otherwise transfer domain names, or rebrand their identities.

- The move to 90-day TLS will shorten the duration a compromised certificate could be exploited, which will bolster ecosystem integrity and reduce the risk of outages and breaches.

- 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.

It’s time to talk about **manual certificate management...**

Did you know that it can take a System Administrator upwards of **one hour** to configure and issue a single digital certificate?

The problem for IT teams is that, in reality, this isn’t about one certificate that must be dealt with four times per year, **it’s about dozens, hundreds, or thousands of digital certificates.**

Manual management is...

- Prone to human error, leading to expired or misconfigured certificates.
- Time-consuming.

It also...

- Prevents proactive monitoring.
- Increases the risk of service outages, security breaches, and non-compliance with industry standards and regulations.

In short, manually-managed digital certificates = vastly increased risk.

90-Day TLS marks the end of the manual management era

90-day TLS is a 77% reduction in maximum term.

This is a significant reduction and, in reality, means at least five times more work for those tasked with taking a manual approach to certificate lifecycle management. Thanks to 90-day TLS, we can, and should, expect drastically increased numbers of digital certificates when it comes into effect - at least five times as many as today.

Manual certificate management is already difficult and tedious. With 90-day TLS, it will become impossible.

- It requires careful planning.
- It involves managing multiple validations at any one time.
- It means issuing certificates to the right places with correct configurations.
- It is vital to set reminders for the expiry date of each certificate.

With a vastly increased number of digital certificates required to meet the standards of 90-day TLS, it's easy to see how IT teams carrying out manual certificate management are likely to become overwhelmed. This will drastically increase an organization's risk of outages and breaches.

Ultimately, when 90-day TLS comes into effect, manual management will no longer provide organizations with the solid foundation of digital trust that they need.

It’s time to automate!

Google's planned reduction to the lifespan of TLS certificates will have a direct impact on organizations unable to leverage automation to manage the lifecycles of vastly increased numbers of digital certificates. In fact, Google’s ‘Moving Forward, Together’ roadmap heavily promotes the use of automation to:

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

Automation plays a crucial role in ensuring the smooth implementation and upkeep of the 90-day TLS protocol. With the increasing reliance on secure communications, organizations need to swiftly and effectively manage the regular updates and certificate replacements required by 90-day TLS.

Only automation can streamline these processes, reducing human error and, minimizing downtime. By leveraging automation, IT teams can easily generate, deploy, and monitor all certificates, enabling seamless encryption and authentication across enterprise systems. Automation also allows for proactive monitoring and alerting, ensuring timely certificate renewals and preventing potential security vulnerabilities caused by expired or misconfigured certificates.

Now is the time to act.

To maintain digital trust, organizations must have a solution to automate the lifecycles of digital certificates, at scale, or risk downtime, outages, and breaches on a scale never seen before.

90-day TLS checklist

The time to prepare for 90-day certificate lifespans is now. To ensure your organization's preparedness, follow this checklist to ensure your ecosystem is prepared for 90-day TLS.

Discovery is a vital first step to preparing for 90-day TLS. With Sectigo Certificate Manager (SCM), organizations can easily:

- Find and display certificates originating from any vendor
- Discover SSL certificates installed on web servers and load balancers on both sides of the firewall
- Monitor certificates for expiration and set to automatically renew
- Identify rogue certificates and bring them under management control

Step 1

Carry out a full SSL/TLS certificate discovery exercise

With Sectigo Certificate Manager:

- Use SCM to scan your external public certificates
- Use SCM to scan your internal public certificates

Without Sectigo Certificate Manager:

- Run a Certificate Transparency log scan for public certificates at https://crt.sh/

or

- Use a third-party application such as Netcraft or Qualys to scan your external and internal public certificates

Step 2

Compile a vendor technology inventory

○ Compile a complete inventory of vendor technologies within your IT ecosystem that require SSL/TLS certificates to function. This list may be exhaustive, and/or only the most critical/urgent.

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

Technology	Application	IP	Certificate	Notes
Amazon	ACM	xxx.xxx.xxx.xxx	example.domain.com	Application hosting
Apache	Apache	xxx.xxx.xxx.xxx	example.domain.com	Promotion website
Kubernetes	Kubernetes	xxx.xxx.xxx.xxx	example.domain.com	Kubernetes for payments
F5	BIG-IP	xxx.xxx.xxx.xxx	example.domain.com	Load Balancer for Germany
Cisco	ASA	xxx.xxx.xxx.xxx	example.domain.com	SSL VPN access

Step 3

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

○ 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: 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

Step 4

Build a plan for the rollout of 90-day certificate issuance

- Set the objective, resources, requirements and priorities for the automation rollout
- Ensure you have all the required resources, software and systems in place for a successful rollout of 90-day TLS.

Click here for more details on the 90-day checklist.

SCM can prepare your organization for 90-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 90-day TLS? Don't worry. Sectigo can help!

Now, Sectigo is offering **FREE ACME AUTOMATION** for all public certificates*.

Want to see ACME Certificate Automation in action?

Schedule a demo today, or find out more here:

https://sectigo.com/90-day-certificates

*Terms and conditions apply, go to https://www.sectigo.com/90-day-certificates for details.

About SECTIGO®

Sectigo is a leading provider of automated Certificate Lifecycle Management (CLM) solutions and digital certificates - trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers.
For more information, visit www.sectigo.com.