stonetusker

Stonetusker Insights · Technical note on platform engineering and certificate management

Public Certificates Drop to 100 Days in March 2027: Check Every Renewal in 30 Minutes

From 15 March 2027 a public security certificate can last at most 100 days, and from 15 March 2029 at most 47 days. The main website usually renews by itself. The certificates that still need a person are where outages start.

For: Anyone with a public website, interface or device endpoint.

By Subeesh Sivanandan, Founder, Stonetusker Systems · Updated 29 October 2026 · About 3 minutes to read · PDF version

The short version

- Public Transport Layer Security (TLS) certificates can last at most 200 days today. The limit falls to 100 days on 15 March 2027 and to 47 days on 15 March 2029.[1]
- By 2029 the proof that you control a domain can be reused for only 10 days, so domain validation also has to run without a person.[1]
- Let's Encrypt moves faster: 64-day certificates by default from 10 February 2027 and 45-day certificates from 16 February 2028.[2,3]

- A search of the public Certificate Transparency logs lists every public certificate you own. Every certificate that still renews by hand is a future outage.

100 days
Maximum public certificate life from 15 March 2027[1]

47 days
Maximum public certificate life from 15 March 2029[1]

10 days
Domain validation reuse window from 2029[1]

A note to forward to your team

Certificate renewal check

Public certificates can last at most 100 days from 15 March 2027 and 47 days from 15 March 2029. Every certificate that still renews by hand becomes recurring work and a likely outage.

Please run the crt.sh search in this note for every domain we own by [date] and reply with three numbers:
1. Public certificates found that are still valid
2. Certificates that renew automatically
3. Certificates that need a person

Owner: [name]
Note: https://stonetusker.com/insights/100-day-tls-certificates.html

Why it matters now

In April 2025 the CA/Browser Forum, the body of certificate authorities and browser makers that sets the rules for public certificates, approved ballot SC-081v3.[1] The maximum lifetime fell from 398 to 200 days on 15 March 2026. It falls to 100 days on 15 March 2027, less than five months from now, and to 47 days on 15 March 2029.

At 47 days each certificate renews about eight times a year. A manual step that happened once a year becomes recurring work, and each renewal is a date that can be missed. With 200 certificates that need a person, at 30 minutes each, a team spends about 90 hours a year at 398-day lifetimes and close to 800 hours a year at 47 days.

The main website usually renews by itself. Outages come from the edges: certificates uploaded by hand to a load balancer or gateway, appliances, partner integrations that pin your certificate, mobile apps and devices, and certificate files baked into images.

Check your public certificates in 30 minutes

Step 1. List every public certificate

Every publicly trusted certificate appears in the public Certificate Transparency logs, and crt.sh offers a free search over them.[4] Replace `example.com` with your domain and repeat for every domain the business owns, including older brands and regional domains.

```
curl -s "https://crt.sh/?q=%25.example.com&output=json" \
  | jq -r '.[] | [.common_name, .issuer_name, .not_after] | @tsv' \
  | sort -u
```

The list also shows expired certificates. Keep the ones whose expiry date is still in the future.

Step 2. Check one endpoint directly

```
echo | openssl s_client -connect api.example.com:443 -servername
api.example.com 2>/dev/null \
  | openssl x509 -noout -issuer -enddate
```

Step 3. Mark how each one renews

Put the list in a spreadsheet and add one column: renews automatically, yes or no. Please be strict. A calendar reminder counts as no.

What the result means

What you find	What it means	Typical effort
Certificates from a managed service or an ACME client that renew by themselves	Ready for shorter lifetimes, if a separate system alerts on expiry	Add independent expiry monitoring
Certificates uploaded by hand to a load balancer, gateway or content delivery network	Each one becomes recurring manual work and a likely outage	Move each to automated renewal
Certificates pinned in apps, devices or partner configurations, or baked into images	Renewal also needs a release or a change by someone else	Engineering work and partner coordination for each one

The rows marked "no" form your project. ACME here means the Automated Certificate Management Environment protocol.

The move, step by step

1. **Build the inventory.** Pull every public certificate from the Certificate Transparency logs, add internal certificates, and record where each one is deployed and who owns it.
2. **Move to the ACME protocol.** Use cert-manager in Kubernetes, a standard client on hosts, or managed certificates from your cloud provider.
3. **Automate domain validation.** Validate through your domain name provider's interface with credentials limited to the validation records, and retire email approval.
4. **Monitor expiry separately.** Alert from a system that is separate from the renewal system when a certificate has less than a third of its lifetime left.
5. **Remove pinning and baked-in certificates.** Load certificates at run time, and replace leaf-certificate pinning in apps, devices and partner configurations.

Clients that support ACME Renewal Information (RFC 9773) let the certificate authority say when to renew, including early renewal after a mass revocation. Without it, Let's Encrypt recommends renewing at about two thirds of the lifetime.[3,6] Its staging environment has issued 64-day certificates since 14 October 2026, so you can test your automation against the shorter lifetime now.[3]

What is still open

- Some certificate authorities may adopt shorter lifetimes earlier than the ballot requires, as Let's Encrypt has. Please check the plans of the authorities you use.
- Support for ACME Renewal Information differs across clients, appliances and cloud services. Confirm it for each part of your estate.
- The renewal hours above are an illustration. Your figure depends on your certificate count and your current process.

Questions

When do 100-day certificates start?

On 15 March 2027. From that date publicly trusted certificates can be valid for at most 100 days. The limit falls to 47 days on 15 March 2029.

Does this apply to our internal certificate authority?

The ballot covers publicly trusted server certificates only, so internal certificates keep the lifetime you set.[[5]] They often cause the worst expiry incidents, so automate them with the same tools.

Can we still buy a one-year certificate?

Some certificate authorities sell multi-year subscriptions. Each certificate issued under one follows the maximum validity in force on the day of issue, so reissue and redeployment still follow the shorter cycle.

What is domain validation reuse?

It is the period for which a certificate authority can rely on an earlier check that you control a domain. It falls to 10 days in 2029, so domain validation also needs automation.

Want a second opinion?

Run the check yourself first. If you would like a second opinion, reply with two numbers only: the public certificates you found and how many of them renew automatically. No domain names, certificate details or command output are needed. Within five working days you receive a short written review with the likely risk areas, an automation approach and a time estimate. It is free and confidential, and a call is optional.

Ask for a second opinion

The button opens an email to subeesh@stonetusker.com with the subject and the numbers to fill in. You can also use the contact page, or reply to the email or LinkedIn message that brought you here.

Next page for your situation

- Delivery Deadline Radar: every other dated change, with a check for each.
- Checklist for ultra-scale teams: eight plain questions and the dates that matter.

Sources

1. DigiCert: TLS certificate lifetimes will officially reduce to 47 days
2. Let's Encrypt: Decreasing certificate lifetimes to 45 days
3. Let's Encrypt: 64-day certificate lifetimes coming February 2027 (7 October 2026)
4. crt.sh: Certificate Transparency search
5. Akeyless: 47-day certificates, what changes and how to prepare
6. Let's Encrypt: ACME Renewal Information

About the author

Subeesh Sivanandan is the Founder and CEO of Stonetusker Systems. He has worked for more than 27 years in release engineering, DevOps, platform engineering & embedded

Linux. His career includes serving as the Principal Engineer & Manager of Release Engineering at Stryker, alongside earlier roles at Nokia, VeriSign, and IP Infusion. LinkedIn profile.

Revision history (recent 3 updates)

Version 2.1, 29 October 2026. Every fact on this page is checked against a minimum of two sources each month.

Version	Date	Change
1.3	16 October 2026	Rewritten as an article for quick readers: introduction, summary of all major changes, what it means and first steps; one figure; commands folded for platform leads; print option and direct email offer
2.0	25 October 2026	Simpler layout and shorter text; the review offer now asks for a few counts only
2.1	29 October 2026	Who-this-is-for box, note to forward moved up, email offer with the numbers listed, and next pages