

Hi team,

The certificate industry is entering a transition that will significantly affect how we manage and secure our infrastructure.

In April 2025, the CA/Browser Forum approved [Ballot SC-081v3](#), which phases down publicly trusted SSL/TLS certificate lifespans from today's 398 days to just 47 days by 2029.

Here's the timeline:

- **March 15, 2026** → Maximum lifespan drops to **200 days**
- **March 15, 2027** → Drops again to **100 days**
- **March 15, 2029** → Final enforcement: **47-day certificates**

This is backed by Apple, Google, and leading Certificate Authorities like Sectigo, and will apply to all publicly trusted certificates.

Why the change?

The goal is to improve certificate hygiene and agility, making it harder for compromised certs to go unnoticed and limiting the damage from misuse or mismanagement. Simply put, shorter lifespans strengthen our overall security posture.

Implications for our current practices:

- **Manual renewal processes won't scale.**
We'll need to handle 12x more renewals than we do today by 2029.
- **Tracking spreadsheets and siloed teams will break down.**
Especially as certs expire faster and across more systems.
- **Legacy infrastructure and custom integrations may not keep up.**
It will risk uptime for apps, appliances, and services.



What's at risk if we're not prepared:

- **Outages** on websites, APIs, internal apps
- **Broken** authentication, email, or secure access
- **Compliance violations** or security events from expired or rogue certs

We'll be initiating discovery and planning in the coming weeks. No action needed from you yet. This message is to raise awareness of what's ahead.

Thanks,

[Your Name]

[Your Title]