SSL Certificates Every 47 Days

Plan of Action & Readiness Checklist

Internal reference document — self-hosted government infrastructure, certificates procured via Sectigo

Background

The CA/Browser Forum's Ballot SC-081v3 is phasing down the maximum validity of publicly trusted SSL/TLS certificates from 398 days to 47 days by March 2029. Certificates issued today are already capped at 200 days, dropping to 100 days in March 2027, and 47 days in March 2029. This document outlines our internal plan of action to move from manual, Sectigo-based certificate issuance to automated ACME-based renewal ahead of these deadlines.

Key Milestones

☐	March 15, 2026 — Max validity reduced to 200 days (in effect now)
☐	March 15, 2027 — Max validity reduced to 100 days
☐	March 15, 2029 — Max validity reduced to 47 days

Plan of Action

1. Inventory Everything Now

- List every domain and subdomain across our self-hosted infrastructure
- Identify which certificates are currently issued through Sectigo
- Note validation level for each (DV, OV, or EV) and expiry dates
- Flag any certificates not centrally tracked

2. Flag Manual Renewal Processes

- Identify servers where certificates are requested and installed manually
- Rank these by public-facing risk and traffic volume
- Treat manual-renewal sites as highest priority for automation

3. Confirm Sectigo ACME Support

- Verify our Sectigo account's ACME endpoint and API access
- Confirm wildcard and OV/EV certificate issuance is supported via ACME
- Coordinate with Sectigo account team on enterprise/volume terms

4. Pilot Automation on One Server

- Select a single, low-risk server for the initial ACME pilot
- Install and configure an ACME client (Certbot, acme.sh, or win-acme)
- Test DNS-01 validation for wildcard and firewalled servers
- Confirm automatic renewal and web server reload work end-to-end

5. Set Internal Deadlines Ahead of CA/Browser Forum Milestones

- Target internal completion at least 60–90 days ahead of each public deadline
- Build in extra buffer for government change-control and approval cycles
- Schedule formal testing and sign-off windows before each phase

6. Scale Automation Org-Wide

- Roll out ACME clients across all self-hosted servers in priority order
- Centralize certificate monitoring and expiry alerting
- Document the process for IT staff onboarding and audits

Cost Considerations

Estimates only — actual costs depend on server count, existing tooling, and Sectigo account terms.

☐	Wildcard SSL certificate (Sectigo, DV/OV/EV): $100–$300+ per year, per domain
☐	ACME automation tooling/platform (up to 2,000 sites): $5,000–$25,000+ per year
☐	Monitoring and alerting tooling: $2,000–$10,000+ per year
☐	Internal engineering/IT implementation time: varies by team capacity

Readiness Checklist Summary

☐	Full certificate inventory completed
☐	Manual-renewal servers identified and prioritized
☐	Sectigo ACME endpoint access confirmed
☐	Pilot server automated and validated
☐	Internal deadlines set ahead of 2027 and 2029 milestones
☐	Change-control/testing process defined for rollout
☐	Org-wide ACME rollout scheduled
☐	Monitoring and alerting in place as a safety net

Prepared for internal distribution — ZeeroTrust / Government Infrastructure Team