SSL | Powering Trust in Business

The 47-Day Readiness Toolkit

Four steps to automated certificates before the next lifetime cut

Guide

How to Use This Toolkit

Publicly trusted TLS certificates are getting shorter on a published schedule. The CA/Browser Forum set it in ballot SC-081v3, and it applies to every certificate authority. The first reduction is already in force. This toolkit takes you from where you are today to renewals that run without anyone watching, in four steps that each end with something you can show.

The three files

The kit is three files. What you only read stays in this guide. What you fill in or send lives in a file you can edit.

File & Description	Use It to
Guide *(this file)* The four steps and the appendix, with the reference material and checklists for each.	Decide what to do and in what order.
Workbook An Excel workbook, "SSL 47-Day Readiness Toolkit - Workbook," with eight working sheets: the summary, the discovery log, the inventory, the DNS mapping, the RACI, the project plan, the renewal proof, and the policy check.	Record what you find, see what it means for you, name owners, and track the plan.
Templates A Word file, "SSL 47-Day Readiness Toolkit - Templates," with six templates: the organizational email, the executive summary, the recommendation memo, the kickoff email, the weekly status update, and the CCoE charter.	Copy, personalize the bracketed fields, and send.

The schedule

Effective date	Maximum certificate lifetime	Maximum domain validation reuse	Renewals per certificate per year	Renewals across 1,000 certificates
Before March 15, 2026	398 days	398 days	about one	about 920 a year (2.5 a day)
March 15, 2026 (in force now)	**200 days**	**200 days**	**about two**	**about 1,800 a year (5 a day)**
March 15, 2027	100 days	100 days	about four	about 3,650 a year (10 a day)
March 15, 2029	47 days	10 days	about eight	about 7,800 a year (21 a day)

To scale the schedule, divide your own certificate count by the lifetime in days: that is your renewals per day. The figures assume each certificate renews once, at the end of its life. Automation usually renews with about a third of the lifetime left, so plan on about 1.5 times these numbers: roughly 32 a day for every 1,000 certificates at 47 days.

The limit applies on the day a certificate is issued. A certificate keeps the lifetime it was issued with, so one issued on March 14, 2027 can last 200 days. The Baseline Requirements also say CAs should stay one day under each limit (199, 99 and 46 days), so plan on those.

Step 0: Know your number

Before Step 1, count the publicly trusted certificates your organization holds. Every figure in this toolkit scales from that one number: the renewals a day in the schedule above, the workload and cost on the workbook's Summary sheet, and the ask in the executive summary. Start with an estimate from your CA accounts and a Certificate Transparency search of your domains (see the Discovery Guide in Step 2), enter it on the Summary sheet, and replace it with the real count once the inventory is built.

Then brief leadership before you build anything. The Summary sheet writes the executive summary text from your estimate; use the executive summary and recommendation templates in the Templates file to secure a sponsor and budget.

What you will have at the end of each step

Step 1. **Automate What You Can Today.** ACME running on every system that can support it, and the internal teams who own those systems informed of what is changing. Assets: ACME First Cheat Sheet and Automation Datasheet in this guide; Organizational Email Template in the Templates file.

Step 2. **Inventory Everything, Then See What Is Left.** A complete inventory of your publicly trusted certificates, with the ones that still renew by hand marked, each with an owner and a validation method. Assets: Discovery Guide in this guide; the Discovery Log, Inventory and DNS sheets in the Workbook.

Step 3. **Solve Validation, Not Just Issuance.** Every domain on a validation method that can run unattended, and a plan for the shrinking validation reuse window. Asset: DCV Automation Checklist in this guide.

Step 4. **Assign Ownership and Prove It Runs.** A named owner for each task, a dated plan, and one full renewal cycle that completed with nobody touching it. Assets: Readiness RACI, Readiness Project Plan and Unattended Renewal Proof in the Workbook; Internal Communications Toolkit in the Templates file.

Appendix. Governance Templates. A charter for the group that owns cryptographic policy, and a checklist to review it against. Assets: CCoE Charter Template in the Templates file; Cryptographic Policy Review Checklist in this guide and the Policy Check sheet in the Workbook.

Questions about this toolkit? Your SSL account team can help, or sales@ssl.com if you do not have an account yet.

Step 1. Automate What You Can Today

Much of your estate can probably renew through ACME already. ACME, the open protocol defined in RFC 8555, issues and renews certificates without anyone filing a request. Turning it on first is the fastest way to shrink the list of certificates a shorter lifetime can threaten.

ACME First Cheat Sheet

A quick reference for deciding what should automate through ACME now and what needs a different path.

What ACME is

ACME (RFC 8555) is the published protocol behind automated certificate issuance and renewal. SSL's ACME service works with ACME clients including Certbot, acme.sh, simple-acme, Caddy, Traefik, and cert-manager for Kubernetes. Each client registers with ACME account credentials (external account binding) that you create in your SSL account, so a stock client needs that one-time setup before it can issue. Check your platform's own documentation for built-in ACME support before assuming you need new software.

With SSL, ACME covers domain-validated (DV) certificates today. OV and EV certificates are ordered through the portal or the REST API, and SSL lists ACME for them as coming soon. No SSL account yet? Registering is free, and nothing is charged until you order a certificate.

Where ACME fits

Good fit for ACME now	Needs a different path
Web servers you control end to end, such as nginx, Apache, and IIS	Devices behind a mobile device manager, which route through SCEP and a private CA
Load balancers and reverse proxies with ACME support	Legacy hardware and appliances that cannot run a client or accept automated challenges
Container platforms and Kubernetes ingress controllers	OV or EV certificates, if your CA does not offer them over ACME yet (SSL does not yet)
Any internet-facing host that needs only domain validation	Workloads that need an isolated, dedicated CA hierarchy for compliance, which route to Private PKI

Worked example: Certbot with SSL's ACME service

Create the credentials once: in your SSL account, open the Dashboard, choose api credentials under Developers and Integration, and copy the Account/ACME Key and the HMAC Key. Then request a certificate for a site that answers on port 80:

```
certbot certonly --webroot -w /var/www/html -d www.example.com \
  --server https://acme.ssl.com/sslcom-dv-ecc --agree-tos --email you@example.com \
  --eab-kid ACCOUNT-KEY --eab-hmac-key HMAC-KEY
```

Certbot 2 and later issues ECDSA by default; for RSA, use sslcom-dv-rsa and add --key-type rsa. Later runs can omit the credential options. Certbot renews 30 days before expiry, so for 47-day certificates set renew_before_expiry = 15 days in the certificate's file in /etc/letsencrypt/renewal/ and run certbot renew --dry-run.

Which client for which platform

SSL's ACME service requires external account binding, so pick a client that accepts it. Each client in this table documents that support, including where to enter the credentials.

Platform	ACME client	External account binding	Where to read more
Apache HTTP Server	mod_md (built in), or Certbot	Yes. Apache HTTP Server 2.4.52 or later supports it (MDExternalAccountBinding)	https://httpd.apache.org/docs/2.4/mod/mod_md.html
nginx and other Linux hosts	Certbot, or acme.sh	Yes	Certbot and acme.sh documentation
Microsoft IIS and Windows	simple-acme (formerly win-acme)	Yes	https://simple-acme.com/manual/account-management
Kubernetes	cert-manager	Yes	https://cert-manager.io/docs/configuration/acme/
Container reverse proxies	Traefik, or Caddy	Yes	https://doc.traefik.io/traefik/reference/install-configuration/tls/certificate-resolvers/acme/ and the Caddy documentation
Go applications	lego	Yes	lego documentation
Infrastructure as code	Terraform ACME provider	Yes	Terraform ACME provider documentation

This table lists clients whose own documentation confirms external account binding. It does not cover every platform, and it is not a compatibility guarantee: confirm the exact setup with SSL before you roll it out.

Three-question decision check

First ask whether the certificate needs to be publicly trusted at all. If it only serves internal systems, it can move to a private CA and leave the 47-day schedule entirely, provided every device and browser that connects trusts your private root. Note it now; you will mark it "N" in the Step 2 inventory. See Private PKI in the Automation Datasheet. If it does need public trust, ask:

1. Can this system run, or call, an ACME client or agent?
2. Is it a DV certificate, or does your CA offer ACME for the validation level you need?
3. Can it complete a DNS or HTTP challenge with no human involved?

Three yeses mean you can automate it through ACME now. A no on any of them points to one of the other paths in the Automation Datasheet.

Automation Datasheet

SSL's automation and infrastructure options at a glance. Use it to pick the right path for each system. Feature availability, limits and integration requirements vary by account tier, so confirm the specifics with SSL before you finalize a rollout plan.

Capability	What it does	Best for
ACME	Automated certificate issuance and renewal over the open RFC 8555 protocol	Web servers, load balancers, containers, and Kubernetes ingress: anything you control end to end
SCEP	Automated enrollment for devices provisioned through a mobile device manager. SSL offers it through Private PKI and Managed PKI, so the certificates are private and outside the 47-day schedule	Mobile and managed-device fleets
REST API	Programmatic certificate ordering and management for custom integrations	Teams building their own automation on top of SSL
SSL Manager	A free Windows desktop application for ordering, installing, and renewing SSL certificates and viewing them with their expiry dates	Small to medium fleets and teams without command-line experience. It is not a fully automated lifecycle management tool
Certificate lifecycle management (CLM) platforms	SSL integrates with enterprise CLM platforms such as Venafi TPP and Keyfactor Command for centralized discovery and renewal	Large or multi-business-unit fleets
Managed PKI Certificates	A shared private CA service enrolling over SCEP, EST, ACME and REST API. Its certificates are private, so they sit outside the 47-day schedule. In early access: request access through SSL	Internal and device certificates at volume
Private PKI (for example Private Compliance PKI)	Dedicated private CA hierarchies for internal certificates that do not need public trust, so they sit outside the schedule. Private Compliance PKI is WebTrust-audited, with dedicated partitions in SSL's HSMs; other private tiers do not carry the WebTrust audit	Regulated environments and high-assurance internal use
Custom-Branded CA	A publicly trusted issuing CA, chained to SSL's root, that carries your organization's name. Its certificates follow the same lifetime schedule as every other publicly trusted certificate	Enterprises that want publicly trusted certificates issued under their own name

Organizational Email Template. Send it before you start any automation work. It puts the schedule, the reason, and the risk in front of every team that owns a certificate before your project needs anything from them. Open it in the Templates file.

Step 2. Inventory Everything, Then See What Is Left

Automation only helps with the certificates you know about. This step builds the complete inventory of your publicly trusted certificates, so the ones automation has not reached stand out: legacy hardware, embedded devices, manually validated domains, and nonstandard subject alternative names.

Discovery Guide

Start from the outside in. The certificate you do not know about is the one that expires. Work through these sources, log each one on the Discovery Log sheet, and add every certificate you find to the inventory. Include publicly trusted certificates only. Internal certificates are not covered by the schedule, and the inventory flags which of yours need public trust at all.

1. **Search Certificate Transparency logs for your domains.** Almost every publicly trusted certificate appears in these public logs, because the major browsers require it, whichever CA issued it, so a search by domain lists certificates you did not know existed. Cert Spotter, from SSLMate, offers a free domain search at https://sslmate.com/ct_search_api/ and others exist. Search every domain you own, with subdomains.

2. **Export the issued list from every CA and reseller account.** Include old accounts and accounts opened by single teams or contractors.

3. **List certificates in your cloud accounts.** Each major cloud has its own certificate and key service. In AWS, list the AWS Certificate Manager certificates and any older IAM server certificates (aws acm list-certificates and aws iam list-server-certificates). In Azure, list the certificates in each Key Vault (az keyvault certificate list). In Google Cloud, list Certificate Manager and load balancer certificates (gcloud certificate-manager certificates list and gcloud compute ssl-certificates list). Repeat for every account, subscription and project.

4. **Check load balancers, CDNs and gateways.** Certificates installed there often come from a CA account nobody remembers. Open the certificate list in each load balancer, CDN and API gateway console, and note which certificates the platform renews for you and which ones someone uploaded.

5. **List certificates in your Kubernetes clusters.** Look for certificate resources and TLS secrets in every cluster and namespace. Where cert-manager is installed, kubectl get certificates --all-namespaces lists the certificate resources. kubectl get secrets --all-namespaces --field-selector type=kubernetes.io/tls lists every TLS secret, including certificates someone created by hand.

6. **Scan your public address ranges.** A scan of your external IP ranges on common TLS ports finds certificates on systems nobody has documented. Start with ports 443 and 8443, then add the ports your mail, directory and VPN services use (465, 636, 993 and 995 are common). The nmap ssl-cert script reads the certificate on each open port. Scan only ranges you own. A scan by address misses a service that answers only to a hostname, which is why the next check matters.

7. **Cross-check against your asset database and DNS zones.** Every hostname that should serve TLS should appear in the inventory. The ones that do not are your gaps.

8. **If you are an SSL customer, add what SSL Manager knows.** SSL Manager is SSL's free Windows desktop application. It lists the certificates ordered through your SSL account with their expiry dates. It needs an SSL account to run, does not scan your network, and sees only that account.

9. **Use a CLM platform for large fleets.** If sorting by hand is not practical because you have a large fleet, several business units, or third-party integrations, SSL integrates with enterprise CLM platforms such as Venafi TPP and Keyfactor Command to centralize discovery and renewal. For fleets that renew often, SSL recommends ACME automation instead of, or alongside, SSL Manager.

By the end of this step you have an inventory of every publicly trusted certificate you can find, with the ones that renew by hand marked. That inventory is the input to Step 3.

Inventory Workbook

The companion workbook, "SSL 47-Day Readiness Toolkit - Workbook," is the working record for Steps 2 to 4 and the appendix. For Steps 2 and 3 it has four sheets. Fill in the tinted rows as you go. Add rows as needed, because the format does not change.

Sheet	Use it to
STEP 2 Discovery Log	Record each source you searched and how many certificates it produced.
STEP 2-3 Inventory	One row per publicly trusted certificate. The columns cover what and who (Certificate / Domain, System / Vendor, Owner, Issuing CA), risk (Needs public trust, Business criticality, Certificate expires, Days left), how it renews (Current renewal method, Automated today, Current DCV method, DCV reuse expiry, Key type), and the Step 3 plan (Target path, Blocking issue, Target date). Priority marks what to fix first.
STEP 3 DNS Auto. Mapping	Confirm your DNS provider and CAA setup for anything routed to ACME through DNS validation.
Summary	Reads the inventory and shows your certificate count, percent automated, renewals a day for each lifetime, and the effort and cost behind the executive summary.

Step 3. Solve Validation, Not Just Issuance

Shorter lifetimes get the attention, but a second schedule matters as much. Before a certificate authority issues a certificate for your domain, it confirms that you control the domain. The rules limit how long an earlier confirmation can be reused, and that reuse window shrinks on the same dates as certificate lifetimes. By March 15, 2029 it is 10 days.

Effective date	Domain validation can be reused for	What it means for you
Before March 15, 2026	398 days	One validation could support a full year of renewals
March 15, 2026 to March 14, 2027	200 days	Validation needs to be refreshed about twice a year
March 15, 2027	100 days	Validation needs to be refreshed about four times a year
March 15, 2029	10 days	A validation older than 10 days cannot support issuance, so nearly every issuance needs a fresh one

The validation reuse schedule

Validation now follows its own schedule, separate from certificate lifetime. Teams that automate issuance often find that validation is still manual, and at a 10-day reuse window a method that needs a person becomes the bottleneck. This step makes validation as automatic as issuance.

OV and EV certificates also reuse organization validation. That period fell to 398 days on March 15, 2026 and does not shorten again under the current Baseline Requirements. The reuse figures in this guide are for proving you control the domain.

DCV Automation Checklist

Domain control validation (DCV) is the check that you control a domain. Work through this before you rely on automation in production.

Know your method

- ☐ Confirm which DCV method each domain uses today: DNS-based, HTTP-based, or email-based. Record it in the Step 2 inventory.
- ☐ Move every domain off email-based validation. The Baseline Requirements already bar validation by email, fax, SMS or post to a domain contact (since July 15, 2025). The remaining email methods (constructed email, email to the DNS CAA contact, email to the DNS TXT contact) stop on March 15, 2028. Email also cannot run unattended.
- ☐ Record when each domain's validation expires, using the reuse window in force today, so you can see which domains need revalidation first. The inventory workbook has a column for it.

Reuse and timing

- ☐ Confirm your automation revalidates a domain by itself when the reuse window runs out, instead of relying on an earlier approval.
- ☐ Plan now for the March 15, 2027 reuse window (100 days) and the March 15, 2029 reuse window (10 days). Each one raises how often you revalidate without changing any certificate's lifetime.
- ☐ Confirm your renewal schedule suits a 47-day certificate. A client set to renew a set number of days before expiry works as long as that number is well under 47. The common 30-day setting renews at about day 17, which is about 2.8 times the workload in the schedule (about 59 renewals a day for every 1,000 certificates). A setting near a third of the lifetime, about 15 days, matches the planning figure of 32 a day. A job that runs on a fixed interval, such as every 60 days, misses it.

DNS-based validation

- ☐ Confirm your DNS provider supports automated record creation through an API. Unattended renewal requires it.
- ☐ If you publish CAA records, confirm they name your issuing CA. A CAA record that names a different CA blocks issuance. With no CAA record at all, any CA may issue.
- ☐ Confirm the credential your automation uses to change DNS records has a named owner and is limited to the records validation needs.
- ☐ If your DNS zone is signed with DNSSEC, confirm it validates. Since March 15, 2026 CAs must check DNSSEC on validation and CAA lookups, and a validation error stops issuance.

HTTP-based validation

- ☐ Confirm your automation can write the challenge file to the expected path without a manual deployment step.
- ☐ Confirm the challenge path is reachable over plain HTTP from the public internet. Authentication or an IP allow-list in front of it will fail validation, and any redirect needs to end at a path the validator can reach.
- ☐ Confirm the challenge answers from outside your own country and network. CAs now check domain control from several network locations around the world before issuing (Baseline Requirements 3.2.2.9, required since March 15, 2025), so geo-blocking, country allow-lists and DNS that answers different resolvers differently can fail even when the challenge works from your desk.
- ☐ Use DNS-based validation for wildcard certificates, because HTTP-based validation cannot issue them.

Before you rely on it in production

- ☐ Run one full unattended renewal cycle end to end and confirm it replaces the certificate in use, not just that it issued.
- ☐ Set alerting on failed renewal and failed validation attempts, not only on expiry. A silent automation failure is worse than a manual process, because nobody is watching for it.
- ☐ Test the failure path: break the challenge on a non-production system and confirm your alert reaches a person.
- ☐ Document a fallback manual-issuance path for anything that cannot be automated yet, so a failure does not turn into an outage while it is fixed.

Use it: Workbook, sheets STEP 2-3 Inventory (the Current DCV method and DCV reuse expiry columns) and STEP 3 DNS Auto. Mapping.

Step 4. Assign Ownership and Prove It Runs

A shift this size does not survive being one person's job. Give the plan a calendar and a name on every line, then prove it with a renewal that nobody touched.

Readiness RACI

R = Responsible **A** = Accountable **C** = Consulted **I** = Informed

Use it: Workbook, sheet STEP 4 RACI. It starts with 15 tasks and a row for the names, and checks that each row has one A.

Readiness Project Plan

A schedule template for the work in Steps 0 to 4 and the appendix. Enter a start date and the dates and timeline fill in. Personalize the owners and durations, then track progress in the Status column.

Key dates to plan against. The 200-day maximum has applied since March 15, 2026. The maximum becomes 100 days on March 15, 2027 and 47 days on March 15, 2029 (CA/Browser Forum ballot SC-081v3). Domain validation reuse follows the same dates and reaches 10 days on March 15, 2029.

Use it: Workbook, sheet STEP 4 Project Plan. It starts with 15 tasks, draws the timeline, and counts the days left to each cut.

Internal Communications Toolkit

Four templates to get a readiness project off the ground and keep it moving: an executive summary, a recommendation memo, a kickoff email, and a weekly status update. Use the first three in order and send the fourth every week.

Use it: Templates file, Internal Communications Toolkit.

Unattended Renewal Proof

The proof that Step 4 is finished is one renewal that completed with nobody touching it. Record it in the workbook and keep it with your project plan.

You cannot wait a full 47 days to find out the plan works. Run your client's early or forced renewal on a non-production system to exercise the whole path (challenge, issue, install, reload). Then break the challenge on purpose and confirm the failed-renewal alert reaches a person. Record both in the workbook.

Use it: Workbook, sheet STEP 4 Renewal Proof.

Appendix. Governance Templates

These two templates are for organizations that already have, or are building, a group that owns cryptographic policy. They are useful after Steps 1 to 4, and nothing in those steps depends on them.

CCoE Charter Template

A starting charter for a small, cross-functional Crypto Center of Excellence (CCoE), the group that keeps your organization ahead of the next lifetime cut instead of reacting to it.

Use it: Templates file, CCoE Charter Template.

Cryptographic Policy Review Checklist

Bring this to your CCoE or executive briefing to confirm your organization is aligned on certificate automation, crypto-agility, and the next scheduled reduction.

Automation coverage

- ☐ We know what percentage of our certificate estate renews automatically today.
- ☐ We have a named owner for every certificate that still renews manually.
- ☐ We have tested a full unattended renewal cycle for our automated systems, not just confirmed issuance.

Validation

- ☐ We know which domain validation method each domain uses and when each validation expires.
- ☐ Our automation revalidates domains on its own when the reuse window runs out.
- ☐ We have reviewed our validation methods against the next scheduled reduction in reuse.

Policy and standards

- ☐ We have a documented policy for which automation path (ACME, SCEP, Managed PKI, Private PKI) applies to which system type.
- ☐ We have a documented exception process for systems that cannot automate yet, with a review date.
- ☐ Our key-length and algorithm standards are current and do not assume lifetimes that no longer apply.

Crypto-agility and readiness

- ☐ We have assessed our post-quantum readiness, or have a plan and date to do so.
- ☐ We have a standing group (a CCoE or equivalent) responsible for cryptographic policy, not an ad hoc owner.
- ☐ We have reviewed this checklist since the last CA/Browser Forum ballot that affected certificate lifetimes.

Next reductions to plan against

The 200-day maximum has applied since March 15, 2026. The maximum becomes 100 days on March 15, 2027 and 47 days on March 15, 2029. Domain validation reuse is 200 days now, 100 days from March 15, 2027, and 10 days from March 15, 2029 (CA/Browser Forum ballot SC-081v3).

Use it: Workbook, sheet APPENDIX Policy Check. Answer Yes or No for each statement and read the score.