AUSTRALIAN GOVERNMENT · TLS CERTIFICATE MANAGEMENT

The End of Manual Certificate Management

Industry changes, government impact, and the path forward

What TLS Certificates Do — and Why Browsers Control Everything

THE BASICS

A TLS certificate binds a **public cryptographic key** to a domain name. When your browser connects to a government website, it checks the certificate to confirm the site is genuine before allowing the connection.

Without a valid certificate, modern browsers display a **full-page security warning** — blocking citizens from accessing services entirely.

WHO CONTROLS TRUST

Certificate Authorities (CAs) issue certificates after verifying domain ownership

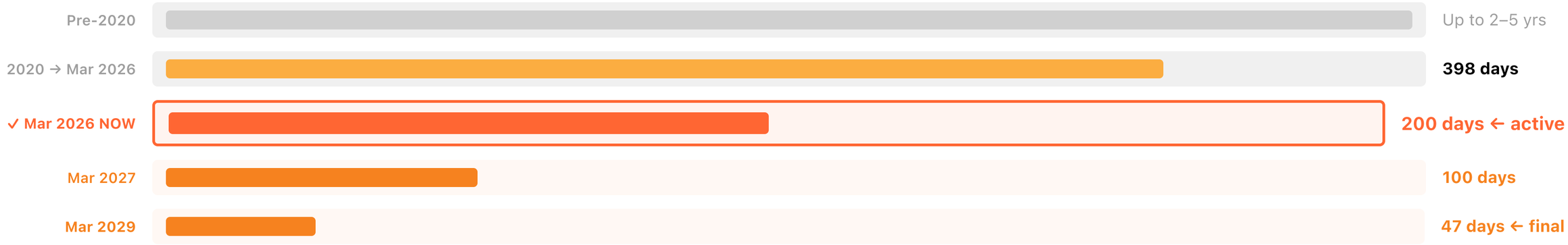
Browser Root Programs decide which CAs to trust — and set the rules CAs must follow

Google Chrome holds ~68% global browser share — its Root Program is the de facto policy setter for the entire web

If Google changes a rule in its Chrome Root Program, every CA in the world must comply — or their certificates stop working in Chrome.

The Ratified Schedule: Certificate Lifetimes Are Already Shrinking

CABForum Ballot SC081v3 passed 11 April 2025. This is binding industry policy — not a proposal. The first reduction took effect **15 March 2026.**



Apple proposed 47 days. Google voted yes immediately. The 200-day limit is already in force. Domain validation reuse also drops to 10 days by 2029 — making manual renewal operationally impossible well before the final deadline.

PART ONE

The Industry Shift

How We Got Here: Apple Proposed 47 Days — Google Voted Yes

CABFORUM BALLOT SC081V3 — PASSED 11 APRIL 2025

Final Maximum Certificate Validity

47 days — effective March 2029. Apple proposed it; Google voted in favour immediately.

Domain Validation Reuse

10 days by March 2029 — manual revalidation at this cadence is operationally impossible

Already In Force

The **200-day limit took effect 15 March 2026** — two months ago. This is not a future problem.

WHY THIS CANNOT BE REVERSED

This is a **ratified CABForum Baseline Requirement** — binding on every Certificate Authority that wants to remain trusted by browsers. It is not a proposal. It cannot be voted down.

Chrome = ~68% of global browser traffic

CAs that don't comply are removed from Chrome's trust store — their certificates stop working for the majority of internet users worldwide, including Australian citizens.

Why 47 days? It's one calendar month (31 days) plus a half-month buffer (15 days) plus one day of wiggle room. At this lifetime, automation is not optional — it is the only viable operating model.

The Security Case for Shorter Certificates

Google's rationale is technically sound — understanding it helps explain why this change is permanent, not reversible.

Limit Key Compromise Exposure

If a private key is stolen, the attacker can impersonate the site until the cert expires. A 398-day cert = up to 13 months of exposure. A 47-day cert = 47 days maximum — a 90% reduction in risk window.

Make Revocation Irrelevant

The web's revocation infrastructure (OCSP/CRL) is notoriously unreliable — browsers often soft-fail checks for performance reasons. Short-lived certs expire before revocation matters.

Force Automation as Standard

Manual renewal at 47-day intervals — across hundreds of systems — is operationally impossible. This is a deliberate forcing function to drive adoption of the ACME protocol and eliminate human error from the renewal process.

Post-Quantum Cryptographic Agility

Shorter cert lifetimes mean the ecosystem can rotate to new cryptographic algorithms faster — critical as quantum computing threatens current RSA and ECDSA key types.

Industry Momentum: This Is Not a Proposal — It's a Direction

WHERE THE INDUSTRY IS ALREADY MOVING

Let's Encrypt — already at 90 days, now offering 6 days

The world's largest CA by issuance volume issues 90-day certs by default. 6-day certificates became generally available in January 2026 — well ahead of the CABForum schedule.

Cloudflare — automated renewal at scale

Manages certificates for millions of domains automatically. No manual intervention required.

GCP, Azure — ACME-native; AWS — automation-first

Major cloud providers have built automation-first certificate management. GCP and Azure support ACME natively; AWS uses its own automated validation workflow. The enterprise world is already there.

THE GAP FOR GOVERNMENT

⚠ The automation-first world assumes modern infrastructure

- ✕ Legacy load balancers and appliances don't support ACME
- ✕ Government procurement cycles run 6–18 months — already longer than the current 200-day window
- ✕ Change Advisory Boards (CABs) weren't designed for renewals every 47 days
- ✕ Certificate inventories are often undocumented across agencies

PART TWO

The Government Impact

The Operational Reality for Australian Government

CURRENT STATE

Most agencies renew certificates **manually, once per year** — often triggered by an expiry alert or an outage

Legacy infrastructure — F5 load balancers, Cisco appliances, on-prem WAFs — requires **manual certificate uploads**

Certificate inventories are **often undocumented** — agencies don't know how many certs they have or when they expire

THE 90-DAY PROBLEM

4×
renewals per domain per year

×100s
of systems per agency

Government procurement and change management cycles run **6–18 months** — longer than the cert validity window itself.

ASD ISM certificate management controls require documented processes and timely renewal — manual workflows at a 47-day cadence (by 2029) create measurable compliance risk starting now.

What Happens When Government Certificates Expire

Citizens Blocked

Chrome, Edge, and Safari display a full-page security warning. Most citizens will not proceed — they cannot access the service.

System Integrations Break

Inter-agency API calls, federated identity (myGovID), and shared services connections fail silently or loudly — often cascading across multiple systems.

Reputational Damage

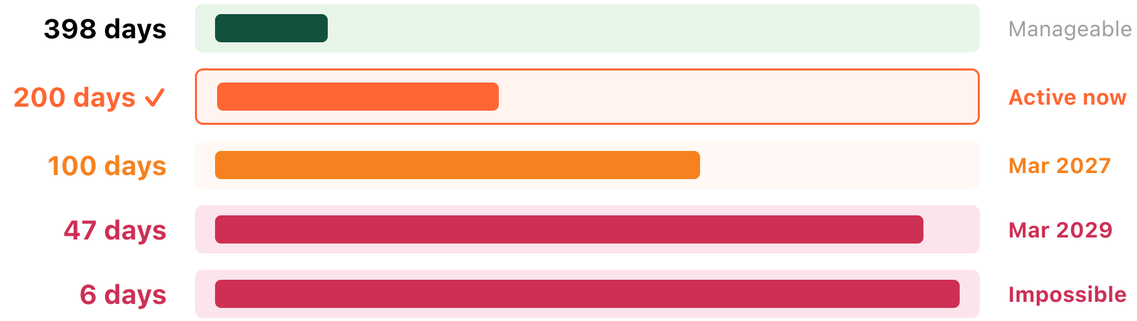
Government website outages from expired certs are publicly visible and frequently reported. They undermine citizen trust in digital government services.

Real-World Precedent

The US federal government experienced multiple certificate expiry outages during the 2019 government shutdown — furloughed staff couldn't manually renew certificates, and services went dark. It was a direct consequence of relying on manual processes. Australian agencies face the same structural risk.

The Manual Management Breaking Point

RENEWAL EFFORT AT EACH VALIDITY PERIOD



THE GOVERNMENT-SPECIFIC GAP

ACME Protocol = The Industry Answer

ACME automates domain validation and cert issuance. Let's Encrypt, GCP, Azure, and Cloudflare support it natively. But it requires modern infrastructure.

Legacy Systems Don't Speak ACME

F5 BIG-IP, older Cisco ASA, on-prem IIS, and many government appliances have no ACME client. Upgrading them requires procurement, testing, and CAB approval.

Process Cadence Mismatch

Government change management processes — CAB meetings, risk sign-off, testing windows — were designed for annual cert renewals, not quarterly ones.

Cloudflare vs. DIY ACME Automation

Both approaches address the shrinking certificate lifetime mandate — but the path to get there is very different.

Capability	DIY ACME Automation	Cloudflare
Legacy system support	Requires ACME client on every system	**Cloudflare proxies — origin unchanged**
Operational overhead	Engineering effort per system	**Centralised, zero-touch**
Failure blast radius	Per-system cert expiry risk	**Edge handles renewal; origin decoupled**
Time to implement	Months (procurement + change mgmt)	**Days to proxy; immediate edge protection**
Audit trail / visibility	Custom tooling required	**Dashboard + CT Monitoring built-in**
ISM/IRAP alignment	Depends on implementation	**IRAP assessed (contact us for scope)**

PART THREE

How Cloudflare Helps

How Cloudflare Insulates You From This Problem

Three layers of capability — deployable independently, in any order, without replacing existing infrastructure.

1 Edge Certificates

Cloudflare issues and auto-renews all publicly-trusted certificates. Your origin server never needs a public cert renewed again.

What this means for government

Citizens always see a valid cert. Legacy origin systems are completely decoupled from the shrinking renewal cycle — whether 200 days, 47 days, or less.

2 Origin CA Certificates

Cloudflare issues 15-year origin certificates trusted only between Cloudflare and your origin. Not publicly trusted — not subject to browser policy.

What this means for government

Legacy appliances get long-lived internal certs. No ACME required. No procurement cycle. No CAB approval for renewals.

3 Advanced Certificate Manager

For agencies needing custom CA chains or bring-your-own-certificate workflows. Cloudflare's API Shield provides separate mTLS client certificate authentication for API and service-to-service security.

What this means for government

Supports whole-of-government PKI, agency-specific CA requirements, and API security with mutual TLS — all managed centrally.

Do You Need to Move Your DNS to Cloudflare?

No. Cloudflare supports two deployment models — agencies keep full control of their existing DNS infrastructure if they choose.

OPTION 1 — FULL SETUP

Cloudflare as Authoritative DNS

Cloudflare manages your DNS records. Domain validation for certificate issuance is fully automated — no manual steps required at any renewal.

Best for: new services, greenfield deployments, agencies ready to consolidate DNS

How Certificate Validation Works on a Partial Setup

Cloudflare uses **delegated DCV** (Domain Control Validation). A one-time CNAME record is added to your DNS pointing `_acme-challenge.yourdomain.gov.au` to Cloudflare. After that, all future certificate renewals are fully automated — no further DNS changes needed.

OPTION 2 — PARTIAL SETUP (CNAME)

Keep Your Existing DNS — CNAME Hostnames to Cloudflare

Your DNS platform (Infoblox, Microsoft DNS, AWS Route 53, whole-of-government DNS) stays in place. You CNAME individual public-facing hostnames to Cloudflare. Cloudflare manages the edge certificate from there.

Best for: most government agencies — no DNS migration required

Wildcard Certificates on a Partial Setup

Wildcard certs (e.g. `*.agency.gov.au`) require DNS-based validation — the same one-time CNAME delegation. Once set up, renewals are automatic. No repeated DNS changes per renewal cycle.

Certificate Transparency Monitoring

WHAT IS CERTIFICATE TRANSPARENCY?

Every publicly-trusted TLS certificate must be logged in a public **Certificate Transparency (CT) log** before browsers will trust it. This creates an auditable, tamper-proof record of every cert ever issued for any domain.

Cloudflare monitors these logs and alerts you whenever a certificate is issued for your domains — whether by Cloudflare or any other CA.

Cloudflare is an active participant in the CT ecosystem — running CT logs and contributing to the infrastructure that keeps the web's certificate system honest.

WHY THIS MATTERS FOR GOVERNMENT

Detect Unauthorised Issuance

If a CA issues a cert for your domain without your knowledge — through a supply chain compromise or CA error — you are alerted immediately.

Shadow IT Visibility

Discover subdomains and services that have been stood up without central IT knowledge — a common issue in large agencies.

ISM Compliance Support

Supports ASD ISM requirements for certificate inventory monitoring. Available on all Cloudflare plans at no additional cost. Note: opt-in — must be enabled per zone in the Edge Certificates dashboard.

Australian Government Alignment

REGULATORY & COMPLIANCE ALIGNMENT

ASD ISM — Certificate Controls

ASD ISM certificate management controls require documented renewal processes and audit trails. Cloudflare's centralised dashboard and CT Monitoring satisfy these requirements for public-facing services.

Essential Eight — Patch Management

Automated certificate renewal aligns with Essential Eight Maturity Level 2+ requirements for timely patching and configuration management of internet-facing services.

PSPF — Information Security

Cloudflare has completed an IRAP assessment. Contact the Cloudflare public sector team for the current assessment report, scope, and applicable workload classifications under the PSPF.

CLOUDFLARE IN THE AUSTRALIAN GOVERNMENT CONTEXT

- **IRAP assessed** — contact the Cloudflare public sector team for current assessment scope and applicable workload classifications
- **Australian PoPs** — Sydney, Melbourne, Perth, Brisbane, Canberra. Traffic stays in-country where required.
- **Whole of Government** — one Cloudflare deployment can cover multiple agency domains under a shared services model
- **ISO 27001 / SOC 2 Type II** — independently audited security controls
- **No vendor lock-in** — BYO certificates, multiple CA support, custom root chains

Recommended Next Steps

KEY TAKEAWAYS

1. **This is already happening.** The 200-day limit took effect 15 March 2026. The path to 47 days by 2029 is ratified CABForum policy — not a proposal, not reversible.
2. **Australian Government agencies face the highest risk.** Legacy infrastructure, slow procurement, and complex multi-domain estates create a perfect storm for cert expiry outages.
3. **Cloudflare provides immediate protection** without requiring infrastructure replacement. Proxy first — modernise at your own pace.

THREE PATHS FORWARD

Protect Now — Weeks

Put Cloudflare in front of your internet-facing services. Edge handles all public cert renewal immediately. No origin changes required.

Assess — 1 to 3 Months

Certificate inventory audit — map all public-facing certs across agency domains. The 200-day limit is already active; the 100-day limit arrives March 2027.

Modernise — 6 to 24 Months

Plan ACME adoption for origin systems on a managed timeline. Cloudflare acts as the stable intermediary throughout the transition.