3Cs
AQUARAH

SSL/TLS CERTIFCATE UPDATE

SSL/TLS Certificates Are Changing: Shorter Validity, Higher Security. Is Your Business Ready?

The Certificate Authority/Browser Forum is introducing major updates to the rules and policies governing SSL/TLS certificates. The upcoming changes will impact how organisations manage certificate lifecycles, maintain security compliance, and ensure a seamless and trusted online experience. Over the years, SSL/TLS Certificates had formed the backbone of HTTPS, acting as a badge or an icon that confirms data security, and browsing safety across web platforms, applications and webpages.

Starting **March 15, 2026**, the maximum allowed validity period for new public TLS certificates will drop step by step, ultimately reaching just **47 days** by 2029. This phased reduction transforms certificate management from an annual task into a near-continuous process.

The New Validity Timeline (for certificates issued on or after these dates):

- **Until March 15, 2026**: Up to 398 days (current standard, get your longer ones now if needed!)
- **March 15, 2026**: Maximum validity reduced to **200 days** (~6.5 months)
- **March 15, 2027**: Further cut to **100 days** (~3.3 months)
- **March 15, 2029**: Final limit of **47 days** (~1.5 months, roughly monthly renewals)

These changes also tighten **Domain Control Validation (DCV)** reuse periods (dropping to as low as 10 days by 2029 for many cases) and affect organization validation reuse for OV/EV certificates.

Why the Change? A Stronger, More Resilient Web

The primary drivers include:

- Reducing the impact of key compromises - shorter lifetimes mean stolen or weak keys become useless faster.
- Addressing weaknesses in current revocation systems (CRL/OCSP) - which struggle at internet scale.
- Encouraging widespread automation to handle frequent renewals reliably.
- Preparing the ecosystem for future cryptographic transitions, including post-quantum readiness.

This isn't optional, all major browsers (Chrome, Safari, Firefox, Edge) will enforce these rules by refusing to trust non-compliant certificates.

Real-World Impact on Your Business

If your website, API, e-commerce platform, intranet, or any online service relies on public TLS certificates:

- Certificate expirations will happen far more often with a higher risk of downtime, "Your connection is not private" warnings, SEO penalties, and lost revenue.
- Manual renewals (buying certificates, generating CSRs, validating domains) will become unsustainable and error prone.
- Teams without automation face increased operational burden, compliance headaches, and potential security gaps.

The good news? Modern tools make this manageable, and even beneficial, by enabling seamless, zero-touch renewals.

Practical Steps to Get Ahead.

Conduct A Full Audit

Create a complete inventory of all TLS certificates—public, internal, PKI, wildcard, SAN, legacy systems, APIs, load balancers, containers, and third-party integrations. This uncovers shadow IT, undocumented certificates, and manual processes that could cause outages.

Implement Automation Immediately

Replace manual management with ACME-based automation for issuance, renewal, revocation, and deployment. Automation reduces errors, lowers overhead, and supports short-lived certificates used in cloud, microservices, CI/CD, and IoT environments.

Update Monitoring and Alerting

Strengthen visibility with alerts for expirations, failed renewals, deployment issues, and configuration changes. Integrate certificate health checks into existing observability tools and ensure clear ownership for responding to alerts.

Test In Staging Before Rollout

Validate automation in a non-production environment to confirm integrations, permissions, renewal timing, and deployment workflows. Gradual rollout reduces risk and exposes issues before they affect production.

Train Your Team

Ensure DevOps, security, and IT teams understand certificate lifecycles, automation tools, and troubleshooting. Shared knowledge embeds certificate management into daily operations and reduces friction.

Review Vendors and Partners

Confirm how cloud providers, CDNs, MSPs, and SaaS vendors handle certificate automation and shorter lifecycles. Clarify responsibilities, visibility, and incident communication to avoid external blind spots.

Businesses that act early will turn this challenge into an opportunity: stronger security posture, fewer incidents, and more reliable digital services.

At **3Cs Aquarah**, we support organizations in navigating these relevant and rapidly evolving security transitions with precision and minimal operational disruption. Our experts provide end-to-end capabilities, from enterprise-wide certificate audit and automation enablement to continuous lifecycle governance ensuring your digital trust infrastructure remains resilient, compliant, and aligned with emerging industry mandates.

Don't wait for the first 200-day cutoff in 2026. Proactive security isn't just best practice, it's essential for protecting your reputation and revenue.
Ready to future-proof your certificates? Contact us today for a tailored audit and roadmap.