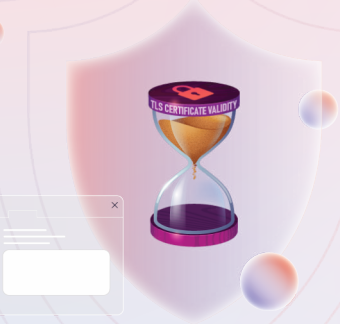
appviewx

Navigating Google's 90-Day TLS Certificate Validity Proposal

In March of 2023, Google announced plans to reduce the maximum validity period for public TLS certificates to 90 days (down from 398 days). The shift to short-lived certificates is intended to **encourage automation and promote agility**, in order to prepare for the evolving PKI landscape and post-quantum cryptography.

What does Google's proposal mean?

- Once effective, newly issued public trust TLS Certificates can only be valid for a maximum of **90 days** (or they will be distrusted by Google browsers). Google has over 60% browser market share and other browsers are expected to adopt this policy.
- Once adopted by the CA/Browser Forum, **Public CAs** will be **restricted** to issuing public trust TLS with a maximum validity of 90 days.
- **Impact** - All organizations, from large to small, will have to shift to short-lived certificates. **TLS certificates will need to be renewed more than four times a year** – putting tremendous stress on PKI and security teams.



When will this proposal take effect?

The effective date is still to be determined.

Google plans to introduce this change either in a future policy update of Google's Chrome Root Program or a CA/B Forum Ballot Proposal.

The industry has been pushing for shorter lived TLS certificate validity for over a decade with validity continuing to be reduced.

How TLS Certificate Lifespans Have Changed Over Time

Why Short-Lived Certificates?

- **Enhanced Security**
- **Encourages Automation**
- **Promotes Agility**
- **Supports Compliance**

https://www.appviewx.com/products/avx-one-clm/

Prepare Now with Crypto-Agility from AVX ONE CLM

Greater **Visibility** - Smart Discovery and inventory of all certificates (public & private) including the associated endpoints, critical metadata, and expiration dates. Actionable dashboards and insights, including 90-Day TLS and PQC analysis, provides complete visibility into PKI assets.

Unrivaled **Automation**- Automation workflows (out-of-the-box and custom), REST APIs, auto-enrollment protocols (ACME, EST/SCEP, Windows auto-enrollment) and extensive integrations enable complete certificate lifecycle automation - eliminating outages and security weaknesses.

Continuous **Control** - Robust policy and compliance engine puts teams in complete control over their PKI and certificate landscapes by creating and enforcing enterprise-wide compliance policies.

Scan QR code to learn more about how AppViewX can be your partner of choice in your cybersecurity journey

AppViewX Inc.,

City Hall, 222 Broadway, New York, NY 10038

info@appviewx.com | www.appviewx.com

+1 (206) 207-7541, +44 (0) 203-514-2226