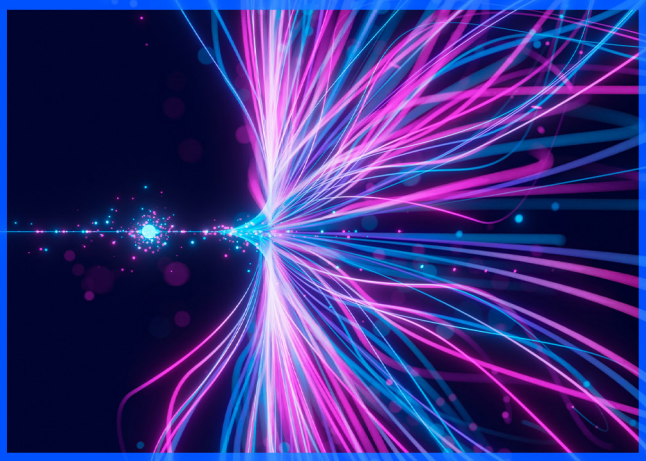
KPMG

SSL/TLS lifespans decrease

PQC challenges ahead



The CA/Browser Forum's drastic reduction of secure sockets layer/transport layer security (SSL/TLS) certificate lifespans to 47 days by 2029, combined with the complex migration to postquantum cryptography (PQC), presents organizations with an unprecedented challenge, demanding a heavy lift to overhaul certificate management and secure systems against emerging quantum threats.

Introduction

The CA/Browser Forum's decision to reduce the maximum lifespan of SSL/TLS certificates from 398 days to 47 days by 2029, coupled with the ongoing transition to PQC, represents a transformative moment for digital security. Driven by industry leaders like Apple, Google, and Mozilla, the certificate lifespan reduction aims to enhance security by minimizing the risks of compromised credentials. Simultaneously, the migration to PQC is critical to counter the emerging threat of quantum computing, which will render current cryptographic algorithms obsolete.

Security benefits

The reduction in SSL/TLS certificate lifespans is designed to strengthen internet security. Certificates underpin secure HTTPS connections, and a shorter validity period—47 days by 2029—limits the time a compromised certificate can be exploited. For example, a stolen certificate will expire faster, reducing its utility to attackers compared to a 398-day certificate. Apple's proposal, supported by Sectigo, Mozilla, and Google, highlights that shorter lifespans mitigate risks from outdated cryptographic algorithms and prolonged exposure to compromised credentials. Additionally, reducing domain control validation (DCV) reuse from 398 days to 10 days by 2029 ensures frequent domain ownership verification, decreasing the chance of misissued certificates being misused (CA/Browser Forum).

This trend toward shorter lifespans builds on a decade-long effort to address evolving threats. Since 2011, certificate validity has dropped from 8–10 years to 398 days. The CA/Browser Forum's recent vote, with 25 in favor and 5 abstentions, reflects industry consensus that 398 days is too long in today's threat landscape. Frequent renewals create a more agile, secure ecosystem, phasing out vulnerable certificates quickly.

> "As quantum computing advances, the new 2025 CA rules empower postquantum cryptography to fortify digital security, safeguarding sensitive data and ensuring resilient trust across global networks in an increasingly quantum-driven world."
>
> — Dr. Aaron Kemp
> US Quantum Lead, KPMG LLP

Operational challenges

Automation is the linchpin for successfully navigating the shift to 47-day certificate lifespans. Tools like Let's Encrypt and CertBot, which leverage the ACME protocol, enable organizations to automate certificate issuance, renewal, and installation, significantly reducing the administrative burden. These solutions are particularly valuable for smaller businesses, as Let's Encrypt offers free certificates and simplifies the renewal process. For larger enterprises, certificate lifecycle management (CLM) platforms, such as Sectigo Certificate Manager, provide comprehensive tools to manage certificates across diverse environments, regardless of the issuing authority.

Automation not only mitigates the risk of outages due to expired certificates but also aligns with the industry's push for crypto-agility—the ability to rapidly adapt to new cryptographic standards or security threats. For example, cloud platforms like AWS, Azure, and Cloudflare offer built-in certificate management tools that streamline renewals for organizations using their services. By integrating automation, organizations can ensure compliance with the new 47-day lifespan and 10-day DCV requirements while minimizing manual intervention.

However, automation is not a panacea. Organizations must invest in training, infrastructure upgrades, and integration with existing systems to fully realize its benefits. Legacy systems, in particular, may require significant reconfiguration or replacement to support modern automation protocols. Additionally, while automation reduces costs associated with manual labor, the initial setup and ongoing maintenance of CLM platforms can be resource-intensive, particularly for smaller organizations.

Conclusion

The reduction of SSL/TLS certificate lifespans from 398 days to 47 days by 2029 is a bold step toward enhancing internet security. By limiting the window for certificate misuse and enforcing frequent domain revalidation, the CA/Browser Forum aims to create a more resilient digital ecosystem. However, this change places a heavy burden on information technology teams, particularly those reliant on manual processes or managing legacy systems. Automation is essential for adapting to this new reality, offering a path to compliance and operational efficiency. Organizations must act swiftly to implement automated certificate management solutions, leveraging tools like Let's Encrypt, ACME, and CLM platforms to future-proof their operations. While the transition will be challenging, it presents an opportunity to modernize certificate management practices and strengthen cybersecurity in an increasingly threat-prone world.

KPMG emerging technologies explores quantum technologies, artificial intelligence, blockchain, and spatial computing to help deliver innovative approaches that drive transformative business outcomes. Through strategic alliances and a business-first approach, KPMG LLP empowers organizations to stay ahead in a rapidly evolving digital landscape.

Contact us

Richard Entrup
Emerging Solutions Leader,
KPMG LLP
T: 201-307-7575
E: rentrup@kpmg.com

Dr. Aaron Kemp
US Quantum Lead,
KPMG LLP
T: 404-358-3138
E: aaronkemp@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**