

The path toward 47 days SSL/TLS certificates

A practical guide for organizations facing short-lived digital certificates



Introduction

If you are reading this, you are likely already aware of the recent decision by the CA/Browser Forum: the maximum validity period of public SSL/TLS certificates will be progressively reduced to 47 days.

This evolution follows a trend that began over 13 years ago, during which certificate lifetimes have continually decreased. The progressive reduction, planned through 2029, is guided by well-defined schedules established by regulatory bodies and major industry players.

The goal is twofold: enhance the overall security of the digital ecosystem and accelerate cryptographic agility while limiting the risks associated with digital identity compromise.

For organizations, it represents a true paradigm shift.

Certificate management is now a continuous, high-frequency process impacting IT operations, regulatory compliance, and strategic risk management.

The move toward short-lived certificates challenges long-standing practices and requires the adoption of new methods, as manual processes and legacy tools will no longer suffice.

Yet, at the heart of this transformation lies a genuine opportunity: organizations that adapt swiftly will not only reduce their risk exposure but also gain agility to comply efficiently with new standards and regulatory requirements as they evolve.

This white paper serves as your strategic guide to approaching this transition confidently. It explores the reasons behind the certificate lifetime reduction, its implications for the digital ecosystem, and the concrete actions your organization can take to strengthen resilience and preserve trust — today and in the future.

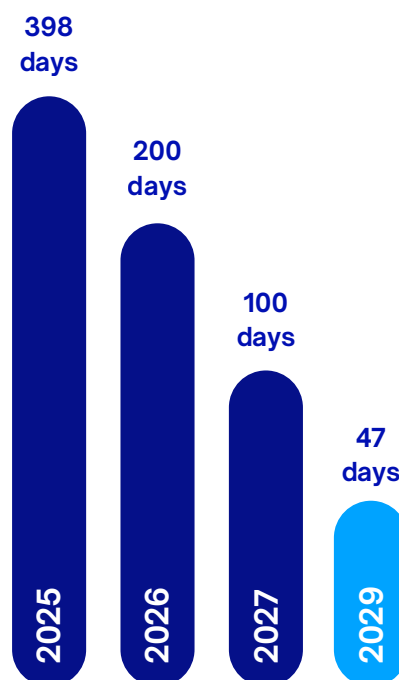
The evolution of SSL/TLS certificate lifespans

Understanding the shift toward shorter validity periods

Digital certificates have long formed the foundation of secure online communication, ensuring identity authentication and encrypted data exchange across the Internet.

Historically, SSL/TLS certificates were issued with multi-year validity, offering operational convenience but also increasing risk. Prolonged use of compromised keys or outdated cryptographic standards often weakened system security over time.

Today, one of the most pressing challenges is the migration toward post-quantum cryptography. In this context, reducing certificate lifetimes is becoming a critical strategy — limiting exposure windows and improving resilience against emerging vulnerabilities.



Who decides these changes?

The reduction in SSL/TLS certificate validity is not the result of a single regulator's decision but rather a collaborative industry consensus. The main driver is the CA/Browser Forum, a voluntary consortium established in 2005.

Key stakeholders include:

Public Certificate Authorities (CAs)

digicert Let's Encrypt ENTRUST SSL.com

Browser vendors

Google Apple Edge Firefox

Other industry participants

Since its creation, the Forum has developed the Baseline Requirements governing the issuance, validation, and management of public certificates — forming the foundation of Internet security standards.

Proposal



Debate



Revision



Vote

The recent decision to limit certificate validity to 47 days was initially proposed by Apple, then rapidly supported by Google. This measure was adopted after extensive debate involving CAs and their customers, illustrating the collaborative nature of this ecosystem.

Why shorter lifetimes?

The security imperative behind accelerated certificate rotation

Reducing SSL/TLS certificate lifetimes introduces new management challenges, but it is a necessary step toward stronger digital security.

4 major reasons for shorter certificate lifespans



1

Limiting exposure to compromise

Shorter validity periods dramatically reduce the window of opportunity for attackers to exploit compromised or mismanaged certificates.

- ▶ The average intrusion detection time (277 days) exceeds new certificate lifetimes.
- ▶ Domain hijacking attacks persist until the certificate expires.
- ▶ Initial validation checks can become outdated within weeks, making long-lived certificates a liability.



2

Addressing revocation inefficiencies

The certificate revocation process has long been a weak point in PKI ecosystems. Some browsers bypass or fail revocation checks, allowing revoked certificates to remain active longer than intended.

- ▶ OCSP implementation varies across browsers, leading to inconsistent protection.
- ▶ Network connectivity issues may prevent real-time revocation checks.



3

Enabling cryptographic agility

Rapid certificate rotation allows faster adoption of new cryptographic standards and quantum-resistant algorithms.

- ▶ The U.S. NIST estimates that quantum computers could break RSA-2048 by 2030.
- ▶ Current certificate lifetimes delay crypto migrations by up to two years.
- ▶ With 47-day cycles, organizations can deploy algorithmic updates enterprise-wide in under three months.



4

Driving automation adoption

Frequent renewals make manual management unsustainable. Short lifetimes serve as a catalyst for automation, accelerating the adoption of Certificate Lifecycle Management (CLM) systems.

- ▶ Manual certificate inventory and handling remains the top cause of certificate-related outages.
- ▶ 47-day cycles require 8× more renewal operations per year.
- ▶ Automated lifecycle management minimizes human error, ensuring speed, consistency, and resilience.

What if no action is taken?

Transitioning to 47-day certificates imposes a new operational rhythm. Failure to adapt exposes organizations to significant business and security risks:

Increased service interruptions

More frequent renewals heighten the risk of unnoticed expirations. A single expired certificate can render a website or application unavailable — directly impacting operations and customer experience.

Erosion of trust and brand reputation

Security warnings or outages degrade user trust and can cause long-term reputational damage.

Operational overload

Manual management becomes time-consuming and error-prone, diverting IT teams from high-value initiatives toward repetitive maintenance tasks.

Regulatory non-compliance

Failure to maintain certificate validity and service availability can lead to audit findings, penalties, or contractual breaches under security frameworks such as NIS2, PCI DSS, or ISO 27001.

The strategic response: intelligent automation

Intelligent automation emerges as the only sustainable approach to managing short-lived SSL/TLS certificates effectively and securely.

A three-pillar framework

1

Lifecycle Automation

Eliminate repetitive manual tasks by automating issuance, renewal, and revocation. The automation platform should be able to handle thousands of certificates simultaneously — with zero human intervention.

2

Visibility and Governance

Gain real-time insight into every certificate deployed across physical servers, clouds, and containers. Centralized visibility enables proactive management and rapid response to incidents.

3

Human Expertise

Transform PKI teams from tactical operators into strategic architects who define security policies, design automation workflows, and drive organizational resilience.

Le CLM : une approche globale et automatisée

Certificate Lifecycle Management (CLM) provides an end-to-end framework for certificate operations — encompassing discovery, issuance, deployment, renewal, monitoring, and revocation.

At its core, CLM delivers:

- ▶ Centralized visibility across all environments.
- ▶ Policy-driven automation for compliance and security.
- ▶ Continuous monitoring to detect anomalies and prevent outages.

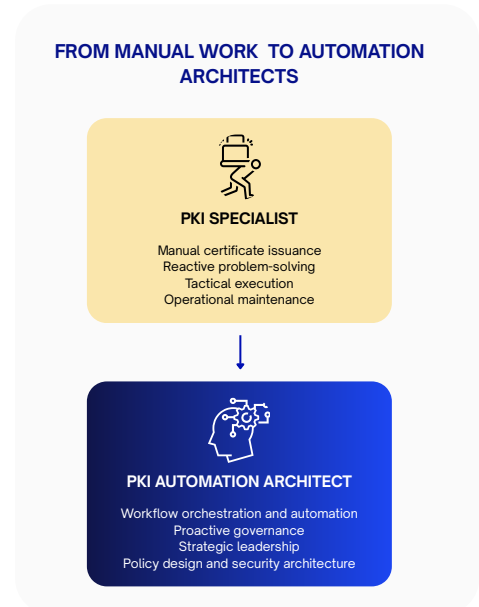
Through this approach, organizations transition from reactive, manual processes to proactive, scalable digital trust management.

The human role in automation

As automation reshapes certificate management, the role of the PKI professional is being fundamentally redefined.

What was once a tactical, manual discipline is evolving into a strategic function centered on policy design, automation orchestration, and continuous governance.

Modern PKI experts no longer spend their time issuing certificates or responding to individual requests. Instead, they architect and optimize automated workflows that operate across the entire enterprise — ensuring resilience, scalability, and compliance.



Design and orchestrate automation

PKI architects define strategies, select appropriate tools (such as ACME), and integrate automation solutions within the organization's existing ecosystem. They ensure these systems align with business needs and meet stringent security requirements.

Ensure compliance and governance

Human oversight remains essential to enforce internal and regulatory policies, assign responsibilities, and validate approval workflows. Continuous adaptation is required to maintain compliance as standards evolve.

Anticipate and manage risk

PKI experts identify and mitigate risks introduced by shorter certificate lifetimes, establishing incident response plans and ensuring rapid remediation in the event of compromise or technical failure.

Enable change and empower teams

They play a key role in training and guiding IT and business teams, fostering a security-first culture and ensuring smooth adoption of automated processes.

While human expertise drives transformation, effective implementation requires tools capable of handling the scale, speed, and complexity of modern certificate operations. The increasing number of both public and private certificates — combined with the need for uninterrupted availability — makes manual management operationally impossible.

In this context, Certificate Lifecycle Management (CLM) has become an essential foundation for enterprise security and compliance. A robust CLM platform provides a unified, automated approach to managing every phase of the certificate lifecycle — from discovery to issuance, renewal, deployment, monitoring, and revocation.

➤ EVERTRUST SOLUTION

Certificate Lifecycle Manager

End-to-end orchestrated certificate management

✓ Comprehensive Visibility

Gain a complete, real-time view of every certificate across your infrastructure — networks, containers, clouds, workloads, and load balancers.

✓ Full lifecycle automation

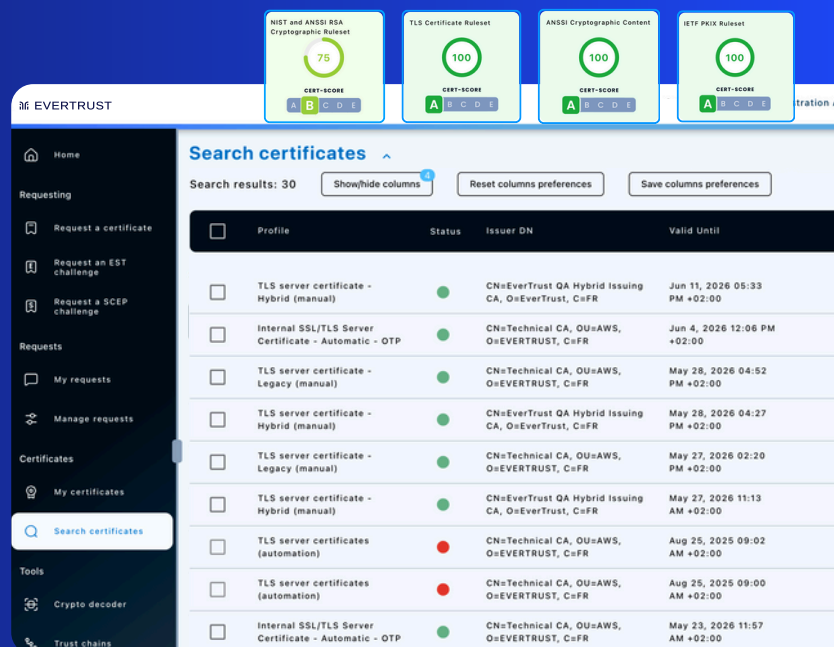
Automate issuance, renewal, deployment, and revocation across both internal PKIs and public Certificate Authorities. This enables consistent enforcement of policies and eliminates manual intervention, even at massive scale.

✓ Intelligent alerts and incident prevention

Receive proactive notifications for expiring or non-compliant certificates. Dynamic dashboards provide real-time insights to maintain continuous trust and reduce the risk of downtime.

✓ Unified policy and compliance management

Apply enterprise-wide security policies automatically — including algorithm selection, key length, and CA restrictions — and maintain complete traceability for audits and regulatory compliance (NIS2, PCI DSS, ISO 27001, etc.).



About Evertrust

Evertrust is a European software vendor specializing in digital certificate and Public Key Infrastructure (PKI) management solutions for global enterprises and organizations.

Founded in 2017 and headquartered in France, Evertrust develops a comprehensive suite of tools that cover the entire certificate lifecycle, including: automated management of public and private certificates as well as a high-performance private Certification Authority (CA) engine.

Evertrust is ISO 27001 certified and a proud member of Hexatrust, and the PKI Consortium.

As an independent European provider, Evertrust stands at the forefront of digital sovereignty and trust infrastructure.

+20%

of major French enterprises supported

+30M

certificates managed

+500K

machine identities secured