

Post-quantum cryptography (PQC) standards alignment

Learn how NIST PQC standards, CA/B Forum certificate lifespan changes, and federal timelines are reshaping cryptography and certificate management.



A cryptographic transition is underway. Finalized post-quantum cryptography (PQC) standards are replacing classical public key algorithms like RSA and ECC with alternatives designed to withstand quantum computer attacks. At the same time, publicly trusted SSL/TLS certificate validity periods are shrinking, reaching a 47-day maximum by 2029.

Three bodies are driving this shift: the [CA/Browser Forum](#), [NIST](#), and the White House. NIST and the CA/Browser Forum set the technical requirements; [Executive Order 14412](#) adds federal urgency to accelerate adoption.

NIST's accelerated deadlines: 2030–2031, not 2035

NIST's original roadmap, IR 8547 ([Transition to Post-Quantum Cryptography Standards](#)), set 2030 as the date for transition, with 2035 as the hard deprecation deadline to retire RSA and ECC.

On June 22, 2026, the White House signed **Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks,"** compressing the federal migration schedule by five years. Start contractor obligations:



- The FAR Council must publish a proposed rule by about December 19, 2026, requiring covered contractors to comply with NIST FIPS, including the PQC FIPS, **by December 31, 2030**
- Adopt PQC-based **digital signatures by December 31, 2031**
- Extend compliance to federal contractors, who must meet post-quantum FIPS requirements by end of 2030

Private industry is moving faster still. **Google** (March 2026) and **Cloudflare** (April 2026) have both targeted full PQC migration across infrastructure, authentication, and encryption by **end of 2029**, a year ahead of the federal deadline.

Behind all of these timelines is the same driver: harvest now, decrypt later (HNDL) risk, where adversaries collect encrypted data today to decrypt once quantum computing matures. With the federal government and the internet's largest infrastructure providers converging on 2029–2031, the 2035 horizon is no longer a safe planning assumption.

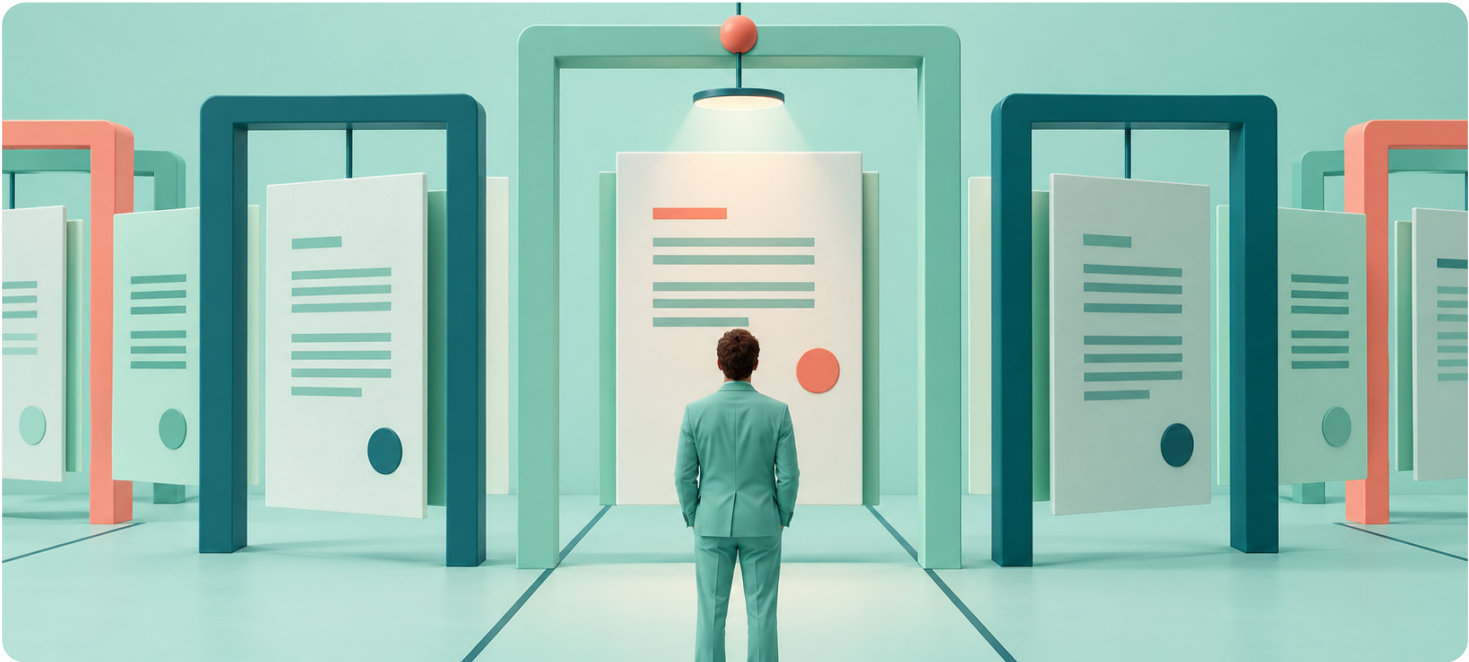
CA/Browser Forum: shorter certificate lifespans

Ballot SC-081v3 (April 2025) set a phased schedule for reducing publicly trusted SSL/TLS certificate validity and DCV reuse periods, limiting the exposure window tied to certificate compromise:

Date	Max certificate validity	DCV Reuse
March 15, 2026	200 days	200 days
March 15, 2027	100 days	100 days
March 15, 2029	47 days	10 days



This schedule applies to publicly trusted SSL/TLS certificates only; it does not mandate validity periods for private PKI.



White House Executive Order 14412

Signed June 22, 2026, EO 14412 sets hard deadlines for federal high-value assets and high-impact systems:

- PQC key establishment (e.g., ML-KEM) by December 31, 2030
- PQC digital signatures by December 31, 2031

Near-term milestones: agencies had 30 days to name a PQC migration lead. OMB issued its implementing guidance, M-26-15, on June 24, 2026, and agency migration plans are due within 120 days (about October 22, 2026). Within 180 days of the order, the FAR Council must propose the contractor rule described above. Within 270 days (about March 19, 2027), CISA and NIST must publish minimum elements for a cryptographic bill of materials (CBOM).

Enterprise impact

NIST, the CA/Browser Forum, and the White House are driving related but distinct changes, together pointing to one priority: crypto-agility built on automation. M-26-15 from the White House calls for a dynamic, continuously updated inventory of all cryptographic assets built with automated tools, feeding a central CBOM. It names logical access control systems based on asymmetric encryption such as PKI as priority systems and requires TLS 1.3 support no later than January 2, 2030. This detailed memo is the strongest federal support for the adoption of automated CLM.

Automated certificate lifecycle management (CLM) supports both 47-day readiness and PQC migration by helping organizations discover certificates, manage renewals, prove domain control, and rotate keys and algorithms as standards evolve.

Five readiness areas matter most:

- 1 Cryptographic inventory** — visibility across all certificates, keys, systems, and algorithms. You can't protect what you can't see.
- 2 Automated certificate management** — end-to-end CLM removing manual work as lifecycles shorten. With lifespans shortening to 47 days, your team is about to face 12x more work; an unsustainable task if done manually.
- 3 DCV ownership and workflow readiness** — repeatable domain validation before reuse windows shrink. Persistent DCV (CA/B Forum Ballot SC-088v3) lets a domain owner publish one DNS record that the CA re-checks automatically, which keeps validation current as the reuse period drops to 10 days.
- 4 Governance and auditing** — policies and audit trails for evolving standards and compliance. CLM allows your team to stay on top of new algorithms and policies, adapting quickly and automatically.
- 5 Crypto-agility** — the ability to replace algorithms and update certificates without disrupting operations. As PQC algorithms are released, your infrastructure needs to adapt fast.

Sectigo Certificate Manager (SCM) helps organizations prepare for shorter certificate lifecycles through CLM automation. The business case goes beyond compliance: a [Forrester TEI study](#) found Sectigo Certificate Manager helped customers reduce outage-related costs by \$2.4 million over three years. [Sectigo Quantum Labs](#) supports PQC readiness with a blueprint for the transition to quantum-safe cryptography and the [Sectigo 47-day toolkit](#) provides your team with the necessary documents and guidance to make the move towards automation.

Sources

<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>

<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>

<https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography>

<https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/>

<https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/>

<https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf>

