zensar

Quantum-Safe Trust Starts with the Certificates You Can't See

Quantum computing has turned cryptography from a background utility into a board-level deadline. The organizations that move first won't be the ones that swap algorithms fastest. They'll be the ones that know where their cryptography lives.

Whitepaper



An RPG Company

Executive summary

- **The blind spot is already costly.** Industry estimates suggest more than 70% of organizations lack a complete inventory of their certificates and keys. Every unknown certificate is a potential outage, audit finding, or entry point.
- **Manual certificate management has hit its limit.** Public TLS certificate lifetimes fell to 200 days in March 2026 and will reach 47 days by 2029. Spreadsheets and calendar reminders can't keep up.
- **Quantum risk is a present-day data problem**. Adversaries are harvesting encrypted data now to decrypt later. Anything that must stay confidential beyond 2030 is already exposed.
- **Regulators have set dates.** US Executive Order 14412 (June 2026) requires quantum-safe key establishment by end of 2030 and signatures by end of 2031 for federal systems, and those requirements are flowing into contracts. The EU expects transition to start by end of 2026.
- **Our view:** Treat post-quantum migration as a crypto-agility program, not a one-time algorithm swap. Start with discovery, centralize control, automate the life cycle, then migrate in phases.

Certificates are the trust layer nobody owns

Digital certificates and their private keys prove which websites, applications, APIs, workloads, and devices can be trusted. They sit underneath every secure transaction, yet ownership is usually scattered across infrastructure, application, cloud, and security teams. Machine identities now outnumber human ones by a wide margin, and most of them are issued, renewed, and retired without a single point of oversight.

That fragmentation creates four recurring failure modes:

Failure mode	What actually happens	Business consequence
Expired certificates	A forgotten certificate lapses and a customer-facing service or internal integration stops working	Outages, lost revenue, emergency change windows
Compromised private keys	Attackers use a stolen key to impersonate trusted systems, intercept traffic or sign malware	Fraud, data theft, reputational damage
Weak or deprecated cryptography	Legacy algorithms, short keys, and old protocols stay in production long after they should be retired	Audit findings, easier interception
Shadow and rogue certificates	Self-signed or unmanaged certificates are issued outside policy and never tracked	Blind spots that attackers find first

Three pressures are converging at once

47 days

Maximum public TLS certificate lifetime from March 2029 (CA/Browser Forum)

2030

Quantum-safe key establishment deadline for US federal high-value systems (EO 14412)

2035

Target date by which RSA and ECC are disallowed under NIST draft guidance (IR 8547)

01 Certificate lifetimes are collapsing

The CA/Browser Forum has approved a phased reduction in public TLS certificate validity: 200 days from March 2026 (already in effect), 100 days from March 2027, and 47 days from March 2029. At 47 days, each public certificate must be renewed roughly eight times a year. For an estate of several thousand certificates, manual renewal stops being a process and becomes a source of outages.

02 Harvest now, decrypt later is already happening

Nation-state actors and well-funded criminal groups are capturing encrypted traffic and data today, expecting that a cryptographically relevant quantum computer will eventually break RSA and elliptic-curve cryptography. Customer records, health data, intellectual property, contracts, and financial information that must remain confidential for years are exposed the moment they are captured, not when the quantum computer arrives.

A simple test for urgency

If how long your data must stay secret plus how long your migration will take is greater than the time until quantum computers can break today's encryption, you are already late.

Most enterprise cryptographic migrations take several years. For data with a seven- to ten-year confidentiality requirement, the window to act is now.

03 Quantum readiness has become a compliance requirement

Post-quantum cryptography moved from research to regulation in under two years:

When	When Milestone	What it means
Aug 2024	NIST publishes FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA)	Production-ready quantum-safe algorithms exist; the "wait for standards" argument is over
Mar 2025	NIST selects HQC as a backup key-encapsulation algorithm	Standards will keep evolving, so systems must be able to change algorithms
Mar 2026	Public TLS certificate lifetime drops to 200 days	Renewal volume roughly doubles
Jun 2026	US Executive Order 14412 and OMB M-26-15	Federal PQC migration deadlines that federal suppliers and contractors will be expected to meet
End 2026	EU coordinated roadmap: Member states begin transition	European organizations need inventories and plans in place
2027	France's ANSSI stops certifying products that are not quantum-safe	Procurement starts filtering out non-PQC products
2030/2031	EO 14412: Key establishment (2030) and signatures (2031) must be quantum-safe; EU: high-risk systems protected by 2030	Core deadlines for most regulated enterprises
2035	NIST IR 8547 (draft): RSA and ECC disallowed	End of the classical-only era

Our point of view: Build crypto-agility, not a one-time swap

Replacing RSA with ML-KEM and ML-DSA is necessary but not sufficient. The algorithm list will keep changing: HQC is still being standardized, FN-DSA (FIPS 206) is in draft, and certificate lifetimes will keep shrinking. The goal is crypto-agility – the ability to change algorithms, keys, and certificates across the estate in days rather than years, through policy and automation, without rewriting applications. Zensar recommends four principles:

Principle	What actually happens
You can't migrate what you can't see	Build a living inventory of every certificate, key, and algorithm across cloud, on-premises, APIs, code signing, and OT. It becomes your cryptographic bill of materials (CBOM).
Prioritize by data shelf life, not by system	Rank assets by how long the data they protect must stay confidential and how exposed they are. Long-lived, externally facing data moves first.
Centralize policy, automate execution	One policy engine for issuance, renewal, and revocation across internal and external CAs. Automation handles volume; people handle exceptions.
Migrate in hybrid phases	Run classical and post-quantum algorithms side by side (hybrid TLS key exchange, hybrid certificates), pilot on lower-risk systems, then scale. This avoids breaking legacy clients.

Questions every leadership team should be able to answer

- How many certificates and keys do we have, where are they, and who owns each one?
- What does certificate management cost us today in labor, tools, and outages?
- Which of our systems still rely on deprecated algorithms or protocols?
- Which data must remain confidential beyond 2030, and what protects it in transit and at rest?
- Could we renew every public certificate every 47 days without adding headcount?
- Could we replace a compromised CA or a broken algorithm across the estate within a week?

How Zensar helps: CertSecure

Zensar CertSecure takes organizations from uncertainty to quantum readiness in a structured path. It starts with a Digital Certificate Discovery Assessment that shows your true certificate inventory, compliance gaps, cost of management, and exposure to quantum-vulnerable algorithms. From there, CertSecure provides centralized certificate life cycle management, automated renewals, real-time monitoring integrated with your ITSM and the Zensar SOC, and a managed PKI-as-a-Service model. Most importantly, it delivers a phased roadmap to hybrid and post-quantum cryptography aligned with NIST and regional mandates.

Conclusion

Quantum computing is still maturing, but the risks tied to certificates and cryptographic assets are already here, and the regulatory clock has started. Organizations that gain visibility and control now will cut outages, pass audits, reduce cost, and meet each deadline as it arrives. Those that wait will face the same migration under far more pressure.

The journey starts with one question: What certificates do you have today?

Book a Digital Certificate Discovery Assessment with the Zensar CertSecure team to find out.

Sources

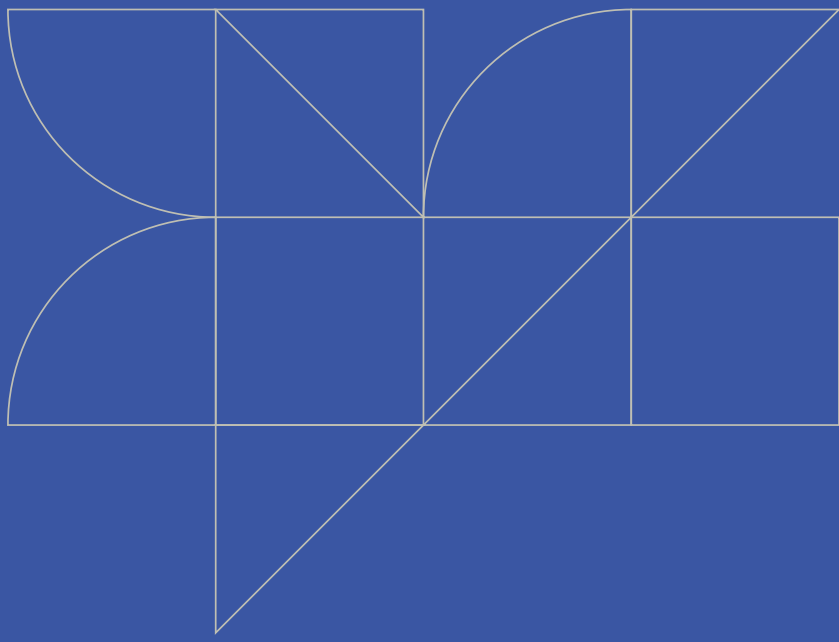
NIST, FIPS 203, 204 and 205 (August 2024); NIST HQC selection announcement (March 2025); NIST IR 8547 initial public draft (November 2024).

CA/Browser Forum Ballot SC-081, TLS certificate validity reduction schedule (2025).

The White House, Executive Order 14412 (June 2026); OMB Memorandum M-26-15 (June 2026).

European Commission, Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (June 2025).

Cloud Security Alliance, "Post-Quantum Cryptography: From Guidance to Mandate" (July 2026).



zensar

An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145+ leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**