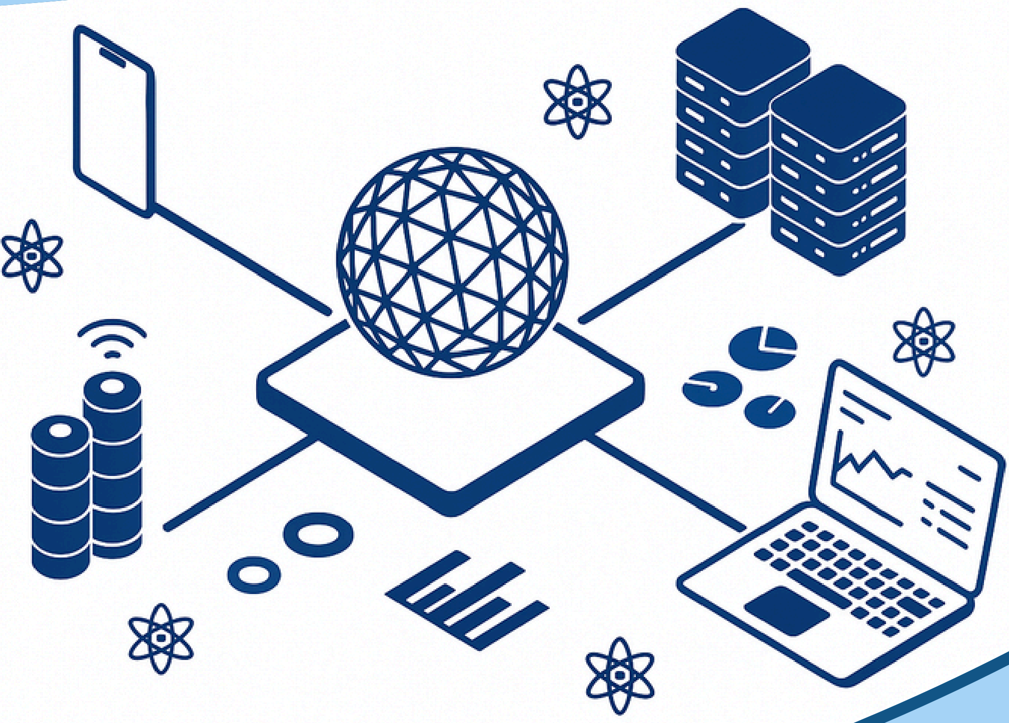
NEWSLETTER

Diplomatic Council Quantum Series

Issue 2 - The Post-Quantum Shift

by Harald A. Summa and Matthias Reidans



office@diplomatic-council.org

www.diplomatic-council.org/quantumleap

Table of Contents

About The Authors

Harald A. Summa is Chairman of the Diplomatic Council Quantum Leap Initiative, founder and honorary president of eco – Association of the Internet Industry, and former CEO of DE-CIX, the world's largest Internet exchange. For over two decades, he has shaped Europe's digital infrastructure and advised the German government on digital-economy strategy, serving on national and regional innovation councils.

Matthias Reidans, Innovation Programme Manager at the Diplomatic Council Quantum Leap Initiative, brings more than 25 years of experience in datacenter transformation, cloud migration, and digital modernization. A recognized expert in quantum infrastructure, he has led strategic projects for IBM, tecRacer, and Rosenberger-OSI, and advocates responsible, real-world deployment of quantum technologies across industries.

About This Series

The Diplomatic Council Quantum Series provides a strategic overview of global developments in quantum technology – from scientific milestones and market dynamics to questions of security, leadership, and readiness.

This edition focuses on Post-Quantum Cryptography (PQC): why the transition has begun, how the internet is adopting hybrid defenses, where enterprises get blindsided (PKI), and what a migration program that actually works looks like—plus where QKD and QRNG fit in a pragmatic quantum-safe portfolio.

To conclude, this edition includes an expert view to translate the technical shift into board-level action.

Key Focus Areas in This Edition PQC:

Why PQC Now

Standards, roadmaps, and HNDL urgency

The Standardized Core

ML-KEM and post quantum signatures in practice

Hybrid Internet Transition

Layered defense without breaking the internet

The 2026 Certificate Shockwave

Automation becomes the prerequisite

Enterprise & Portfolio

Enterprise Playbook + Quantum-Safe Portfolio

Diplomatic Council DC Quantum Leap Initiative UN Consultative Status

From “Future Risk” to Present Action: Why PQC Starts Now

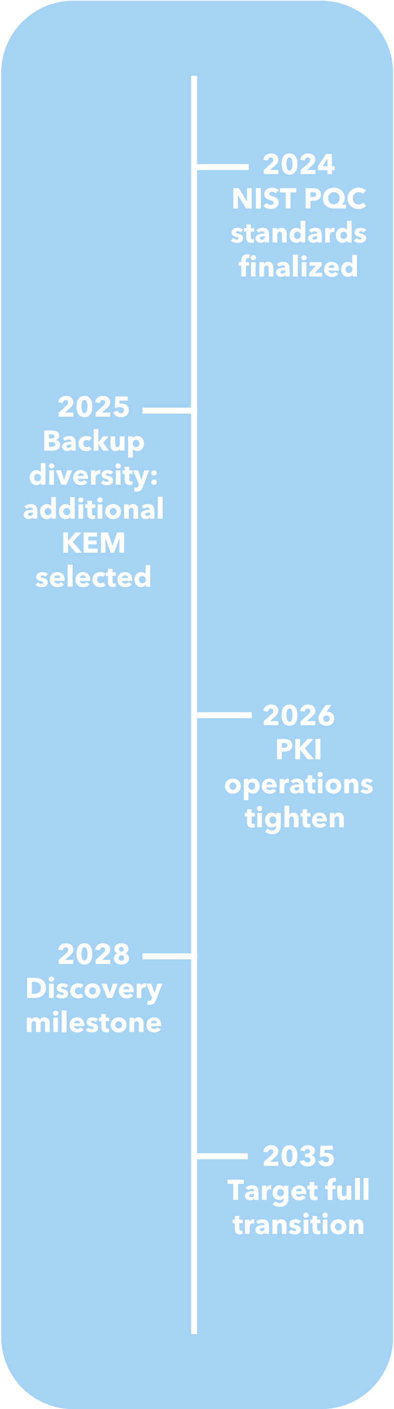
For years, post-quantum cryptography lived in the comfortable category of “important, but not urgent.” That era is ending. Not because a cryptographically relevant quantum computer has arrived, but because the world has stopped waiting for it. Standards are in place, roadmaps are published, and infrastructure cycles are compressing. PQC is shifting from research topic to delivery discipline.

The real driver is a quiet but brutal attack model: harvest-now, decrypt-later. If an adversary can copy encrypted traffic today, they can store it and crack it later the moment quantum capability matures. That flips the usual security mindset. You’re not protecting only future data, you’re protecting today’s data from tomorrow’s tools. And that’s why key establishment and transport protection move to the front of the queue.

If you wait for certainty, you migrate in crisis mode!

But here’s the trap: organizations treat PQC like a one-time algorithm swap. It isn’t. PQC is a trust-stack rewrite—keys, certificates, signatures, hardware roots, libraries, and operational processes. The winners will not be the companies that “pick the perfect algorithm.” They’ll be the ones that build crypto-agility: inventory, policy, automation, and the ability to rotate primitives without chaos.

A useful mindset is to treat PQC like a major cloud migration: it touches everything, and success is mostly execution. If you wait for a single “Q-Day,” you’ll be forced into a rushed transition. If you start now, you control the timeline—and you turn a looming risk into a maturity upgrade.



2024 NIST PQC standards finalized

2025 Backup diversity: additional KEM selected

2026 PKI operations tighten

2028 Discovery milestone

2035 Target full transition

The New Cryptographic Alphabet: What Got Standardized (and Why That Matters)

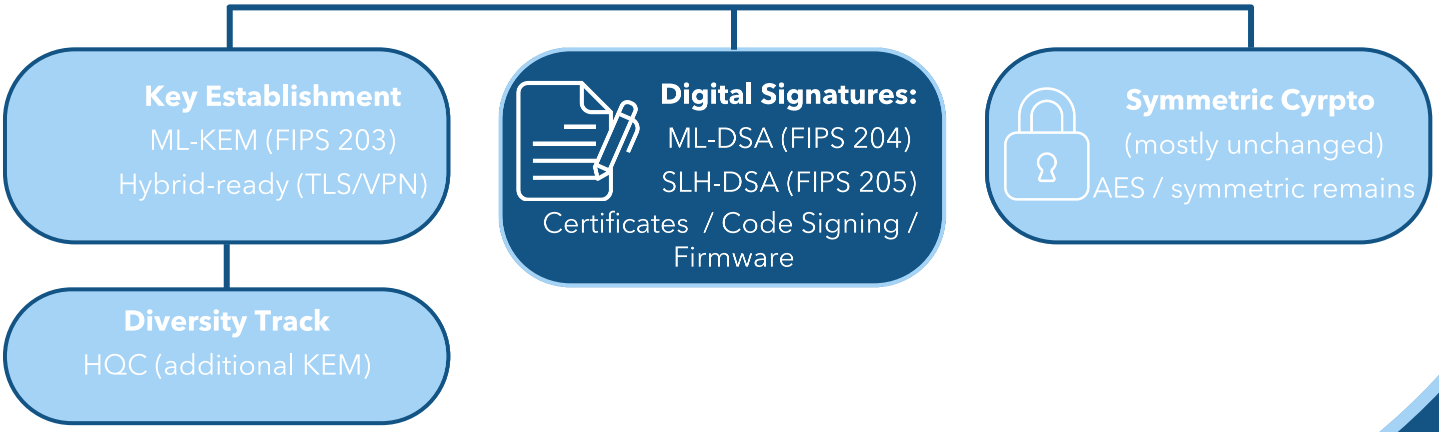
PQC is often presented as a simple replacement: “swap RSA/ECC for something quantum-safe.” Reality is more nuanced. The post-quantum portfolio is built to cover different trust jobs—confidentiality, authenticity, long-term verification—and each behaves differently in real systems.

Start with key establishment. A key exchange is the lock on the wire: it protects sessions in TLS, VPNs, and secure messaging. That’s why modern migration guidance prioritizes quantum-resistant key establishment early—to blunt harvest-now, decrypt-later. The industry trend is hybridization: combine a classical method with a PQC method so you get a safety net even if one side ages badly.

Signatures are the second pillar. They secure identities, software updates, and certificate chains—the “who are you” of the internet. But signatures are also where many organizations underestimate complexity: certificate formats, HSM support, firmware signing, code signing pipelines, and third-party validation logic. A signature algorithm can be mathematically excellent and still operationally painful.

The smartest move is to stop thinking in single algorithms and start thinking in resilience. NIST’s decision to standardize an additional, different encryption approach as a backup is a signal: diversity matters. In practice, that means designing systems that can carry multiple algorithms and rotate them without downtime.

PQC adoption is therefore a maturity test: do you have a cryptographic bill of materials, protocol agility, and a controlled rollout path? If yes, PQC is just the next upgrade. If not, it becomes a fire drill.



Key Establishment
ML-KEM (FIPS 203)
Hybrid-ready (TLS/VPN)

Digital Signatures:
ML-DSA (FIPS 204)
SLH-DSA (FIPS 205)
Certificates / Code Signing / Firmware

Symmetric Cyrpto
(mostly unchanged)
AES / symmetric remains

Diversity Track
HQC (additional KEM)

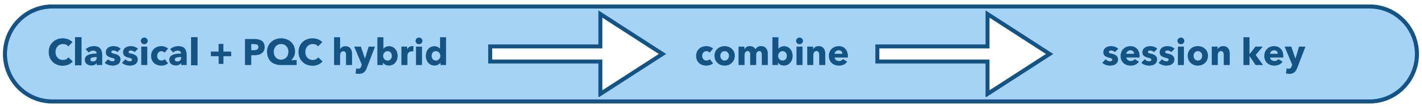
Hybrid by Design: How the Internet Is Actually Transitioning

The internet cannot afford a “flag day” security upgrade. TLS sits under everything—payments, healthcare, identity, cloud APIs—and anything that breaks TLS breaks business. That’s why the transition path is not a clean replacement, but a safer overlap: hybrid key exchange.

In a hybrid TLS handshake, you run a classical exchange alongside a post-quantum key encapsulation mechanism (KEM) and then combine the outputs into one session secret. The design goal is brutally practical: if a post-quantum primitive ever needs to be swapped or tightened, classical security still holds; if quantum capability matures, the post-quantum component carries the session. Hybrid isn’t elegant—it’s resilient, deployable, and engineered for uncertainty.

And it’s not theoretical anymore. Major browsers and edge networks have already shipped post-quantum hybrids by default, and that rollout surfaced something more valuable than a benchmark: it exposed the real internet. Middleboxes, TLS inspection appliances, and legacy network controls that silently interfere with modern handshakes became visible overnight. That friction is the point—because “works in the lab” is meaningless when production networks are full of brittle intermediaries and hidden dependencies.

The strongest proof of momentum is scale. When an edge network reports that a majority of human-initiated traffic is already protected with post-quantum encryption, it marks a shift from pilot to baseline. PQC is no longer just a government roadmap item; it’s moving into the default posture of the consumer internet.



Classical + PQC hybrid → **combine** → **session key**

Strategic Outlook:

- **Hybrid reduces migration risk while standards mature**
- **Start where rollback is easy: TLS termination and gateways**
- **Plan signatures as a multi-year trust program**

Executive rule: deploy hybrid at the edge first, then rebuild trust with PQ signatures

PKI Under Pressure: The 2026 Certificate Shockwave

Most PQC roadmaps focus on algorithms. The next operational shock is less glamorous: certificate lifetimes. Public-trust PKI is moving toward dramatically shorter validity windows, and the step changes begin in 2026. That means more frequent issuance, more automation, and far less tolerance for manual processes.

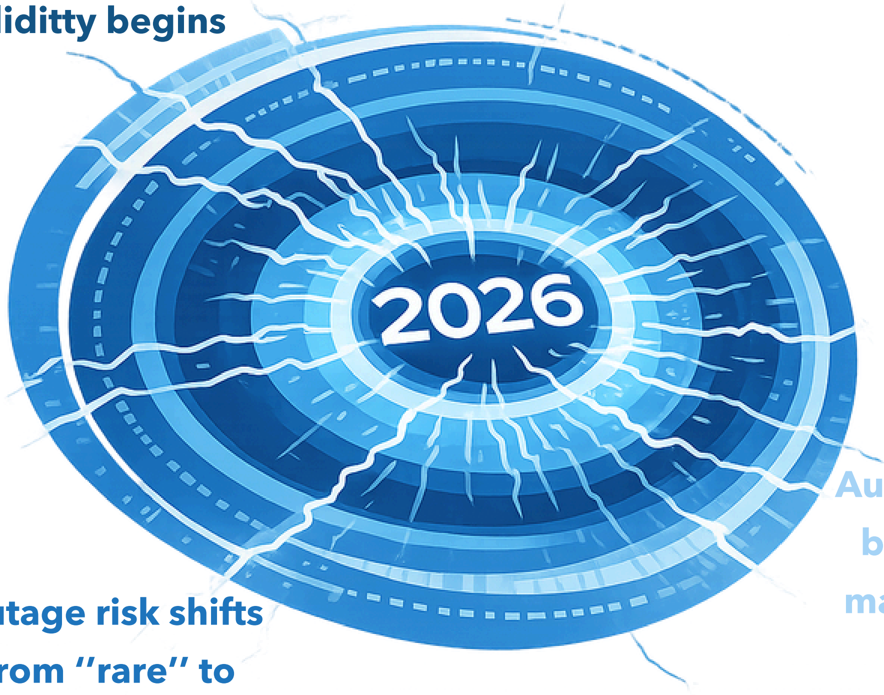
Why does this matter for PQC? Because automation is the missing prerequisite. If your certificate lifecycle is fully automated—issuance, renewal, deployment, rollback—you suddenly gain the ability to rotate crypto primitives with similar discipline. Short lifetimes force the modernization that PQC needs anyway.

There's also a deeper reason. PQC signatures can increase computational and bandwidth overhead in some contexts. Even if you keep today's classical signatures in the short term, your PKI will have to evolve to support hybrid worlds: mixed chains, dual validation logic, and updated libraries across clients and servers.

This is where organizations get blindsided. They treat PKI as a back-office function, until it becomes a frontline reliability issue. In a world of shorter lifetimes, outages are often self-inflicted: failed renewals, misconfigured ACME flows, brittle certificate pinning, outdated appliances.

Use the 2026 certificate pressure as a forcing function. Modernize your certificate management first—inventory, automation, deployment pipelines—and you create the runway for PQC adoption. Do it the other way around and PQC becomes harder than it needs to be.

200-day max validitty begins



Automation becomes mandatory

Outage risk shifts from “rare” to “routine”

Who is Shipping PQC: The Race to Own the Default Layer

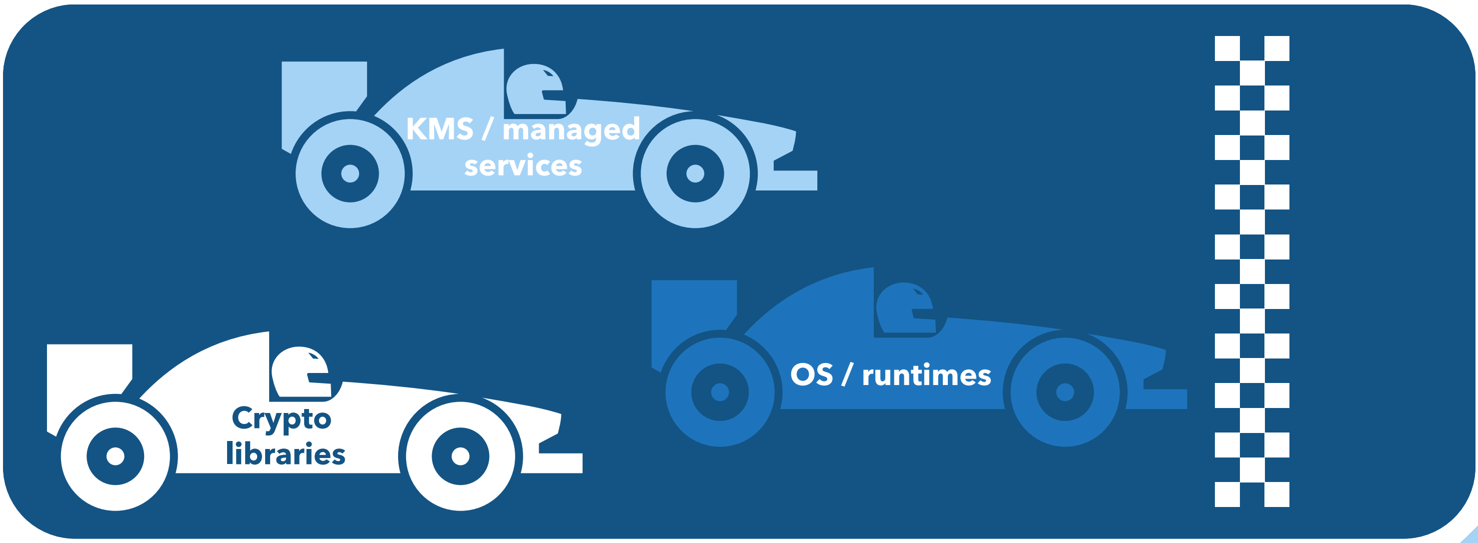
PQC isn't being won by the loudest conference keynote. It's being won by whoever quietly becomes the default layer: the OS APIs developers call, the cloud primitives enterprises consume, the libraries embedded in everything.

Three moves define the new provider landscape. First, platform vendors are pushing PQC into foundational APIs—so application teams can adopt without writing cryptography. Second, cloud providers are exposing quantum-safe key encapsulation mechanisms in managed services, encouraging hybrid patterns as the safe default. Third, the open-source ecosystem is wiring PQC into ubiquitous crypto libraries—because if OpenSSL supports it cleanly, the world follows.

For buyers, this changes procurement. "Do you support PQC?" is a weak question. Strong questions are operational: Do you support hybrid TLS at scale? Can your KMS generate and unwrap with hybrid KEMs? Do your HSMs and code-signing flows support PQC roadmaps? Can you inventory crypto usage across services? Can you rotate algorithms without re-architecting?

The provider market will look noisy—lots of announcements, uneven maturity. Your job is to separate demo features from production posture. Prefer vendors who show full-stack thinking: crypto agility, secure defaults, interoperability, and clear migration guidance.

Bottom line: PQC will be adopted the same way cloud was adopted—through primitives that make the secure path the easy path. Align with platforms that lower friction, and you convert a multi-year risk into a manageable rollout.



A Migration That Actually Works: The Enterprise Playbook

PQC migration doesn’t fail in cryptography—it fails in execution.

PQC succeeds when it stops being a crypto project and becomes a business resilience program. The hardest part isn’t choosing algorithms; it’s discovering where cryptography lives and how deeply it is embedded across products, vendors, and day-to-day operations.

Phase 1 – Discover & Prioritize.

You need a cryptographic inventory that is honest:
protocols in use, key sizes, certificates, libraries, hardcoded dependencies, and long-lived data flows. Migration guidance converges on one point: prioritize key establishment and transport early, because it directly reduces harvest-now, decrypt-later risk.

Phase 2 – Deploy Under Control.

Start with hybrid TLS where failure is survivable: external-facing systems and critical service-to-service lanes. Validate performance, compatibility, and monitoring before you expand to VPN gateways, APIs, and cross-border links. In parallel, modernize PKI automation—because certificate lifecycles and signature transitions are where many rollouts quietly die.

Phase 3 – Harden Trust Roots.

Code signing, firmware signing, device identities, and update infrastructure must be evaluated for PQC readiness—especially in long-lived assets (industrial, medical, infrastructure). This is where supply chain maturity shows: if key vendors cannot provide crypto agility, you inherit their constraints and risk.

Start where rollback is easy. Finish where trust is foundational.

Phase 4 – Govern Like Reliability.

Assign ownership, define an architecture standard, and treat PQC changes like any major reliability change: staged rollouts, canaries, rollback plans, and metrics. If you wait for perfect certainty, you lose control. If you build agility, uncertainty becomes manageable.

Beyond PQC: QKD, QRNGs, and the Quantum-Safe Portfolio

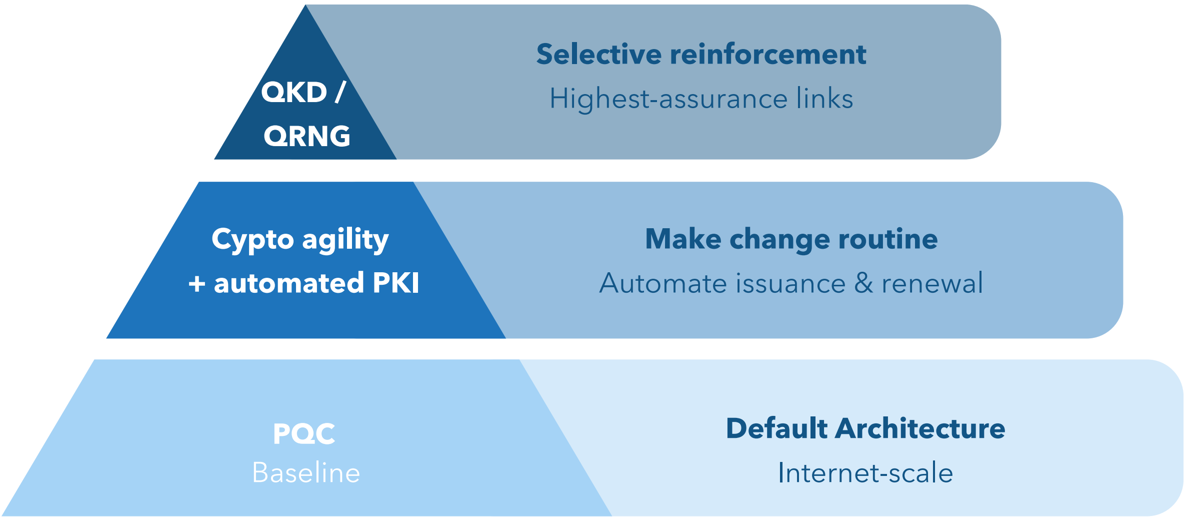
Post-quantum cryptography will be the global baseline. But baseline is not the same as maximum assurance. The organizations with the highest security demands—critical infrastructure, defense supply chains, sovereign networks—are building a portfolio approach: PQC as the default, and specialized quantum technologies as layered reinforcement where it matters.

Quantum Key Distribution (QKD) is often misunderstood as a replacement for public-key cryptography. It isn't. QKD is a complementary tool that can strengthen specific high-security environments by providing different trust assumptions—especially when combined with modern symmetric encryption and strong operational controls. The key word is "specific": QKD has deployment constraints, and it must be engineered carefully to avoid side channels and implementation pitfalls.

That's why standards and interoperability work matter. If quantum communication networks cannot interoperate safely, they don't scale beyond pilots. Meanwhile, quantum random number generation (QRNG) can strengthen entropy quality in security architectures—again as a complement, not a miracle.

For most enterprises, the near-term winning architecture is simpler: hybrid PQC for transport, PQC signatures for trust chains, automated PKI, and a disciplined migration program. The strategic signal for 2026 is coordination: public-sector roadmaps mature, certificate lifetimes compress, and ecosystem policy (including the EU's quantum strategy and the upcoming Quantum Act) accelerates industrial alignment.

The future will reward a specific capability: the ability to rotate trust at speed. PQC is the first major test of that capability. Passing it turns quantum risk into competitive advantage.



Expert View - Harald A. Summa

Post-Quantum Security Is a Leadership Decision, Not a Late IT Upgrade

For years, post-quantum security was treated as a future topic—important, but not urgent. That is no longer the case. With standards maturing, infrastructure cycles accelerating, and geopolitical risk increasing, post-quantum readiness is becoming a present-day leadership issue.

This transition should not be reduced to an algorithm debate. The key strategic question is whether organizations can build the capabilities required to adapt securely over time: crypto agility, operational discipline, and governance that connects security decisions to business continuity.

Post-quantum security also has a broader dimension. It affects trust in digital infrastructure, resilience across critical systems, and ultimately the ability of institutions and companies to operate with confidence in an increasingly contested digital environment. In this sense, it is not only a technical upgrade—it is part of digital sovereignty.

For 2026, the priority is clear: move post-quantum security out of the expert niche and into executive ownership. Define a migration logic, align internal teams and vendors around interoperability, and treat cryptographic modernization as a long-term reliability program.
Organizations that act early will do more than reduce risk. They will build trust, resilience, and strategic freedom.

Expert View - Matthias Reidans

Post-Quantum Readiness Is an Architechture Problem

Post-quantum readiness is often framed as a cryptography upgrade. In practice, it is an architecture and operations challenge. The hardest part is not selecting algorithms, but identifying where cryptography is embedded across protocols, applications, certificates, devices, and long-lived data flows—and then modernizing these layers without disrupting operations.

This is why migration should begin with structure, not tools. Organizations need a realistic cryptographic inventory, clear priorities, and a transition model that can absorb change. In most environments, that means starting with hybrid approaches in transport and key establishment, while preparing PKI and certificate lifecycle automation for a more dynamic future.

PQC is not a single replacement event. Enterprises will operate mixed environments for years: classical and post-quantum mechanisms, legacy systems and modern infrastructure. The winning strategy is not perfection, but controlled interoperability.

From a technical strategy perspective, the key capability is crypto agility: the ability to rotate algorithms, update trust mechanisms, and maintain resilience as standards and implementations evolve. That is what turns uncertainty into a manageable engineering problem.