

Preparing Enterprise Cybersecurity for the Quantum Era

A practical framework for post-quantum cryptography discovery, prioritization and migration

Quantum cybersecurity is not one technology or one project. The principal enterprise action is to understand where public-key cryptography protects valuable information and plan a managed transition to standardized post-quantum cryptography (PQC). This paper sets out an inventory-led, risk-prioritized migration approach, clarifies the distinct role of quantum security research and describes the current boundaries of the Quantum Use Case Studio.

APPLICATION

Quantum Use Case Studio

<https://quantum-use-case-studio.pages.dev/>

Version 1.0 | 21 October 2026

Decision-support research. Verify technical, security, legal and supplier requirements before acting.

Contents

Executive summary

1. What quantum cybersecurity means
2. The migration challenge is an inventory problem
3. Prioritize using risk and lead time
4. A phased PQC migration
5. Engineering principles for safer transition
6. Quantum security research is a separate track
7. Governance and measures
8. What the Quantum Use Case Studio supports today

Conclusion

References

Executive summary

A future cryptographically relevant quantum computer could threaten widely used public-key cryptography. Organizations do not need to predict its arrival date to begin useful work. They can identify cryptographic dependencies, prioritize data and systems, engage suppliers, design for change and build a sequenced migration plan.

- Treat PQC migration as an enterprise architecture and service continuity program, not only an algorithm upgrade.
- Inventory where cryptography is used and which services, vendors and data flows depend on it.
- Prioritize by information lifetime, business criticality, exposure, dependency reach and migration lead time.
- Use standards and current product support validated for the actual deployment; test interoperability and performance.
- Separate software-based PQC migration from quantum key distribution and from experimental quantum security research.

The first control is visibility. An organization cannot prioritize, budget or safely migrate cryptography it has not found.

NIST has finalized three PQC standards: FIPS 203 for ML-KEM key establishment, FIPS 204 for ML-DSA signatures and FIPS 205 for SLH-DSA signatures [1]. NIST's NCCoE migration project centers on cryptographic visibility and risk management alongside interoperability and benchmarking [2]. The European Commission's roadmap asks EU Member States to start the transition by the end of 2026 and to prioritize high-risk cases no later than the end of 2030; this is coordinated public-sector guidance, not a blanket deadline imposed on every private company [3].

1. What quantum cybersecurity means

Quantum cybersecurity spans at least three distinct domains. First is protecting existing information and trust systems against future quantum-enabled cryptanalysis. Second is using quantum technologies in security contexts, such as quantum key distribution or quantum random-number generation, where operational and threat-model questions must be assessed. Third is security of quantum computing platforms and their supply chains. A governance program should name which domain it is addressing.

PQC is the near-term cryptographic migration focus in this paper. It consists of cryptographic algorithms designed to resist attacks by both classical and quantum computers and can be implemented in conventional computing and communications infrastructure. It is not quantum hardware. QKD is a different approach that relies on quantum communication capabilities and specialized endpoints, links and operating assumptions; it does not replace the need to review endpoint security, authentication, key management or broader cryptographic dependencies.

A sufficiently capable quantum computer could affect some public-key methods used for key establishment and digital signatures. The timing and capabilities of such a machine are uncertain. Long confidentiality lifetimes and long system replacement cycles can nevertheless make advance planning rational. Risk framing should avoid claiming that all encryption is immediately broken or that every organization faces the same urgency [4].

2. The migration challenge is an inventory problem

Cryptography is embedded in applications, identity systems, networks, devices, libraries, cloud services, code-signing pipelines, certificates, firmware and supplier products. It may be configured centrally, buried in dependencies or implemented in equipment with long replacement cycles. A contract-level list of algorithms is not enough; teams need to connect cryptographic use to systems, data, owners and operational impact.

Inventory field	Why it matters
System, service and owner	Establishes accountability, business criticality and remediation path.
Algorithm, protocol and function	Shows whether cryptography supports key establishment, signatures, authentication, encryption or integrity.
Library, module, appliance and version	Makes product support, patchability, validation and supplier dependency visible.
Data sensitivity and required secrecy lifetime	Helps prioritize information that must remain confidential for years.
Network path, endpoint and trust dependencies	Identifies where one service relies on another for identity, certificates or key establishment.
Location, supplier, contract and regulatory context	Supports jurisdictional review, procurement planning and evidence collection.
Replacement effort and outage tolerance	Informs sequencing, test design, budget and continuity planning.

NIST's NCCoE describes a cryptographic inventory as a record of algorithms, protocols, keys and certificates, systems and dependent applications, and data protected by cryptography. The inventory should describe key metadata without collecting key material [2]. Discovery tools can help, but automated findings need owner confirmation and must be paired with architecture, procurement and supplier records.

3. Prioritize using risk and lead time

A practical prioritization model combines several dimensions rather than treating every RSA or elliptic-curve reference equally. Consider (a) data confidentiality lifetime, (b) value and impact if exposed, (c) public-key cryptographic exposure and external accessibility, (d) number and criticality of dependent systems, (e) migration and supplier lead time, (f) operational replacement windows and (g) compliance or national guidance relevant to the service.

"Harvest now, decrypt later" is one reason to act before a cryptographically relevant quantum computer exists: information collected today could retain value into a future period when cryptanalysis becomes more capable. This concern is most relevant where sensitive information must remain confidential for a long time. NIST recommends inventorying systems that use cryptography and planning transition to its finalized standards [4].

- Start with high-impact external-facing services and long-lived sensitive information.
- Identify identity, certificate, key-establishment and code-signing dependencies with broad blast radius.
- Prioritize assets with long procurement, firmware, certification or replacement cycles.
- Record assumptions and confidence; unknown is a discovery task, not evidence of low risk.
- Coordinate across security, architecture, infrastructure, application owners, procurement, legal and suppliers.

4. A phased PQC migration

Phase	Core activities	Evidence to exit the phase
1 Mobilize	Assign executive sponsor and program owner; define scope, governance, target reporting and procurement engagement.	Named owners, decision forum, scope and funded discovery plan.
2 Discover	Combine software and network discovery, architecture review, supplier questionnaires, CBOM and system owner validation.	Prioritized inventory with ownership, confidence and dependencies.
3 Prioritize	Map data lifetimes, exposure, business impact, replacement cycles, jurisdiction and supplier readiness.	Risk-ranked backlog, sequencing rationale and risk acceptance process.
4 Design and pilot	Select standards-based implementations; test interoperability, performance, certificates, protocols, key management and rollback.	Approved architecture, representative test results, rollback and operational runbooks.
5 Migrate	Coordinate product upgrades, endpoint changes, certificates, application releases, customer and partner testing.	Production evidence, control validation, exceptions and updated inventory.
6 Sustain	Monitor standards, vulnerabilities, supplier roadmaps and crypto agility; repeat discovery and track residual risk.	Continuous inventory, change triggers, periodic assurance and metrics.

NIST's migration work explicitly covers cryptographic visibility and risk management as well as interoperability and benchmarking [2]. EU coordination adds a cross-border dimension: organizations serving public utilities or operating across Member States should monitor applicable national implementation guidance and sector-specific requirements [3]. The EU roadmap itself is not a substitute for legal advice or national competent-authority direction.

5. Engineering principles for safer transition

Crypto agility

NIST defines crypto agility as the ability to adapt and replace cryptographic algorithms across protocols, applications, software, hardware and infrastructure without disrupting running systems [5]. In practice, this requires abstraction boundaries, supported configuration, lifecycle management, inventory updates, test coverage and change ownership. Agility is not an excuse to leave deprecated methods indefinitely enabled; measure both the ability to change and the completion of change.

Interoperability and performance

PQC can change key, signature and certificate sizes, handshake behavior, memory use and network traffic. Benchmark representative hardware and protocols; test middleboxes, constrained devices, certificate chains, update channels, latency, throughput and failure handling. Verify algorithm identifiers, implementation versions, validation status and supported operating modes with each vendor. Avoid selecting products based on a generic “quantum-safe” label.

Hybrid approaches and cryptographic boundaries

Hybrid key establishment may combine conventional and post-quantum components during transition, but the exact construction, protocol profile, standards status and validation requirements matter. Do not assume that combining algorithms automatically yields a secure or compliant system. Use current NIST and applicable sector guidance and test end-to-end interoperability.

6. Quantum security research is a separate track

Organizations may explore QKD, quantum random-number generation, quantum sensors for security, or quantum-inspired security analytics. These are research or deployment decisions with their own threat models, performance criteria, operational prerequisites and assurance needs. They do not replace a PQC inventory or migration plan.

Track	Primary question	Decision evidence
PQC migration	Where are classical public-key mechanisms used, and how should systems transition?	Cryptographic inventory, standards mapping, validated implementation, interoperability and rollout evidence.
Quantum key distribution	Does a specific link and use case justify a quantum communication system?	Threat model, endpoint authentication, network topology, availability, cost, operational controls and comparison with alternatives.
Quantum random-number generation	Does the source meet the randomness, assurance and integration needs of the system?	Validated entropy assessment, implementation assurance, health tests, certification requirements and failure behavior.
Quantum platform security	How are access, workloads, dependencies, cloud control plane and sensitive data protected?	Supplier assurance, identity and access controls, isolation, logging, data paths, incident response and contract evidence.

7. Governance and measures

A migration program should be owned as a cross-enterprise change portfolio. The CISO or designated security executive sets risk appetite and escalation; enterprise architecture maps dependencies; cryptography specialists define standards; product owners plan changes; procurement and legal manage supplier commitments; risk and audit challenge evidence. Sensitive or regulated systems retain their existing approval and control processes.

- Inventory coverage: proportion of in-scope critical services with validated owner and cryptographic dependencies.
- Prioritization quality: high-risk assets with a documented rationale, data lifetime and planned treatment.
- Supplier readiness: products and contracts with confirmed PQC roadmaps and tested support.

- Migration execution: systems upgraded, exceptions accepted, rollback tested and dependencies closed.
- Crypto agility: time and effort to replace an algorithm or provider in representative systems.
- Residual exposure: unresolved high-risk dependencies, target dates and accountable decision makers.

Do not report “quantum safe” as a binary state without scope, algorithm, implementation, validation, protocol and date. Report the evidence and gaps that support each claim.

8. What the Quantum Use Case Studio supports today

The Studio includes a separate high-level cybersecurity workspace for recording selected cryptographic inventory indicators, data sensitivity and lifetime, dependencies, an owner and notes. It distinguishes PQC migration planning from quantum security research. Its purpose is to help structure an initial conversation and preserve a local triage record.

The current prototype does not scan code or networks, discover cryptography automatically, verify standards compliance, validate implementations, calculate security risk, connect to supplier systems or execute cryptographic migrations.

The Studio runs in the browser and saves its records in local browser storage on the current device. It has no account system, tenant isolation, server-side database, encryption service or enterprise audit log. Do not enter personal, regulated, confidential, classified or secret information. Use qualified security and cryptography specialists for implementation decisions.

Potential future product extensions could include controlled cryptographic bill-of-materials imports, integrations with discovery tooling, supplier evidence tracking, migration workflow and reporting. These ideas are roadmap possibilities, not current product functionality.

Conclusion

Quantum-era cybersecurity is an information, architecture and change-management challenge. Start with visibility, prioritize systems according to risk and lead time, use finalized and applicable standards, test interoperability and keep the inventory current. PQC migration is a practical workstream today; quantum security research can proceed alongside it without being confused with it.

Explore the Quantum Use Case Studio: <https://quantum-use-case-studio.pages.dev/>

References

- [1] NIST. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204 Module-Lattice-Based Digital Signature Standard; FIPS 205 Stateless Hash-Based Digital Signature Standard. Published 13 August 2024. [Source](#)
- [2] NIST National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography project and FAQ. [Source](#)
- [3] European Commission. Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Published 23 June 2025; see also the Commission PQC policy overview. [Source](#)
- [4] NIST. What Is Post-Quantum Cryptography? [Source](#)
- [5] NIST Computer Security Resource Center. Crypto Agility. [Source](#)
- [6] European Commission. Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a coordinated implementation roadmap for the transition to PQC. [Source](#)