2030 and Beyond: Preparing for PQC Migration

Version: 1.0

Date: October 2025

Publisher: ThotQuantum Insights

Classification: Public

Status: Draft

1. Executive Summary

Quantum computing represents one of the most disruptive technological evolutions of our generation.
While it promises enormous benefits in materials science, AI, and optimization, it simultaneously poses a direct and existential threat to modern encryption.

According to the U.S. National Institute of Standards and Technology (NIST), current asymmetric algorithms such as **RSA** and **Elliptic Curve Cryptography (ECC)** will be deprecated after 2030 and disallowed after 2035. This timeline marks the end of classical cryptography as we know it - and the start of a global race toward post-quantum cryptography (PQC).

Enterprises relying on today's encryption standards risk long-term data exposure due to *"Harvest Now, Decrypt Later"* attacks: adversaries are already collecting encrypted data today with the intent to decrypt it once quantum computers reach practical scale.

ThotQuantum's mission is to make this transition both practical and secure. As a European cybersecurity innovator, we are developing quantum-resistant Data encryption-as-a-Service designed to protect critical information well beyond the quantum threshold.

2. The Quantum Threat Landscape

The progress in quantum computing has accelerated faster than traditional risk models predicted.
Recent breakthroughs in quantum error correction and modular architectures demonstrate that **2048-bit RSA and 256-bit ECC could be broken within the next decade** once stable quantum processors reach maturity.

NIST's **Post-Quantum Cryptography (PQC)** initiative, culminating in **NIST IR 8547**, establishes a global migration framework.
It defines two critical milestones:

- **2030** - Deprecation of classical RSA and ECC algorithms.
- **2035** - Mandatory disallowance of non-PQC algorithms for critical systems.

For organizations managing sensitive data with long confidentiality lifetimes - such as healthcare records, legal archives, or defence communications - this timeline means that data encrypted today may already be vulnerable tomorrow.

The *Harvest Now, Decrypt Later* strategy exploits this gap: attackers capture ciphertext today, store it, and wait until quantum computers can decrypt it instantly. Once that happens, decades of encrypted data could become transparent in seconds.

The race to quantum-safe encryption is therefore not theoretical - it has already begun.

3. Impact on Existing Cryptographic Systems

Today's digital trust relies on asymmetric cryptography:

- **RSA** underpins most certificate authorities and secure email.
- **ECC** (including ECDH and EdDSA) powers TLS 1.3, mobile security, and blockchain systems.
- **PKI** infrastructures depend on these algorithms for identity validation and signature integrity.

When quantum computers achieve sufficient qubit stability, **Shor's algorithm** will render both RSA and ECC obsolete, breaking their mathematical foundations.
This will invalidate most digital signatures, disrupt TLS sessions, and compromise long-term encrypted storage.

For enterprises, this is not just a cryptographic risk - it's a **business continuity and compliance threat**.
Regulated sectors such as finance, government, and healthcare will face mandatory cryptographic upgrades to maintain compliance with **ISO-27001**, **NIS2**, and emerging **EU Cyber Resilience Act** standards.

The window for secure migration is closing. Enterprises must start modernizing now to avoid operational and reputational disruption.

4. ThotQuantum's Migration Framework

ThotQuantum is developing a pragmatic, standards-aligned approach to post-quantum readiness.
Our Migration Framework provides a step-by-step pathway that integrates smoothly with existing enterprise infrastructures.

Step 1 - Assessment

Conduct a full inventory of encryption assets, keys, certificates, and data lifecycles. Identify critical systems using vulnerable algorithms (RSA, ECC) and determine confidentiality lifetimes.

Step 2 - Hybrid Transition

Deploy ThotQuantum's **Hybrid Encryption Model**, combining **Elliptic-Curve (EC)** communication with **ML-KEM (Kyber)** key encapsulation - the NIST-standardized lattice-based algorithm.
This dual-layer (double wrapping) approach ensures both **immediate backward compatibility** and **future-proof security**.

Data is symmetrically encrypted using **AES-256-GCM**, with hybrid-derived keys combining classical and post-quantum entropy via HKDF derivation.

Step 3 - Full PQC Adoption

As PQC implementations mature, transition fully to NIST-certified post-quantum algorithms (Kyber, Dilithium, Falcon).
ThotQuantum's infrastructure supports **cryptographic agility**, allowing algorithm replacement without redesigning the security architecture.

Our EaaS platform integrates with **Vault, Kubernetes, and Keycloak**, ensuring seamless DevSecOps adoption and compliance with zero-trust principles.

5. Recommendations for Enterprises

1. Prioritize Cryptographic Inventory
   - Document all encryption algorithms, key lengths, and data lifetimes.
   - Identify assets requiring long-term confidentiality (10+ years).

2. **Begin Testing Hybrid Endpoints Early**
    - Pilot hybrid EC + ML-KEM configurations in internal systems.
    - Ensure interoperability with existing TLS and PKI frameworks.
3. **Align with Compliance Standards**
    - Integrate PQC readiness into your **ISO-27001 Information Security Management System (ISMS)**.
    - Follow **ENISA** and **NIS2** guidance for quantum migration.
4. **Adopt Cryptographic Agility**
    - Design systems capable of algorithm substitution without downtime.
    - Use modular architectures that support post-quantum key exchange.
5. **Engage with Trusted Innovators**
    - Partner with providers like ThotQuantum for enterprise-grade, compliant PQC solutions.
    - Participate in industry readiness pilots and standardization initiatives.

6. Conclusion - The Countdown to 2030

The quantum transition is not a future event - it is an unfolding reality.
By 2030, the cryptographic standards that secured the digital economy for decades will be deprecated.
Enterprises that begin preparation today will gain resilience, compliance, and competitive advantage in a post-quantum world.

ThotQuantum's 2026 Startup Initiative focuses on scaling R&D and securing strategic investment to expand our Data encryption-as-a-Service platform globally. This milestone supports our mission to deliver **European-engineered, quantum-safe encryption infrastructure** aligned with ISO-27001 and NIST PQC standards.

The quantum era redefines trust.
Enterprises must evolve before the algorithms that protect them expire.