Charter of Trust

Decrypting the Future: Global Timelines for Post-Quantum Cryptography and why they matter

Publication date: 07 April 2026

Contributors:

- Allianz SE
- Atos Group
- Robert Bosch GmbH
- Danfoss
- IBM
- Infineon Technologies AG
- Microsoft Cooperation
- Mitsubishi Heavy Industries
- Siemens AG
- TÜV SÜD AG
- Zscaler

Charter of Trust – PQC Working Group

Classification: CoT Public

Table of Contents

The Charter of Trust: Our Mission

Amidst an increasingly severe and complex threat landscape, the Charter of Trust (CoT) was established at the Munich Security Conference on 16 February 2018 as a non-profit alliance of leading global companies and organizations. Since then, a continuously evolving group of members and partners work together across sectors to strengthen cybersecurity, cultivate digital trust and make the digital world of tomorrow a safer place. Today, our initiative consists of 12 Partners and 17 Associated Partners operating in nearly 170 countries across five continents and representing more than 1.8 million employees.

Figure 1: CoT across the globe

The following publication is issued by the **Charter of Trust Working Group on Emerging Technologies**. Its mission is to address and provide guidance to businesses on how to manage the cybersecurity risks triggered by AI and Quantum Computing.

In November 2025, the Charter of Trust published its Post-Quantum Cryptography Ambition, re-affirming its commitment to a proactive, well-coordinated, and risk-driven transition to post-quantum cryptography.

The present publication is a step into supporting such a transition, nourished by the Charter of Trust's partners knowledge, experience and practice related to global developments and impacts of PQC.

1. Introduction

Quantum computing poses a fundamental long-term challenge to today's cryptographic foundations. While cryptographically relevant quantum computers are not yet available, the risk of future decryption of data captured today ("harvest now, decrypt later") means **business leaders, risk owners, and strategy decision-makers** must prepare well in advance.

This paper is written for responsible management of long-lived data, systems, and digital trust. It is not a technical specification for cryptographic implementation. Instead, it provides a **strategic view of post-quantum cryptography (PQC) readiness and migration**.

The focus is on **preparedness, governance, and migration**, including crypto-agility, protocol-level impacts, and supply-chain dependencies. Detailed algorithm design is out of scope. By framing PQC as a strategic transformation rather than a purely technical change, this paper supports informed decision-making across sectors and regions.

First, the paper identifies four priority domains for post-quantum cryptographic (PQC) upgrades: financial services, government and defense, operational technology, and healthcare.

These sectors store highly sensitive data and operate systems with long life cycles, making them particularly exposed to quantum-related risks. The paper then outlines the current quantum landscape, including the technical foundations of PQC, the threats posed by quantum computing, expected development timelines, and potential attack scenarios.

Building on this context, it provides a brief comparative overview of national and regional PQC transition timelines, highlighting how governments across different regions are beginning to structure the shift toward quantum-resistant cryptography. Finally, drawing on existing national frameworks and guidance documents, the paper synthesizes common migration steps and presents practical, phased implementation guidance for organizations beginning or structuring their PQC transition. It concludes by summarizing the key findings and draws together the implications for organizations preparing for the transition to post-quantum cryptography.

The purpose of this paper is to outline the **business and systemic risks** associated with quantum-vulnerable cryptography and compare **global regulatory and policy timelines** shaping PQC adoption.

2. Sectoral Prioritization & Use Cases

While each national or regional government has a different approach and timeline to PQC transition (as we see in chapter 4), certain business sectors are more exposed to quantum computing risks and should be prioritized for migration.

The following section clarifies the rationale for sectoral prioritization, outlines the assets requiring the most stringent, long-term protection, and aligns PQC algorithm primitives with distinct sectoral needs as guided by current US NIST standards (as of August 2025 – FIPS 203/204/205) and global best practices.

The emergence of quantum computing introduces transformative, strategic, long-term risks to the confidentiality and integrity of digital systems across all sectors. Adversaries may already be harvesting encrypted data for later decryption. Though PQC transition is not mandatory for all sectors yet, a sector-wide PQC adoption, following leading standards (notably NIST FIPS 203/204/205, 2025), is pivotal for national, economic, and public health security.

Based on sector characteristics, data retention obligations, and system lifecycles, the following four domains exhibit the highest priority for post-quantum cryptographic (PQC) resilience.

2.1 Four domains of highest priority for PQC resilience

Financial services

Financial services require immediate PQC prioritization due to long-standing data retention and confidentiality obligations. Transaction records, audit logs, and customer identity credentials must be protected for decades to enable regulatory compliance, fraud investigation, and systemic accountability. The threat of “harvest now, decrypt later” makes this sector acutely vulnerable.

Sector infrastructure including payment rails, settlement networks, and authentication systems evolve slowly, with operational life cycles that commonly extend over a decade. As these systems are deeply interconnected, any cryptographic compromise can propagate rapidly across institutions and geographies, threatening economic stability.

Government and Defense

Governmental and defense entities manage some of society’s most enduringly sensitive data, from classified intelligence to diplomatic exchanges and national archives, with confidentiality requirements lasting for decades or longer. Many critical hardware platforms, such as military communication systems, satellites, and embedded defense technologies, also have operational lifespans of 20 to 40 years, making cryptographic retrofitting both complex and protracted.

Given governments’ roles in setting standards and procurement requirements, early PQC adoption in public-sector organizations serves both as a security imperative and a catalyst for sector-wide acceleration.

Operational Technology

Critical infrastructure sectors, including energy, utilities, transportation, and manufacturing rely on operational technologies designed for 10 to 20 years (or more) in deployment lifetimes. These environments depend on cryptographic protection for control systems and field devices that are not easily upgradable after deployment.

Compromising these systems could result in data breaches, disruption of essential public services, physical safety hazards, and cascading operational failures. PQC-based resilience is a prerequisite for maintaining societal continuity.

Healthcare

The healthcare sector faces dual imperatives: protecting sensitive patient data and ensuring the reliable operation of life-critical devices. Healthcare data (e.g., electronic health records, diagnostic images, genetic data) usually require confidentiality well beyond typical retention periods, with many records stored for a lifetime. “Harvest now, decrypt later” exposure is acute: data stolen in 2025 may still be sensitive in 2050.

Devices and hospital technologies may be operational for 20 years or longer, amplifying the risk of quantum-vulnerable cryptography being embedded for a device’s entire service life. PQC-readiness has rapidly transitioned from best practice to regulatory expectations and patient safety imperatives.

The consequences of cryptographic compromise in healthcare are not limited to privacy loss: they directly affect patient safety, care continuity, and regulatory compliance, elevating the sector’s criticality in the context of quantum preparedness. PQC deployment in healthcare is recommended to focus on immediate device procurement standards, retrofitting critical hospital infrastructure, and upgrading all workflows involving long-lived records.

PQC sector prioritization is based on:

- The enduring sensitivity of processed or retained data,
- The operational lifecycle and upgradability of supporting systems,
- And the potential impact of cryptographic failures on national, economic, or public safety interests.

Quantum risk peaks where the required data confidentiality or system reliability horizon extends beyond the anticipated arrival of large-scale quantum computing. The following tables summarize the categories of assets most dependent on long-term cryptographic protection for each of the high priority sectors.

2.2 Assets most dependent on long-term cryptographic protection

Financial Services

Asset Category	Examples	Protection Requirement
Long-lived data	Transaction histories, customer identity records, audit trails	Multi-decade confidentiality and integrity
Long-lived systems	Payment and settlement platforms, authentication services	Operational integrity across 10+ years
Archival and backup assets	Encrypted backups, compliance archives	Regulatory and forensic retention over decades

Government and Defense

Asset Category	Examples	Protection Requirement
Sensitive data	Classified intelligence, diplomatic exchanges, national archives	Multi-decade to indefinite confidentiality
Long-lived systems	Military communications, satellite systems, secured embedded platforms	Secure operation over 20 to 40 years
Permanent records	Legal documents, policy archives	Integrity preservation over indefinite timespans

Operational Technology

Asset Category	Examples	Protection Requirement
Operational data	Grid telemetry, safety logs, maintenance records	Long-term integrity and availability
Long-lived devices and systems	SCADA systems, industrial controllers, transportation signaling	Secure operation for 10–20 years
Archival assets	Operational backups, historical performance data	Multi-year storage for compliance and recovery

Healthcare

Asset Category	Examples	Protection Requirement
Patient data records	Electronic health records, medical images, genetic/genomic data	Lifetime (multi-decade) confidentiality and integrity
Long-lived devices and systems	Implantable and hospital devices, radiology, and diagnostic equipment	Reliable secure operation for 10 to 20+ years
Archival and backup assets	Encrypted health record backups, research datasets	Retention for regulatory and care continuity over decades

A more detailed overview of PQC Use Cases and Sector Alignment is provided in the Annex.

3. The Quantum State of Play

Cryptography is foundational in cybersecurity and a key part of secure communications, ensuring their content is not intercepted involuntarily. With the expected development in quantum computing, this security is at risk. As it is essential to understand the Quantum State of Play, this section outlines the technical aspects of PQC, then the posed threats, the expected time horizon, current technical solutions and attack scenarios.

3.1 Quantum State of Play

Several upcoming quantum technologies can bring advantages in multiple fields:

- Future Quantum Computers could potentially accelerate certain categories of calculations despite several caveats.
    - The actual list of use cases (quantum-based simulations, artificial intelligence, quantum-based optimization, etc.) remains controversial.
    - Maturity is still limited for widespread deployments.
    - It remains to be seen whether sufficient scalability can ever be reached with an acceptable level of error rate.
- Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) might improve the security level of communication between classic computers by relying on principles of quantum mechanics. However, these solutions can only cover limited use cases, as they are complex to implement and do not protect from quantum threats on asymmetric cryptography. For most use cases, transition to PQC will be the most effective and feasible way to protect against quantum computing risks.

Despite the improvements through quantum technologies, **quantum computers are also expected to become a threat for a significant part of cryptography.**

It is important to distinguish between two main categories of computing models in the world of quantum computers:

- **Gate-based quantum computers** are the quantum equivalent of classic digital computers, where bits are replaced by Qubits and classic gates (e.g. NAND gates) are replaced by a Turing complete set of quantum gates (e.g. Clifford group gates + T gates).
- **Alternate types of quantum computers** (e.g. quantum annealers as used by D-Wave) are more comparable to former classic analog computers, where a mathematical problem is converted into a physical equation.

3.2 Cryptography and Quantum threats

It has been formally proven that **a future gate-based quantum computer** with a sufficient number of Qubits of sufficient quality will have the capability to endanger many parts of cryptography as we know it.

Shor's algorithm can break classic asymmetric cryptography (e.g. RSA and ECC crypto algorithms) thanks to an exponential acceleration of the mathematical problem that protects the private keys (i.e. factorization in prime numbers for RSA).

It was thought that Grover's algorithm could provide a quadratic acceleration that would require to double the size of classic symmetric algorithms (e.g. AES) or increase the size of hash functions though this statement and the feasibility of such attack was recently put in doubt. This would tend to demonstrate that AES-128 algorithms would remain acceptable, although some organizations are transitioning AES-256 for additional protection.

Crypto algorithms like RSA, ECC or AES are basic building blocks of well-known security protocols, like TLS that are leveraged by application protocols like ubiquitous HTTPs on the Internet.

Breaking crypto algorithms can thus endanger most application protocols and consequently communication used by IT applications and OT equipment.

Depending on which algorithm is broken in which use case, this can lead to a breakdown of confidentiality, integrity or authenticity properties provided by the higher-level protocols. The impact depends on the threat model and on the assets protected by cryptography.

Alternate types of quantum computers[1] might also weaken cryptography (e.g. by leveraging optimization capabilities provided by quantum annealers to accelerate cryptoanalysis). Importantly however, there is no proof of this being true or not, at least not in ways comparable to what Shor's algorithm can provide to break cryptography.

Overall, this means that:

- New asymmetric algorithms are required to withstand future Quantum Computers.

[1] Based for instance on Quantum Annealing, where a mathematical optimization problem must be converted into a physical problem of quantum mechanics.

- Even if this is still hypothetical, existing symmetric and hashing algorithms might have to be adapted with larger sizes.
- A certain variety of algorithms is required, because:
    a. New asymmetric algorithms are meant to be used in different use cases with distinct requirements in terms of speed and size.
    b. It cannot be excluded that a cryptographic algorithm might be broken by a quantum or a classic computer.[2]

3.3 Harvest-Now, Decrypt Later

Though cryptographically relevant quantum computers with a sufficient amount of good quality qubits are not available yet, the most important scenario to consider is of the type *"harvest-now, decrypt-later"*. Indeed, malicious actors might store sensitive data in advance, before it can be handled by a quantum computer and decrypted in the future.

An equivalent issue might affect document signature scenarios with a signed document harvested now by an adversary who will be able to later retrieve the private keys from public certificates and then have a tampered signed document on behalf of the original signatory.

This can affect confidentiality or integrity of the data depending on the protection offered by the cryptographic algorithm.

3.4 Cryptographic Algorithms and Protocols

The US' National Institute of Standards and Technology (NIST) has selected a certain number of new base algorithms for PQC following a competition process, as a substitute for classic asymmetric algorithms like RSA and ECC. The NIST selection process has been followed by a standardization process for the two main mechanisms, with aim of keeping sufficient diversity and:

- Key Encapsulation Mechanisms (KEM), with ML-KEM (based on lattice cryptography) and HQC (based on code cryptography).
- Signatures with ML-DSA and FN-DSA (based on lattice cryptography) and SLH-DSA (based on hash-based cryptography).

Besides the NIST PQC competition, other base algorithms have been standardized or are supported for standardization by multiple bodies like the Internet Engineering Task Force (IETF), ANSSI (France), BSI (Germany). These include XMSS and LMS (hash-based signatures), which were previously standardized by NIST, and FrodoKEM (recommended by BSI) and Classic McEliece for KEM (initially and until 2025 recommended by ANSSI), which are under active standardization at ISO/IEC.

Indeed, different PQC algorithms display different sizes of keys as well as different processing times. As such, choosing a PQC algorithm is linked to the desired security protocol. All base algorithms must be integrated as building blocks into higher level protocols such as TLS, X.509,

[2] Most cryptographic algorithms are not formally proven and must rely on heuristics (e.g. AES) or mathematical conjectures (e.g. RSA or ECC).

SSH, IPsec. These must also to be standardized by bodies like IETF, ISO, ITU, ETSI, and will be so at varied paces.

In general, the need for a smooth migration path from classic to PQC cryptography requires to use some form of hybrid in a temporary phase.

There can be special exceptions to this rule, for instance where long-existing algorithms like hash-based signature schemes (e.g. XMSS) are proven to be quantum-resistant and can be used in very specific use cases (e.g. one signature with one key).

3.5 Attack Scenarios

Threats from future cryptographically-relevant Quantum Computers such as “Harvest Now – Decrypt Later” are just adding to existing threats, from current classic computers, see Figure 2. They will add up on well-known issues such as implementation errors, insufficient randomness, and side-channel attacks.

Key-exchange compromise

Many widely deployed secure communication protocols rely on public-key exchange mechanisms. Their security is tied to factoring or discrete logarithms. An attacker can passively intercept and then store encrypted network traffic today using classical infrastructure. While the encrypted sessions remain confidential in the short term, the captured data can be retained until future cryptographically relevant quantum computers make it feasible to derive session keys from the recorded handshakes. In parallel, implementation weaknesses, such as insufficient randomness during key generation, reuse of ephemeral parameters, or downgrade attacks, may already reduce the effort required for a future decryption.

Impact

Impact is expected to be very progressive, since the first Quantum Computers capable of breaking cryptography will first be very few and with very limited capacity, but this will greatly worsen with time.

The result is a delayed loss of confidentiality. Sensitive communications assumed to be protected at the time of transmission, including intellectual property, customer data, and strategic communications, may be exposed years later, long after incident response or contractual safeguards are possible. For organizations with long data retention or confidentiality requirements, this creates a compliance, legal, and reputational risk that cannot be mitigated retroactively.

Digital signature and trust-chain attacks

Attack scenario

Digital signatures underpin software updates, device identity, authentication, and public key infrastructures (PKIs). In a future quantum-enabled attack, an adversary could derive private signing keys associated with vulnerable signature schemes and use them to forge legitimate-looking signatures. Even before such capabilities are available, attackers can exploit poor key protection, insufficient entropy during key generation, or compromised hardware security modules to prepare for later abuse. Once a signing key is broken, all assets signed with that key, past and future, become suspect.

Impact

Impact will depend on the use, whether digital signature is hardware- or software-based, but also how the signed artefacts are managed afterwards, whether signed artefacts are centrally managed (e.g. signed documents stored in a qualified archive), whether additional quantum-safe signatures can be later applied.

A successful signature compromise undermines trust at scale. Attackers could distribute malicious software updates, impersonate trusted services, or invalidate regulatory and audit evidence that relies on cryptographic signatures. In regulated environments, this may lead to operational shutdowns, forced certificate revocations, large-scale re-issuance efforts, and loss of customer trust. Unlike data breaches, trust-chain failures often require costly ecosystem-wide remediation rather than isolated fixes.

Side-channel and implementation-driven attacks

Attack scenario

Side-channel attacks exploit information leaked through timing, power consumption, electromagnetic emissions, or error messages during cryptographic operations. These attacks are effective today and remain effective in a post-quantum world. In fact, complex cryptographic implementations, including post-quantum algorithms, can increase the attack surface if not carefully implemented. An attacker may use side-channel leakage to extract partial secrets, reduce key entropy, or bypass algorithmic security assumptions, potentially lowering the computational effort required for both classical and future quantum attacks.

Impact

Side-channel exploitation enables targeted, high-impact breaches that often bypass perimeter defenses. Compromise of cryptographic keys through implementation leakage can lead to unauthorized access, persistent system compromise, and silent manipulation of data or communications. Because these attacks exploit legitimate cryptographic operations, they are difficult to detect and may remain unnoticed for long periods, amplifying business and operational damage.

Threat combinations

In practice, these attack scenarios do not occur in isolation. The most realistic future threats are hybrid in nature: classical attacks used to weaken systems today, combined with future quantum capabilities to complete the compromise. This reinforces the need for a holistic approach that addresses algorithm choice, implementation security, key management, and crypto agility, ensuring that systems can evolve as the threat landscape changes.

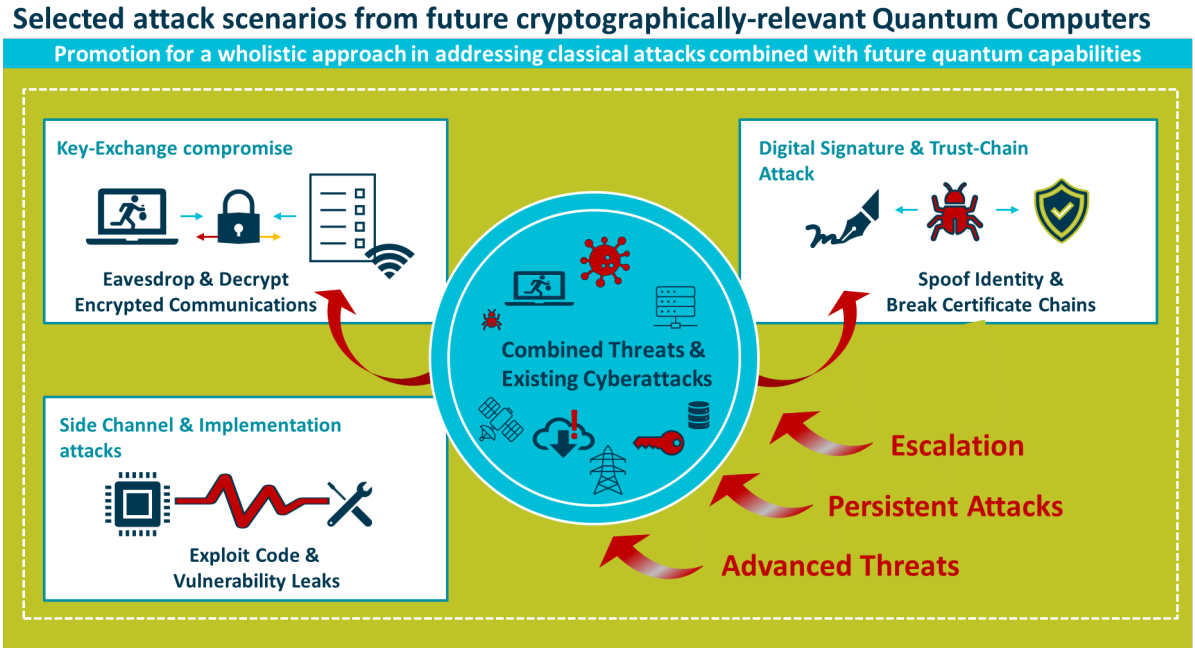

Figure 2: Selected attack scenarios from cryptographically relevant Quantum Computers

4. Global PQC Transition Strategies: A comparative perspective

It is understood that shying away from PQC transition is not an option. PQC threats are realistic and now near cybersecurity and business risks. Several national governments and regional organizations have already outlined PQC transition timelines and guidance – some mandatory, some on a voluntary basis for businesses. We give a brief comparative overview of six key national and regional timelines for PQC across the world.

4.1 United States

In 2022, the White House set the goal in National Security Memorandum 10 (NSM 10) to "prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035" (The White House, 2022a).

To implement NSM-10, the Office of Management and Budget (OMB) issued Memorandum **M-23-02, "Migrating to Post-Quantum Cryptography," in 2022, requiring** federal civilian agencies to inventory their cryptographic systems as an initial step toward mitigating quantum risks. The memo directs agencies to conduct and maintain a **prioritized inventory of cryptographic systems that could be vulnerable to quantum decryption**, including where cryptography is used and the sensitivity and longevity of the protected data (The White House, 2022b).

The Federal Information Security Modernization Act (FISMA) requires federal civilian agencies to use **NIST PQC cryptographic standards and transition guidance.** In November 2024, NIST published a request for comment on "Transition to Post-Quantum Cryptography Standards" (NIST, 2024). It proposes timelines for deprecating and disallowing quantum-vulnerable

algorithms to transition to post-quantum cryptography. Adherence to the final timelines will be mandatory for U.S. government, but the timelines could change in a final published document.

Because national security systems (NSS) are governed separately and are considered higher risk, the Committee on National Security Systems (CNSS) published CNSSP-15 ”Use of Public Standards for Secure Information Sharing” in March 2025 to direct their transition (CNSS, 2025). It requires use of the National Security Agency's (NSA) Commercial National Security Algorithm Suite 2.0, shortened CNSA 2.0, (NSA, 2025). CNSSP-15 establishes mandatory post-quantum cryptography (PQC) adoption timelines for NSS to counter quantum computing threats and "harvest now, decrypt later" attacks. The directive requires implementation of NIST-standardized quantum-resistant algorithms: ML-KEM for key establishment and ML-DSA with LMS/XMSS for digital signatures.

Beginning in 2027, CNNSP-15 requires CNSA 2.0 algorithms in all new products and services that provide cryptographic protections for users or for updates and equipment and services which cannot or will not be updated to CNSA 2.0 algorithms must be phased out and replaced **by 2030**. Policy implications extend to commercial sectors through supply chain requirements and vendor certification programs. Therefore, federal agencies with national security systems and defense contractors need to allocate resources for testing, validation, and workforce development.

Compliance is currently only required for those operating NSS. It will be verified as part of the Risk Management Framework (RMF) assessment of Security Control SC-12 (cryptographic key establishment and management) by the NSS acquisition officials and operators, the NSA or National Information Assurance Partnership (NIAP).

CNSA 2.0 positions the United States as the leader in quantum-safe security through its aggressive timelines while establishing frameworks for allied nations' PQC strategies, strengthening collective cybersecurity resilience.

4.2 Europe

Europe’s approach to preparing for the quantum era has evolved from awareness building toward structured, policy-driven deployment frameworks, with the European Commission and Member States now aligning on timelines, coordination mechanisms, and regulatory incentives for migrating classical cryptographic systems to quantum-resistant alternatives. In June 2025 the European Commission, supported by the NIS Cooperation Group, published a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, following an earlier Recommendation issued in April 2024 (European Commission, 2025). This document establishes key milestones for Member States, with the expectation that all EU Member States begin transition activities – including cryptographic inventories, stakeholder engagement and pilot projects – by the end of 2026 and that high-risk and critical infrastructure systems should be protected with quantum-safe cryptography by no later than the end of 2030.

This roadmap is explicitly linked to a broader EU cybersecurity legislation. Directives such as NIS2 (EU Directive on the security of network and information systems) and sector-specific frameworks like the Digital Operational Resilience Act (DORA) embed requirements for crypto-agility and cryptographic risk management into governance and compliance obligations. Under these rules, organizations must maintain continuous oversight of cryptographic assets,

demonstrate the ability to change algorithms, and integrate quantum-resilience into risk planning and key lifecycle management.

From a standardization perspective, European engagement on PQC is deeply entangled with international processes. ENISA (the EU Agency for Cybersecurity) continues to publish technical reports on PQC algorithm families, integration challenges and best practices for hybrid deployments (where classical and quantum-safe algorithms coexist to mitigate risk during transition). These contributions both inform and are informed by global standardization efforts such as those led by NIST and technical bodies like ETSI and the IETF, which are working on approving and refining protocols to support post-quantum primitives in common use cases (e.g., key exchange and digital signatures).

National cybersecurity authorities within the EU also play a vital role in interpreting and operationalizing the roadmap within domestic contexts. Agencies such as Germany's Federal Office for Information Security (BSI) and France's ANSSI have long-standing cryptography guidance and evolving positions on quantum risk, encouraging risk-based assessments, hybrid cryptography pilots, and integration of PQC in critical services. While these national frameworks vary in specificity, they broadly echo EU strategic aims, by prioritizing early inventory, phased migration and alignment with regulated deadlines.

Operationally, the EU's PQC roadmap is iterative: a public consultation launched in 2025 by the NIS Cooperation Group is intended to gather feedback from industry, academia and critical infrastructure stakeholders to refine and expand the roadmap's guidance and sector-specific measures. This signals an ongoing evolution of policy and practice rather than a static plan.

In synthesis, the European PQC roadmap in 2026 is characterized by: coordinated EU-level direction with clear start and high-risk protection deadlines; integration of PQC readiness into cybersecurity compliance regimes (e.g., NIS2 and DORA); technical contributions from ENISA and international standardization bodies to enable interoperable and certified quantum-safe solutions; and active engagement from national security agencies to tailor implementation to local risk environments-all underpinned by continuous stakeholder consultation and evolving best practices.

4.3 United Kingdom

The UK's Government, led by the National Cyber Security Centre (NCSC), part of the Government Communications Headquarters (GCHQ), has introduced a national roadmap to guide the transition to postquantum cryptography (PQC). Released in early 2025, this framework outlines how the UK will protect government, industry, and critical national infrastructure from the emerging risks posed by largescale quantum computers.

The roadmap establishes clear milestones, with the overarching objective of achieving full adoption of quantum-resistant encryption across all critical UK systems by 2035. Key targets include completing cryptographic discovery, inventories, and migration plans by 2028; delivering priority system upgrades for high-value assets and legacy environments by 2031; and reaching full deployment of PQC across critical systems by 2035. The NCSC's accompanying guidance emphasizes the need for early and deliberate planning.

The UK's policy is backed by updated technical recommendations and alignment with international standards. Building on earlier work, including the NCSC's 2020 paper on quantum-safe preparations, the guidance now supports adopting NIST-standardized quantum-safe

algorithms as they become available (NCSC, 2020 & NCSC, 2025). Recommended algorithms include CRYSTALSKyber, known in UK guidance as MLKEM, for key establishment, and CRYSTALSDilithium, referred to as MLDSA, for digital signatures. A major principle of the roadmap is crypto agility: systems should support both classical and postquantum algorithms during the transition and remain adaptable to future cryptographic changes as standards evolve.

To expand national readiness, the NCSC is also investing in supporting mechanisms for industry. One major initiative is the PQC Industry Pilot Scheme, launched through the NCSC's Assured Cyber Security Consultancy program (NCSC, 2026). Beginning in 2026, this scheme will certify private sector consultancies with the skills to assist organizations in cryptographic discovery, planning, and migration. The goal is to develop a robust UK ecosystem of PQC qualified experts who can guide both government and industry through the decade-long transition to quantum-safe encryption.

4.4 Japan

Japan's cybersecurity policy is led by the National Cybersecurity Office (NCO), which serves as the central coordinating body responsible for formulating and implementing cybersecurity strategies.

In addition to the NCO, ministries such as the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) implement cybersecurity policies within their respective domains.

The Japanese government has begun considering a migration to post-quantum cryptography (PQC) by 2035, taking international cooperation into account. A migration roadmap is scheduled to be developed within fiscal year 2026. Japan is carefully assessing the timeline for the practical realization of quantum computers and aims to promote the transition to PQC in a way that does not compromise cybersecurity.

The Financial Services Agency (FSA) has instructed domestic financial institutions to formulate migration plans in preparation for Harvest Now, Decrypt Later (HNDL) attacks. The FSA has also emphasized that, alongside planning, institutions should conduct risk assessments and improve cryptographic agility, and prioritize systems with a higher need for migration.

Recommended cryptographic algorithms for use in Japan are evaluated and selected by the Cryptography Research and Evaluation Committees (CRYPTREC), which publishes the CRYPTREC Ciphers List.

CRYPTREC has begun preparations to include PQC algorithms in the CRYPTREC Ciphers List. It has started security and implementation performance evaluations for NIST standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA).

Overall, Japan's policy is to advance the migration of PQC in alignment with international trends while closely monitoring developments in other countries.

4.5 Singapore

Singapore's PQC migration strategy is guided by the Cyber Security Agency of Singapore (CSA), which provides governance within existing Critical Information Infrastructure (CII) regulations (CSA, 2025a). The migration is intended as a multi-year, phased process, with organizations encouraged to start promptly to avoid rushed implementations and to manage complex

cryptographic inventories effectively (Lim, H. W., 2025). The scope covers CII owners, government agencies, and private-sector organizations handling sensitive or long-lived data, ensuring comprehensive coverage across cloud and legacy systems.

Singapore does not mandate a universal PQC transition deadline across all sectors, but key regulatory bodies such as MAS (for the financial sector) and CSA have issued guidelines encouraging immediate preparation. This approach aligns with international best practices, emphasizing a risk-based, phased transition. The National Quantum-Safe Network Plus (NQSN+), launched by the Infocomm Media Development Authority (IMDA) in 2023 as part of Singapore's Digital Connectivity Blueprint to 2030, aims to roll out quantum-safe communications infrastructure nationwide (IMDA, 2025). Tooling and implementation support are central to the strategy. Automated cryptographic discovery tools, hybrid cryptography deployment, and CSA's Quantum Readiness Index (QRI) help organizations assess readiness, prioritize actions, and engage senior management (CSA, 2025b). Assurance is maintained through continuous governance, monitoring, and board-level oversight, supported by risk-based prioritization frameworks and testing of hybrid systems (CSA, 2025a).

4.6 Australia

The Australian Signals Directorate (ASD) and its Cyber Security Centre have established a national policy framework to accelerate the transition to PQC (ASD, 2025). ASD updated its official cryptographic guidance in late 2024 to mandate the retirement of vulnerable public key algorithms by 2030. Under this policy, widely used methods such as RSA, elliptic-curve cryptography (ECDH/ECDSA), and even SHA256 will no longer be approved for secure government use beyond 2030. This accelerated schedule reflects Australia's determination to ensure that government systems and critical infrastructure are quantum-safe well ahead of the moment when quantum computers could compromise today's encryption.

ASD's Information Security Manual (ISM) operationalizes this policy by requiring agencies to phase out traditional public key cryptography by the end of 2030 and migrate to approved quantum-resistant alternatives. The Protective Security Policy Framework (PSPF) further reinforces this direction: beginning in 2025, all newly procured government cryptographic technologies must use PQC capable or PQC default solutions in line with ASD guidance (Department of Home Affairs, 2025). Together, these measures lay out a clear national roadmap and send a strong signal to vendors and government suppliers that quantum-safe algorithms must be embedded into products and services now.

Australia's transition is supported by detailed guidance from the Australian Cyber Security Centre. Its publication *Planning for PostQuantum Cryptography*, first released in 2022 and updated in 2025, explains the urgency of early preparation and highlights the risk that adversaries could harvest encrypted data today and decrypt it later using quantum technology (ASD, 2022). To help organizations respond methodically, ASD introduced the "LATICE" framework, which encourages entities to **L**ocate their uses of cryptography, **A**ssess risk and sensitivity, **T**riage priorities, **I**mplement PQC solutions, and **C**ommunicate or **E**ducate stakeholders continuously throughout the transition. A central principle of this guidance is crypto agility: systems should be designed so that encryption algorithms can be replaced or upgraded with minimal operational disruption, ensuring that organizations remain adaptable as standards evolve.

On standards, Australia is aligned with the international consensus emerging around PQC. The ISM now endorses NIST's newly standardized algorithms as the foundation for postquantum systems, including CRYSTALSKyber (referred to as ModuleLattice KEM, or MLKEM, in Australian guidance) for key establishment and CRYSTALSDilithium (MLDSA) for digital signatures. The ISM's 2024 update also raises the baseline for classical cryptography by requiring new systems expected to operate beyond 2030 to use stronger primitives such as SHA384/512 and AES256, ensuring they are ready to integrate PQC during their lifecycle. Requirements in the PSPF make these standards real: Commonwealth agencies must ensure any new cryptographic equipment or software supports ASD-approved quantum-safe algorithms.

Core Criteria	Governance / Regulation	Timelines / Milestones	Scope / Applicability	Tooling / Implementation Support	Assurance / Readiness Verification
USA	NSA directive CNSA 2.0, based on NIST-standards.	Software and firmware updates by 2025, hardware cryptographic modules by 2030.	Mandatory for NSS, federal agencies, defense contractors.	NIST-standards, hybrid deployment approach, cryptographic inventories, risk-based migration strategy.	Direct verification through FIPS Risk Management Framework when acquisition.
EU	European Commission Recommendation on PQC (2024) and Coordinated Implementation Roadmap for the Transition to PQC (2025), developed with the NIS Cooperation Group; supported by ENISA guidance and aligned with NIS2 and DORA regulatory frameworks.	By **end of 2026**: Member States to initiate PQC transition activities (crypto inventory, planning, pilots). By **2030**: protection of high-risk and critical systems with quantum-safe cryptography.	Applies to **EU Member States**, national public administrations, operators of **essential and important entities** under NIS2, and critical sectors (energy, telecom, finance, transport, public services). Indirect impact on suppliers and ICT vendors via procurement and compliance.	ENISA technical reports and migration guidance; EU-level encouragement of **crypto-inventory**, **crypto-agility**, and **hybrid (classical + PQC) deployments**; alignment with international standards via **ETSI, IETF**, and adoption of NIST-standardized PQC algorithms.	Embedded in **risk-based cybersecurity governance** under NIS2 and DORA; national oversight by competent authorities; audits, supervisory measures, and incident-driven reviews rather than standalone PQC certification.

UK	NCSC national roadmap.	Cryptographic discovery, inventories, migration plans by 2028; priority system upgrades by 2031; full adoption by 2035.	Government, industry, critical infrastructure.	NCSC accompanying guidance; technical recommendation and international standards alignment (NIST), crypto-agility (hybrid) approach.	PQC Industry Pilot Scheme to certify private sector experts for PQC migration.
Japan	Based on **National European cybersecurity authorities** (e.g. BSI, ANSSI, NCSC equivalents) issuing national cryptographic and quantum-risk guidance consistent with EU direction.	National timelines aligned with EU roadmap; pilots and phased deployment during **2025-2030**, prioritizing classified, sovereign, and long-lived data.	Mandatory for **governmental and national security systems**; guidance-driven but increasingly expected for regulated industries	National cryptographic catalogues, security profiles, protocol hardening guidance; support for staged migration and hybrid cryptography.	Compliance checked through national cybersecurity supervision, accreditation schemes, and security audits tied to existing national frameworks.
Singapore	CSA guidance within existing CII regulations; board-level priority.	Start ASAP; phased migration; public consultation 2025 for Handbook & QRI.	CII, government, sensitive private-sector data.	CSA QRI self-assessment; cryptographic discovery tools; hybrid deployment strategy.	QRI self-assessment; board engagement; continuous governance and monitoring.
Australia	ASD cryptographic guidance.	From 2025 all newly procured crypto-graphic tech to be PQC capable; retirement of vulnerable public key algorithms and completed migration by 2030.	Mandatory for governmental agencies and suppliers; non-binding for private entities.	ASD ISM manual, PSPF framework, ACSC Planning for PQC guidance, LATICE framework, crypto-agility approach.	Integrated in cybersecurity governance framework of ASD and ACSC, risk management requirements.

Table 1: Comparative PQC migration summary

5. Implementation Guidance – Practitioner Playbook for PQC Migration

Several national guidelines and handbooks have issued recommendations and requirements for migration. As outlined in section 4, this includes for example the US' NSA directive CNSA 2.0 and NIST-standards, the UK's NCSC national roadmap, Singapore's CSA guidance and the Australian ASD Information Security Manual.

Based on these guidelines, this section summarized the main common steps and provides practical, step-by-step guidance for organizations starting or structuring their Post-Quantum Cryptography migration. The approach follows a proven, phased sequence aligned with industry best practices, including those reflected in the TNO PQC migration handbook, while remaining adaptable to different organizational sizes, sectors, and risk profiles.

Step 1 - Establish cryptographic inventory and visibility

Objective

Understand where and how cryptography is used across the organization.

What to do:

- Identify all cryptographic assets across applications, infrastructure, cloud services, OT, and embedded systems.
- Capture algorithms, key sizes, protocols, libraries, certificates, trust anchors, and dependencies.
- Include third-party software, managed services, and supplier integrations.
- Document ownership, lifecycle, and update mechanisms for each cryptographic component.

Why it matters:

You cannot migrate what you cannot see. Most organizations underestimate the spread of cryptography, particularly in legacy systems and supply chains. This step directly addresses the primary blocker observed in PQC readiness efforts.

Step 2 - Perform quantum-aware cryptographic risk assessment

Objective

Assess which cryptographic assets are at risk and when.

What to do:

- Classify data by confidentiality duration (short-lived vs long-lived).
- Identify use of quantum-vulnerable algorithms in key exchange, signatures, and PKI.
- Evaluate exposure to "Harvest Now - Decrypt Later" scenarios.
- Consider implementation risks such as poor entropy, key reuse, and side-channel exposure.

- Assess external dependencies where algorithm replacement is not fully under your control.

Why it matters:

PQC migration is a risk-driven exercise, not a blanket replacement. This step ensures that effort is focused where quantum impact and business impact intersect.

Step 3 - Define PQC and crypto-agility policy

Objective

Create organizational rules that enable controlled, future-proof cryptographic change.

What to do:

- Define approved cryptographic algorithms and deprecation timelines.
- Introduce crypto-agility requirements into architecture and procurement policies.
- Specify requirements for algorithm agility, key rotation, and update mechanisms.
- Align PQC policy with existing security governance, risk, and compliance frameworks.

Why it matters:

Without policy, cryptographic decisions remain ad hoc and inconsistent. A clear policy ensures that PQC readiness becomes part of standard security and architecture decision-making.

Step 4 - Prioritize systems and use cases for migration

Objective

Sequence migration activities based on risk and feasibility.

What to do:

- Prioritize systems handling long-lived or high-value data.
- Focus on externally exposed interfaces such as TLS, VPNs, APIs, and PKI.
- Identify systems with long replacement cycles (industrial systems, devices, firmware).
- Consider hybrid or transitional approaches where full PQC deployment is not yet feasible.

Why it matters:

Not all systems need to move at the same pace. Prioritization avoids unnecessary disruption while reducing meaningful risk early.

Step 5 - Plan and execute controlled migration

Objective

Introduce PQC in a way that preserves interoperability and operational stability.

What to do:

- Test PQC or hybrid algorithms in non-production environments.
- Validate performance, interoperability, and operational impact.

- Update certificate lifecycles, key management processes, and monitoring.
- Engage vendors and suppliers on PQC roadmaps and contractual commitments.

Why it matters:

PQC migration is not only a cryptographic change - it is an operational one. Early testing prevents performance surprises and integration failures.

Step 6 - Monitor, adapt, and evolve

Objective

Ensure long-term resilience as standards, threats, and technologies evolve.

What to do:

- Track standardization updates and implementation guidance.
- Periodically reassess cryptographic risk and inventory.
- Update policies and architectures as PQC maturity increases.
- Embed PQC readiness into continuous risk management processes.

Why it matters:

Quantum risk evolves over time. Continuous monitoring ensures that today's mitigation does not become tomorrow's legacy problem, see Figure 3 .

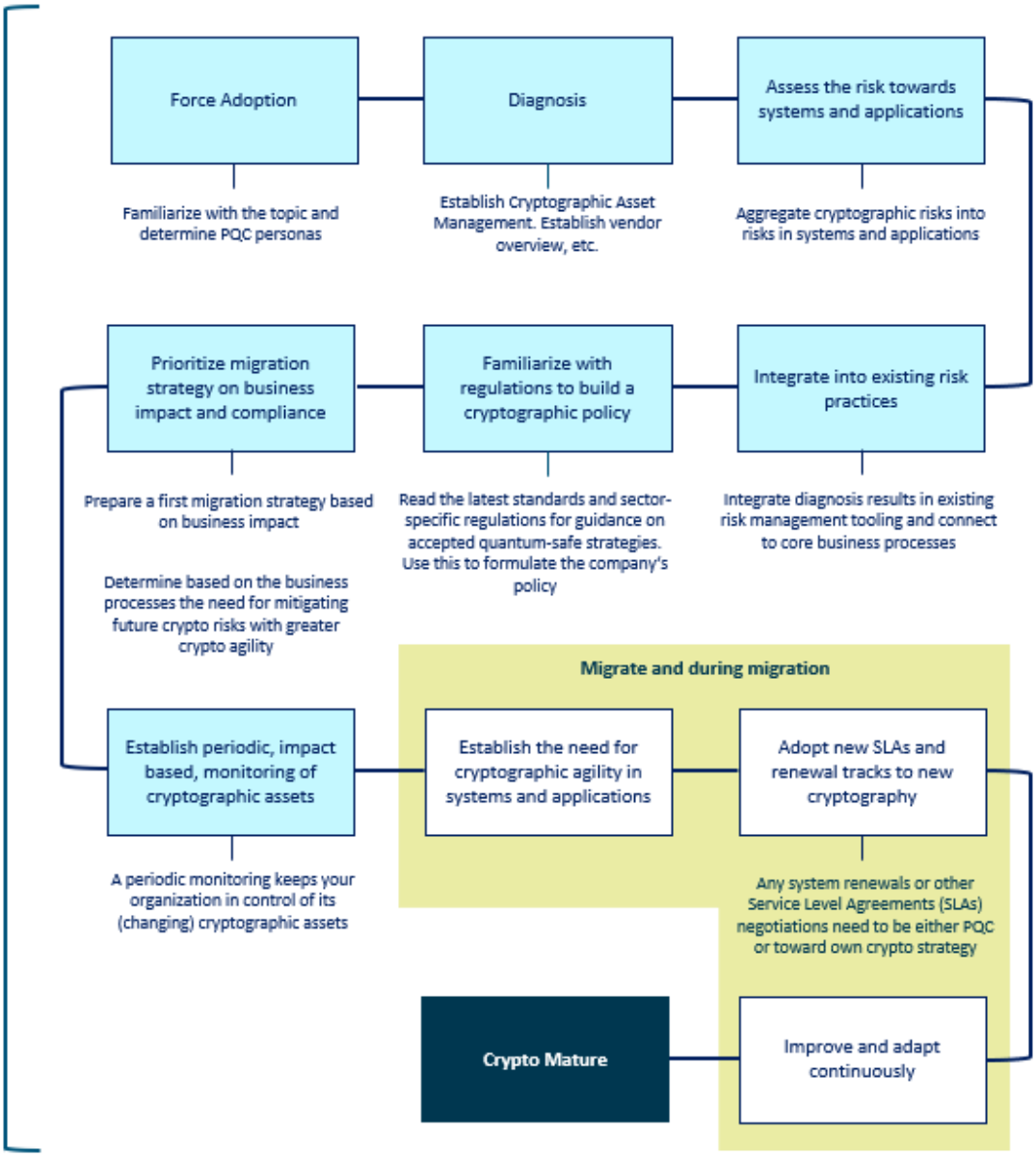

Figure 3: Roadmap towards a mature cryptographic management organization. Source: Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (2024), p.17

6. Conclusion

The transition to post-quantum cryptography is not a future problem — it is a present one. The threat of adversaries harvesting encrypted data today for decryption once quantum computing matures means that organizations with long-lived data and systems are already exposed. Waiting for cryptographically relevant quantum computers to arrive before acting is not a viable risk management strategy.

Exposure is not uniform across sectors. Financial services, government and defense, operational technology, and healthcare face the sharpest quantum risk, driven by decades-long data retention obligations, slow system replacement cycles, and the societal consequences of cryptographic failure. For these sectors, PQC readiness has moved from best practice to strategic imperative.

Globally, the direction of travel is clear. The United States, European Union, United Kingdom, Singapore, and Australia have each established structured PQC transition frameworks, with mandatory deadlines converging around the late 2020s and 2030. Organizations operating across jurisdictions should expect compounding compliance requirements and align migration plans accordingly.

At the same time, the geopolitical dimension of PQC standardization is becoming increasingly salient. The emergence of a “splinternet” infrastructure, characterized by regionally fragmented digital ecosystems, suggests that cryptographic standards diverge along political and strategic lines. As a result, organizations must not only manage technical migration but also navigate a politically charged landscape in which interoperability, regulatory alignment, and long-term cryptographic agility become critical strategic considerations.

This paper offers a comparative overview of regional PQC transition frameworks and identifies the business and systemic risks associated with quantum-vulnerable cryptography, providing insights for organizations preparing for the transition to post-quantum cryptography. Overall, PQC migration is a strategic transformation, not a technical patch. Cryptographic inventory, governance structures, crypto-agility, and supply chain engagement are as central to success as algorithm selection — and organizations that treat PQC readiness as an architectural and organizational challenge will be best positioned as quantum risks continue to mature.

Abbreviations

Technical Terms

Acronym	Expansion	Definition
AI	Artificial Intelligence	Branch of computer science focused on creating systems that can perform tasks requiring human-like intelligence, such as learning, reasoning, problem-solving, perception, and language understanding.
FALCON	Fast-Fourier Lattice-based Compact Signatures over NTRU	A post-quantum digital signature scheme based on lattice cryptography, designed to produce very small signatures and strong security against quantum attacks by using NTRU lattices and Fast Fourier sampling techniques.
FIPS	Federal Information Processing standards	Set of publicly announced standards and guidelines developed by NIST for use in computer systems, covering areas such as cryptography, data security, and interoperability.
HQC	Hamming Quasi-Cyclic	Type of post-quantum cryptographic scheme based on the hardness of decoding random linear codes, specifically using quasi-cyclic codes to enable efficient key generation, encryption, and digital signatures resistant to quantum attacks.
ML-DSA	Module-Lattice Digital Signature Algorithm	Post-quantum digital signature algorithm standardized by NIST, based on module-lattice problems, designed to provide authentication and integrity while remaining secure against quantum-computer attacks (derived from the CRYSTALS-Dilithium design).
ML-KEM	Module-Lattice Key Encapsulation Mechanism	Post-quantum cryptographic key-encapsulation algorithm standardized by NIST, based on module-lattice problems, used to securely establish shared encryption keys that are believed to be resistant to attacks by quantum computers (derived from the CRYSTALS-Kyber design).

PQC	Post-quantum cryptography	Field of cryptography focused on developing algorithms that remain secure against attacks by quantum computers.
PSPF	Protective Security Policy Framework	Policies and guidelines ensuring the protection of information, people, and assets through standardized security governance, risk management, and protective measures.
QKD	Quantum Key Distribution	Method for securely generating and sharing cryptographic keys using quantum mechanics principles.
QRNG	Quantum Random Number Generation	Device or system that produces truly random numbers by measuring inherently unpredictable quantum phenomena.
RMF	Risk Management Framework	Structured process used to identify, assess, mitigate, and monitor risks in information systems, commonly referring to the framework defined by NIST for integrating security and privacy risk management into system development and operation.
R&D	Research and Development	Activities undertaken by organizations to innovate, create, and improve products, technologies, or processes through systematic investigation and experimentation
SCADA systems	Supervisory Control And Data Acquisition	Industrial control systems used to monitor, control, and automate infrastructure and industrial processes.
SPHINCS+	Stateless Practical Hash-based INCremental Signature scheme	Hash-based, stateless digital signature scheme designed for post-quantum security, using only cryptographic hash functions to provide strong resistance against quantum attacks without relying on structured mathematical assumptions.
XMSS	eXtended Merkle Signature Scheme	Hash-based digital signature scheme designed for **post-quantum security**, providing strong security guarantees even against quantum computers, by using a tree of one-time signatures combined with Merkle hash trees.

Organizations and Institutions

Acronym	Expansion
ANSSI	Agence nationale de la sécurité des systèmes d'information (French)
ASD	Australian Signals Directorate
CNSA	Commercial National Security Algorithm (USA)
CSA	Cyber Security Agency (Singapore)
BSI	Germany’s Federal Office for Information Security (German)
DORA	Digital Operational Resilience Act (EU)
EMA	European Medicines Agency (EU)
ENISA	EU Agency for Cybersecurity (EU)
FDA	Food and Drug Administration (USA)
GCHQ	Government Communications Headquarters (UK)
HHS	Health and Human Services (USA)
IETF	Internet Engineering Task Force (int.)
IMDA	Infocomm Media Development Authority (Singapore)
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology (USA)
NSA	National Security Agency (USA)
NSS	National Security Systems (USA)
NQSP+	National Quantum-Safe Network Plus

References

Publications of national & supranational institutions

Australia

Department of Home Affairs (2025): "Protective security Policy Framework", Australian Government. URL: https://www.protectivesecurity.gov.au/pspf-annual-release

ASD (2025): "Guidelines for cryptography", in: *Information security manual*. Australian Signals Directorate. Australian Cyber Security Centre. URL: https://www.cyber.gov.au/sites/default/files/2025-07/22.%20ISM%20-%20Guidelines%20for%20cryptography%20%28June%202025%29.pdf

ASD (2022): "Planning for post-quantum cryptography", Australian Signals Directorate. Australian Cyber Security Centre. Last updated 22 September 2025. URL: https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

European Union

European Commission (2026): "NIS2 Directive: securing network and information systems", Background. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Commission (2025): "Implementing and delegated acts – DORA". URL: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

European Commission (2025): "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography", Publication. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Japan

National Cybersecurity Office (NCO) (2025): Commitment to a Free, Fair and Secure Cyberspace. URL: https://www.cyber.go.jp/eng/index.html

Transition to Post-Quantum Cryptography (PQC) in Government Agencies and Other Organizations (Interim Report) (in Japanese only). URL: https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf

Cryptography Research and Evaluation Committees (CRYPTREC) (2025): Publications. URL: https://www.cryptrec.go.jp/en/index.html

Japan Financial Services Agency (JFSA) (2024): Guidelines on Cybersecurity for the Financial Sector. URL: https://www.fsa.go.jp/common/law/cybersecurity_guideline_en.pdf

Netherlands

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (2024): "The PQC Migration Handbook. Guidelines for Migrating to Post- Quantum Cryptography." Revised and Extended Second Edition. *Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek.* URL: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

Singapore

CSA (2025a): "Quantum-Safe Migration Handbook", Draft for Public Consultation. Cyber Security Agency of Singapore. URL: https://isomer-user-content.by.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20(Oct%202025).pdf

CSA (2025b): "Quantum Readiness Index", Draft for Public Consultation. Cyber Security Agency of Singapore. URL: https://isomer-user-content.by.gov.sg/36/949031c3-6734-4d33-985e-71331fa8ade4/Draft%20for%20Public%20Consultation%20-%20Quantum%20Readiness%20Index%20(Oct%202025).pdf

IMDA (2025): "Digital Connectivity Blueprint (DCB)", Background. Infocomm Media Development Authority. URL: https://www.imda.gov.sg/how-we-can-help/digital-connectivity-blueprint

United Kingdom

NCSC (2026): "Assured Cyber Security Consultancy. Post-quantum cryptography (PQC) pilot", Assurance scheme. National Cyber Security Centre. URL : https://www.ncsc.gov.uk/schemes/assured-cyber-security-consultancy/pqc-pilot

NCSC (2025): "Timelines for migration to post-quantum cryptography", Guidance. National Cyber Security Centre. URL : https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

NCSC (2020): "Preparing for Quantum-Safe Cryptography", Paper. National Cyber Security Centre. URL : https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

United States of America

CNSS (2025): "Use of Public Standards for Secure Information Sharing", Committee on National Security Systems. CNSSP-15, Version March 2025. URL: https://www.cnss.gov/CNSS/issuances/Policies.cfm

NIST (2024): "Transition to Post-Quantum Cryptography Standards", Initial Public Draft NIST IR 8547. National Institute of Standards and Technology. U.S. Department of Commerce. URL: https://csrc.nist.gov/pubs/ir/8547/ipd

NIST (2026): "Post-Quantum Cryptography", Project Overview. National Institute of Standards and Technology. Computer Security Resource Centre. URL: https://csrc.nist.gov/projects/post-quantum-cryptography

NSA (2025): "Announcing the Commercial National Security Algorithm Suite 2.0", National Security Agency. Cybersecurity Advisory. CNSA 2.0. URL: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

The White House (2022a): "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems", 4 May 2022. Press Release. URL: https://bidenwhitehouse.archives.gov/briefing-room/statements-

releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

The White House (2022b): "Memorandum for the Heads of Executive Departments and Agencies", Office of Management and Budget. Executive Office of the President. URL: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

Publications and Articles

Freyer O, Ostermann M, Minssen T et al. (2025): "Quantum cryptography and data protection for medical devices before and after they meet Q-Day", NPJ Digit Med; 8, 620. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12540643/

Gaur, N. / Elmore, M. (2025): "Why pharma and life sciences must act now on the quantum threat", World Economic Forum. URL: https://www.weforum.org/stories/2025/09/pharma-life-sciences-quantum-threat-cybersecurity/

Geller, E. (2025): "NIST explains how post-quantum cryptography push overlaps with existing security guidance", Cybersecurity Dive. URL: https://www.cybersecuritydive.com/news/nist-post-quantum-cryptography-guidance-mapping/760638/

Health Management (2025): "Medical Devices Face Post-Quantum Security Deadlines". URL: https://healthmanagement.org/c/it/News/medical-devices-face-post-quantum-security-deadlines

Ivezic, M. (2025): "Post-Quantum Crypotgraphy (PQC) Standardization – 2025 Update", POSTQUANTUM. URL: https://postquantum.com/post-quantum/cryptography-pqc-nist/

Lim, H. W. (2025): "Quantum-safe cryptography: When and how to start", NCS. URL: https://www.ncs.co/en-sg/impact-insights/quantum-safe-cryptography-when-and-how-to-start/

Medicrypt (2025): "Navigating Post-Quantum Cryptography in Medical Device Cybersecurity", Blog. URL: https://www.medcrypt.com/blog/navigating-post-quantum-cryptography-in-medical-device-cybersecurity

PKI Consortium (2025): "Post-Quantum Cryptography Conference 2025 Concludes with Urgent Call for Global Migration to Quantum-Resistant Encryption Systems", Public Key Infrastructure Consortium. URL: https://pkic.org/2025/11/04/post-quantum-cryptography-conference-2025-concludes-with-urgent-call-for-global-migration-to-quantum-resistant-encryption-systems/

Quantum Xchange (2024): "2025 Outlook: Navigating the Quantum Revolution in 2025 and Beyond", Blog. URL: https://quantumxc.com/blogs-podcasts/the-quantum-revolution-in-2025-and-beyond/

Saha, P. (2025): “Why Do Organizations Need PQC Assessment in 2025?”, Encryption Consulting. URL: https://www.encryptionconsulting.com/why-do-organizations-need-pqc-assessment-in-2025/

Schwartz, N./ Wirth, A. (2025): “Medical device manufacturers need to act now on post-quantum cryptography”, Medical Design & Outsourcing. URL: https://www.medicaldesignandoutsourcing.com/medical-device-encryption-post-quantum-cryptography/

Stubbs, M. (2025): “Updated whitepaper for 2025 – ‘The new NIST standards are here: what does it mean for PQC?’”, Comment. PQ Shield. URL: https://pqshield.com/updated-whitepaper-for-2025-the-new-nist-standards-are-here-what-does-it-mean-for-pqc-in-2025/

Swayne, M. (2025): “NIST Cybersecurity Center Outlines Roadmap for Secure Migration”, Insider Brief. Quantum Insider. URL: https://thequantuminsider.com/2025/09/19/nist-cybersecurity-center-outlines-roadmap-for-secure-migration/

Westerbaan, B. (2025): “State of the post-quantum Internet in 2025”, The Cloudflare Blog. URL: https://blog.cloudflare.com/pq-2025/

Appendix: PQC Use Cases and Sector Alignment

As reflected in NIST's 2025 standards (FIPS 203/204/205), different PQC primitives support distinct operational and regulatory contexts. The various PQC primitives offer distinct strengths, therefore it is recommended to select appropriate schemes as required by aligning them with the operational and regulatory context of each sector.

Due to the emerging nature of this field, there is the risk in future that weaknesses are discovered in one of the standardized algorithms. During the competition to standardize these algorithms, some algorithms made it through multiple rounds of review before they were discovered to have weaknesses. Therefore, it is critical that systems incorporate crypto agility to enable transition to new algorithms if current algorithms are found to have weaknesses in the future.

NIST has adopted Lattice-based and Hash-based cryptography standards. In addition, there are code-based and multivariate cryptography schemes. Though, since 2022, the multivariate 'Rainbow' was effectively broken and this scheme was removed from the NIST referenced standards.

Here are the few examples including the NIST referenced schemes:

A. Lattice-Based Cryptography (e.g., ML-KEM/CRYSTALS-Kyber, ML-DSA/CRYSTALS-Dilithium, FALCON)

Lattice-based schemes support secure communications, efficient key establishment, and robust digital signatures. Their performance characteristics make them suitable for large-scale transactional environments in finance, securing government communications, securing medical device communications, health record exchanges, and industrial systems that require high-throughput encryption. Despite their usefulness, lattice-based signature algorithms could still be problematic due to added latency during session establishment due to at least one additional round-trip in crypto protocol scope.

B. Hash-Based Cryptography (e.g., SPHINCS+)

Hash-based signatures provide strong assurances of long-term integrity and are well-suited to software update signing, document authentication, and archival protection. These characteristics align with the needs of government record preservation, financial document integrity, and support digital signatures for electronic consent forms, software/firmware updates in devices, and validation of medical records' integrity over decades.

C. Code-Based Cryptography (e.g., HQC)

Code-based cryptosystems are appropriate for encrypting long-term archives and sensitive communications. Their longstanding research history and resilience to quantum attacks make them pertinent for government, financial, healthcare, and research-intensive sectors requiring persistent confidentiality.

D. Multivariate Cryptography

Multivariate signature schemes support authentication and identity mechanisms, making them relevant to public-sector identity systems and financial authentication processes where durability and trustworthiness are paramount. Since 'Rainbow' was effectively compromised in 2022, this scheme has been an active field of research. There have been many proposals with updated designs compared to older multivariate proposals. However, none of the proposed designs such as 'Mayo', have been proven to be effective to be adopted as standards. The following table summarizes a few examples of primary use-cases for various PQC primitives relevant to various sectors.

PQC Family	Primary Uses
Lattice-based	Communications, signatures, key establishment
Hash-based	Software signing, integrity assurance
Code-based	Archive encryption, secure communications
Multivariate	Authentication, signatures

In conclusion, financial services, government/defense, and critical infrastructure exhibit the highest consequential long-term quantum risk due to the longevity of their systems, the enduring sensitivity of their data, and the societal consequences of cryptographic failure. Strategic PQC deployment for these domains is now guided by formal NIST standards finalized in August 2025, and further migration planning should reference these specifications. Prioritizing PQC-aligned protection for long-lived assets in these sectors is indispensable to national security, public trust, and economic resilience in the quantum era. Before delving into global timelines of PQC transition, the following section the technical state of play and threat landscape.