BLimPQC WP4 report on regulation development

Work Package 4

Beyond the Limits of PQC

March 31, 2026

Author	Organisation
Outi-Marja Latvala (Edit.)	VTT
Mirko Sailio	VTT
Anni Karinsalo	VTT
Ville Ollikainen	VTT
Niko Keskitalo	Bittium
Sini Ruohomaa	Ericsson
Mikko Karppinen	Icareus
Jorma Kivelä	Jutel
Suvi Lampila	SSH
Gizem Akman	University of Helsinki
Valtteri Niemi	University of Helsinki
Petri Jehkonen	Xiphera

Executive Summary

Advances in quantum computing challenge a foundational assumption of today's digital security. A cryptographically relevant quantum computer can break the mathematical basis of modern cryptography, leaving much of today's digital life such as banking information, government communications and other critical services vulnerable. The risk of "harvest now, decrypt later" type of attack is moving governments and regulators to mandate the use of Post-Quantum Cryptography (PQC), with several governments signalling ambitions to reach broad or full PQC adoption by the mid-2030s. This report examines how regulation is shaping the transition to PQC, with a focus on impacts, constraints, and opportunities for organisations and markets.

The report first provides an overview of the global regulatory landscape for PQC. It reviews developments in the European Union, the United States, and other regions worldwide, highlighting differences in regulatory maturity, approaches, and timelines. While some jurisdictions rely primarily on guidance and roadmaps, others have introduced binding mandates and reporting obligations. Overall, regulatory approaches remain uneven, increasing the importance of coordination, interoperability, and crypto-agility.

The report then analyses sector-specific regulatory implications for critical infrastructure, finance, telecommunications, and media systems. These sectors face distinct challenges due to long system lifecycles, complex supply-chains, and stringent security requirements. In many cases, PQC adoption is driven indirectly through existing cybersecurity regulation, procurement requirements, and evolving standards rather than explicit PQC mandates.

The discussion section synthesizes these findings from a BLimPQC Work Package 4 perspective. It shows that PQC migration is shaped by the interaction of regulation, standardisation, market forces, and supply-chain dependencies. Regulatory pressure creates urgency and direction, but practical deployment depends on technical readiness, interoperability, and coordination across vendor ecosystems. Uncertainty about timelines, combined with the long tail of legacy systems, suggests that PQC migration will be a multi-year process with uneven progress across sectors. At the same time, regulation creates opportunities for organisations that anticipate emerging requirements and invest early in crypto-agile, interoperable solutions.

This report is the first in a series of Work Package 4 studies on regulation impacts and opportunities. Subsequent reports will build on this regulatory analysis by examining PQC-related use cases, business opportunities, and the evolving regulatory and market landscape.

Contents

1 Introduction

Quantum computers are developing quickly. Even though they have interesting applications, they also pose a fundamental challenge to the cryptographic systems that underpin today's digital security. Modern public-key algorithms, e.g. RSA and elliptic curve cryptography, derive their security from the computational hardness of problems such as integer factorisation and discrete logarithms. Large-scale, fault-tolerant quantum computers (CRQCs, cryptographically relevant quantum computers) will be able to solve these problems efficiently using Shor's algorithm, rendering widely deployed encryption and authentication schemes vulnerable. As a consequence, any data encrypted with these classical schemes today may be at risk under a "harvest now, decrypt later" threat model, where adversaries collect encrypted data in the present with the expectation of decrypting it once quantum capabilities mature.

In order to address these emerging risks, international standardisation bodies have begun work on post-quantum cryptography. The U.S. National Institute of Standards and Technology (NIST) initiated its PQC algorithm competition in 2016 and announced the first algorithms selected for standardisation in 2022. In 2024, the first finalized PQC standards—FIPS-203 (ML-KEM, based on CRYSTALS-Kyber), FIPS-204 (ML-DSA, based on CRYSTALS-Dilithium), and FIPS-205 (SLH-DSA, based on SPHINCS+)—were published. FIPS-206 (FN DSA, based on Falcon) is currently in draft, and in early 2025 NIST selected HQC for

standardisation as well. Other standardisation organisations have also produced standards for several prominent algorithms, such as FrodoKEM and Classic McEliece. For a more thorough investigation and discussion of standardisation efforts, please refer to the BLimPQC Work Package 3 report "Review on PQC Standardisation Activities".

As standardisation matures, regulatory and policy frameworks are beginning to shape the timelines for PQC migration. Governments and sector specific regulators are issuing mandates and guidance to ensure that organisations manage the transition in a coordinated manner. Migration to PQC is not merely a technical exercise; it involves reviewing the current status, planning, resource allocation, testing, compliance, and long term maintenance. In this report, we first provide a global overview of regulations related to PQC migration, followed by a sector specific analysis of relevant regulatory developments. We conclude with a discussion section that synthesizes regulatory developments and examines how regulation, standardisation, market forces, and supply chain dependencies shape the transition to post quantum cryptography, highlighting challenges related to timelines, interoperability, and legacy systems. This is the first of three reports in BLimPQC work package 4, Regulation Impacts and Opportunities. The second report on use cases and business opportunities will be published in March 2027 and the final report on regulation and business landscape in March 2028.

2 Global Regulatory Landscape for PQC

In this section we provide an overview of the global regulatory landscape shaping the transition to post-quantum cryptography. It reviews policy frameworks, regulatory guidance, and migration timelines across major jurisdictions, including the European Union, the United States, and other regions worldwide, and highlights differences in regulatory maturity, approaches, and levels of coordination. Together, these developments illustrate how governments are beginning to translate emerging quantum risks into concrete expectations for organisations and markets.

2.1 EU Regulatory Environment

As of the time of writing, there is no explicit EU PQC regulation. However, there are requirements coming from other EU directives. NIS2, Directive (EU) 2022/2555 [1] establishes a requirement for high common level of cybersecurity. It promotes, but does not require "the use of encryption technologies, in particular end-to-end encryption". It requires each member state to adopt a national cybersecurity strategy, which include adopting policies on the cybersecurity requirements (including encryption) for ICT products and services in public procurement.

Digital Operational Resilience Act (DORA) [2] requires that some organisations (e.g. critical infrastructure operators) adopt cybersecurity risk management measures, including state-of-the-art cryptography. Failure to comply can result in liability issues for the responsible organisations and their managers. Cyber Resiliency Act (CRA) [3] defines requirements for all products with digital elements in EU markets starting 11.12.2027, including requirement to protect confidentiality through encryption. The Radio Equipment Directive (RED) (Directive 2014/53/EU) [4] also imposes security related requirements on connected radio equipment placed on the EU market; however, it does not currently include explicit PQC requirements, and PQC relevance arises only indirectly through its general security and compliance obligations.

European Cybersecurity Strategy [5] notes the alarming cybersecurity situation of European actors. The strategy suggests using regulation, investment and policy to improve the resilience, technological sovereignty and leadership in cybersecurity. Efficient encryption is identified as a key component of cybersecurity, to be integrated into all digital investments. The strategy also notes importance of providing further impetus for development of state-of-the-art encryption expertise.

Other regulations which implicitly require the use of PQC technologies also exist. The General Data Privacy Regulation (GDPR) [6] establishes a requirement of "appropriate level of security" when processing PII (personally identifiable information), using efficient technical measures to prevent unauthorized access to such data. Protection of European Union Classified Information (EUCI) [7] defines that classified

Figure 1: EU PQC roadmap timeline [11]

information may only be transmitted by electronic means protected by approved cryptographic products. Approval to handle EUCI can be revoked upon notification of breach or significant change in design or security measures [8]. If quantum computing enables the breaking of non-PQC cryptography, many currently approved encryption technologies would quickly lose their approval for EUCI usage.

European Union Agency for Cybersecurty (ENISA) has conducted multiple studies on the PQC preparedness in Europe. They provide suggestions for the private sector to prepare for the transition. [9]

EU member states issued a roadmap and timeline for starting the use of PQC [10]. NIS Cooperation Group PQC workstream, founded by the European Commission, provides a high-level roadmap and recommendations for a coordinated EU-wide transition to post-quantum cryptography. The timeline suggests, that as first steps, all the EU countries initiate a national PQC transition strategy by end of 2026. High-risk cases should aim to transition to using PQC by end of 2030. Quantum-safe defaults should be achieved and transition finished by 2035. [11]

2.2 United States: Standards, Policies, and Federal Timelines

The Quantum Computing Cybersecurity Preparedness Act (Public law 117-260) [12] aims to ensure that U.S. Federal Government IT systems plan and prepare for migration to post-quantum cryptography. This federal law requires federal agencies to inventory cryptographic systems, plan migration strategy and report the progress to the U.S. Congress. By creating federal accountability for PQC migration, the law establishes migration as national cybersecurity priority.

A White House national security memorandum (NSM-10) [13] sets U.S. policy to mitigate risks from cryptographically relevant quantum computers by prioritizing a transition to PQC across federal systems. It directs NIST and other agencies to establish a migration plan with a target transition timeline to quantum-resistant cryptography by 2035, ensuring government and infrastructure cryptographic systems are upgraded.

The Office of Management and Budget (OMB) memo "OMB-M-23-02" [14] describes the preparatory steps on how to implement high-level policy NSM-10 before the finalisation of NIST standards. It establishes requirements and timeline for federal agencies to start inventorying their quantum-vulnerable cryptographic systems and submitting the inventory results annually to Office of the National Cyber Director (ONCD) and CISA. These authorities will assess the resulting risk based on the inventories.

In the U.S. defense context, the Department of Defense Chief Information Officer (DoD CIO) issued a memorandum titled Preparing for Migration to Post-Quantum Cryptography [15]. The memorandum translates earlier federal policy guidance into concrete organisational requirements for the defense ecosystem, including comprehensive cryptographic inventories, designated PQC migration points of contact, and centralized approval processes for testing, evaluating, and deploying PQC-related technologies. While the memorandum primarily applies to Department of Defense components, it also affects vendors and suppli-

ers supporting defense systems by reinforcing strict coordination, certification, and migration planning expectations.

Executive Order 14144 (2025) for PQC implementation requirements [16] mandates that federal agencies implement PQC "as soon as practicable". The order creates mandatory timelines for the transition for federal actors. Vendors have to ensure their products are PQC-compliant to remain eligible for federal contracts, and the Director of the Cybersecurity and Infrastructure Security Agency (CISA) is required to maintain and update information about PQC-compliant products. The June 2025 modification [17] shifts emphasis from proactive PQC development to vulnerability identification and risk management. In the same period, Executive Order 14306 [18] further reinforced U.S. federal cybersecurity modernisation efforts by sustaining and amending earlier executive actions, including Executive Order 14144. This order strengthens the continuity of federal cybersecurity policy, maintains pressure on agencies to modernise cryptographic practices, and supports ongoing coordination across civilian, defense, and national security domains.

In support of implementation, NIST, CISA and Homeland Security have created a roadmap with the related infographic [19]. Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools [20] addresses the technical challenges of identifying cryptographic assets. The strategy emphasizes automation as a pre-requisite for effective PQC migration. Compared to Europe, U.S. regulation for PQC is more standard-driven (NIST FIPS 203, FIPS 204, FIPS 205), policy-mandated (NSM-10 and OMB guidance), and integrated within broader cybersecurity executive actions. European regulators often refer to NIST PQC standards when assessing "quantum-safe" cryptography requirements, so early U.S. standards tend to influence EU standard adoption timelines and certification benchmarks.

2.3 Global Readiness for Post-Quantum Cryptography

Outside of the EU and United States examined before, the global PQC landscape is progressing unevenly. Countries across Asia, Oceania, Africa, and Latin America have recognized the arrival of a quantum era and they are defining national strategies for PQC migration. However, there are significant differences in the focus and maturity of migration efforts. Post-Quantum Cryptography Coalition published a short overview of PQC regulations around the world in the middle of 2025 [21]. They noticed that regulations are emerging rapidly, but they are not fully aligned, which might create challenges for vendors and for international interoperability.

Within Asia, China is conducting its own national PQC standardisation effort [22] [23]. Previously, China has focused more on the quantum key distribution (QKD) solution to the quantum threat, and could therefore use a two-pronged approach to quantum security [24]. Regarding China's cryptography-related legislation [25], that applies to all cryptography used, not only PQC, China explicitly mentions commercial actors. In contrast, in the U.S., the commercial actors' cryptographic solutions are primarily regulated when applied in the federal use, for example regarding cloud applications[26].

South-Korea has also run a national standardisation competition. Its winners were announced in January 2025: Digital signatures HAETAE and AIMer; PKE/KEMs SMAUG-T and NTRU+. [27]. There is also a pilot project to verify the applicability of the Korean algorithms across various industries over four years until 2028 [28]. South-Korea published a migration plan [29] targeting 2035 for converting national systems to PQC.

The National Cyber Command Office (NCO) in Japan has set the target for migrating government agencies to PQC at 2035 in an interim report, based on similar timelines abroad [30] [31]. However, it does not provide a full roadmap for Japan nor finalize any PQC algorithm choices. The Cryptography Research and Evaluation Committees (CRYPTREC) provide technical guidelines for adopting, evaluating and implementing PQC in government systems [32].

Singapore is preparing a migration handbook [33]. This draft version urges organisations to begin planning now because PQC migration will be a multi year effort, but does not prescribe a completion date. The main message is to begin preparation early, adopt crypto-agility, and plan a phased, risk based transition to PQC. The handbook is complemented by the Quantum Readiness Index (QRI) [34], which is a voluntary self assessment tool developed by the Cyber Security Agency of Singapore (CSA) with industry

partners. Over the wider ASEAN region, there are overlapping regulatory frameworks that complicate PQC implementations. Organisations in the region need to take into account national, international and sector-specific standards. [35]

India's Telecommunication Engineering Centre has produced a technical report on migration to post-quantum cryptography, emphasizing early preparation, phased migration, and alignment with NIST PQC standards [36]. Hybrid schemes and crypto-agility are discussed in detail, but a timeline for the PQC migration is not specified.

Countries in the Anglosphere are following a largely similar path with guidance documents and timelines. The National Cyber Security Centre of the United Kingdom provides a clear timeline for UK industry, government and regulators: planning done by 2028, highest priority PQC migration by 2031 and full PQC migration by 2035 [37]. Canadian Centre for Cyber Security outlines similar milestones for the non-classified IT systems of the government [38], although initial planning is required already in 2026. The guidance provided to other organisation encourages starting preparations immediately and migrating once standards and validated implementations are ready [39]. Australia is recommending a slightly expedited timeline: a refined transition plan in place by the end of 2026, starting the transition by the end of 2028 and finishing by 2030 [40].

In Latin America, the degree of awareness of the quantum threat and engagement of the governments varies widely. An academic survey across Brazil, Mexico, Argentina, Colombia, and Chile finds that no Latin American country yet has dedicated PQC regulation. [41] The authors also consider the risk of relying too heavily on foreign standards and products in PQC, and encourage local research and development to mitigate this risk. There is a need for national PQC migration plans, regulation, regional and international cooperation and investment in talent pipelines to facilitate the transformation.

A white paper by the Africa Quantum Consortium [42] outlines a continental strategy focusing on sovereignty and sustainable development as Africa enters the quantum era. The paper argues that Africa should avoid duplication of effort, utilize the talent potential of its young and growing population and create a truly transnational model for quantum development. This strategy document discusses opportunities for various quantum technologies and is not focused on PQC.

In the Middle East, progress in PQC migration is uneven, with United Arab Emirates and Israel leading. UAE has approved a national encryption policy that urges government entities to formulate clear transition plans to PQC [43]. Israel has provided a document on best practices for organisational cyber-readiness [44] with a general assessment of a quantum timeline, placing post-quantum era at around 2035.

Overall, the global landscape of PQC migration is progressing rapidly but unevenly. There are differing national priorities and levels of technological maturity. Some regions have established specific timelines, while others suggest migration as soon as feasible, without specifying milestones or deadlines. Many regions are still in an exploratory phase of the process, lacking dedicated PQC regulation or even higher level strategy. This fragmentation increases the risk of interoperability challenges. Roadmaps and guidance documents commonly emphasize crypto-agility as an ongoing requirement, and recommend hybrid schemes specifically for the transition period. Global coordination efforts continue through standardisation bodies and multinational industry groups. As a result, we may see a convergence toward more harmonized PQC requirements in the future, even if the pace of implementation differs.

2.4 Finland's PQC Strategy in the European Context

Finland is following the European post-quantum cryptography roadmap by implementing national quantum strategies. The Finnish NCSC has stated that PQC transition steps should be initiated as soon as possible, using the EU PQC roadmap as the guiding principle [45]. Finnish national working group for cryptography also indicates, that all crypto-products coming to evaluation need PQC resilient key-factoring methods [46]. The working group also recommends following the European PQC roadmap. National Emergency Supply Agency (NESA) has also published a roadmap for PQC transition, which is largely identical to the EU PQC roadmap [47].

3 Sector-Specific Impacts and Regulatory Implications

This section provides a sector-specific analysis of the impacts and regulatory implications of post-quantum cryptography migration. We examine how evolving regulations and standards affect critical infrastructure, finance, telecommunications, and media industries, as these are the focus areas within the BLimPQC project. Each subsection highlights unique challenges, compliance requirements, and technical considerations relevant to PQC adoption within these sectors.

3.1 Critical infrastructure

There is no explicit PQC regulation related to critical infrastructure at the time of writing the report.

The EU Network Code on Cybersecurity (NCCS) [48] affecting cross-border electricity industry will have minimum and advanced cybersecurity controls defined by 2027, to be implemented in the high-impact perimeter in 2028. However, the exemption procedures of NCCS allow significant leeway, permitting up to three years at a time to delay implementation. In the provisional list of European and international standards and controls [49], existing IEC and NIST standards such as NIST SP 800-53 [50] are referenced and the use of the latest version of the standards is encouraged. PQC is therefore indirectly referenced in the upcoming requirements. The water sector in the United States operates mostly under non-binding best practices for cybersecurity. The America's Water Infrastructure Act [51] requires emergency response plan to be put in place that covers cybersecurity. However, this regulation does not reference concrete criteria but calls for *"strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system"*. The Environmental Protection Agency (EPA) provides best practice guidance, but has failed to enforce cybersecurity evaluations as part of mandatory surveys due to litigation [52].

In Operational Technology (OT) environments, integrity and authenticity are often more important cybersecurity goals than confidentiality. Additionally, retrofitting the plethora of vendor-specific protocols to use classical best practice encryption algorithms or PQC algorithms is often not feasible. Therefore it is likely that mitigations focus on tighter segmentation and access control, particularly when connected over the internet and adopting PQC on use cases and outer layer that share standardized protocols with the IT environments.

3.2 Finance

Even prior to DORA, financial organisations have been following strict cybersecurity practices. Some of the financial industry's compliance requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) [53] extend to other sectors as well. The PQC requirement is implicit with *strong cryptography based on industry-tested and accepted algorithms along with key lengths that provide a minimum of 112-bits of effective key strength* as some PCI-DSS reference standards, such as BSI TR-02102-1 [54], have been updated to include PQC algorithms.

In January 2026, G7 Cyber Expert Group (CEG) published a roadmap [55] to encourage a coordinated approach for migration to quantum-resistant cryptography and transition to cryptographic agility in financial industry. The risk-based assessment in existing compliance requirements allows leeway in transition scope and timeline.

In the past, the financial organisations have been simultaneously one of the first to require and adopt new cryptographic algorithms and the last to let go of the old algorithms. This also applies to the ongoing PQC transition. There are financial companies that have set their internal PQC migration target deadline to 2029 and are actively engaging vendors and partners to reach this goal. The regulatory landscape beyond cryptographic requirements may prove to be more challenging for the successful and timely migration. The intentionally rigid internal policies of many banks hinder not only PQC transition itself, but prerequisite software or protocol updates, such as update from Transport Layer Security (TLS) 1.2 to TLS 1.3 in the production environments.

3.3 Mobile Communications and Telecommunications

This section examines how regulation, governmental directives, and other regional, national (including Finland), and international requirements influence and shape the transition to post quantum cryptography in wireless mobile communications and telecommunications systems across Finland, the EU, the U.S., and global markets.

A comparative case study is used to analyse regulatory, policy, and security baseline requirements relevant to secure mobile communication and secure mobile device platforms for classified or otherwise sensitive information. The analysis will include requirements relevant to secure mobile communication and secure mobile device platforms for classified or otherwise sensitive information:

- Network security mechanisms (e.g., IPsec),
- Device management communication (e.g., TLS),
- Secure boot, secure enclave, device attestation, and mobile device platform assurance frameworks and network-independent applications in cellular network management communication (e.g., TLS).

3.3.1 Wireless mobile communications

Mobile communication standards have been specified by the 3rd Generation Partnership Project (3GPP) for 3G, LTE, and 5G, and it is expected that 3GPP will do the same for 6G. Already since 3G, regulators have been stakeholders and active participants in 3GPP work. The collaboration between regulators and industry is carried out in 3GPP in a seamless manner, i.e., regulators take an active role already when 3GPP defines its work plan. The list of regulators, industry participants, and requirements is included in the detailed work item. The specification progresses and is finalized with these work items.

Some security-related standards in 3GPP are based on initiatives from various regulators. Tsunami warning systems, broader public warning systems, and automatic emergency calls from cars in the event of accidents are among the causes of these initiatives.

As regards post-quantum cryptography, 3GPP TR 33.703 V0.3.0 [56] is a technical report on "Study on Transitioning to Post-Quantum Cryptography in 3GPP". The work item SA-250858 [57] includes the justification for transitioning to PQC in 3GPP. In addition to companies from several countries as supporting members, there were four governmental organisations: Federal Ministry for Economic Affairs and Climate Protection (BMWK) (German: Bundesministerium für Wirtschaft und Klimaschutz), Federal Office for Information Security (BSI) (German: Bundesamt für Sicherheit in der Informationstechnik), NIST, and Department for Science, Innovation and Technology (DSIT-UK). These German, British, and American organisations are expected to ensure that national regulations are implemented such that companies receive standards in time to meet all regulatory requirements.

The work item SA-250858 [57] refers to two governmental documents, "Timelines for migration to Post-Quantum Cryptography" [58] by the UK National Cyber Security Centre (NCSC) and the National Security Memorandum [59], released by the White House of the United States. These documents from the UK and the United States are substantial for defining the need for timelines of PQC transitions.

The NCSC of UK [58] presents the key milestones as:

- By 2028: defining migration goals and building an initial plan for migration.
- By 2031: carrying out early and highest-priority PQC migration activities, and refining the plan to have a thorough roadmap for completing migration
- By 2035: completing migration to PQC in all systems, services, and products.

Similarly, the national security memorandum [59] shows that the United States aims to prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, to mitigate as much quantum risk as feasible by 2035.

3.3.2 Satellite and Space Systems

Space systems and satellite communications are increasingly subject to regulatory and standardisation frameworks. Satellite constellations, emerging satellite business models, and associated ground infrastructure must comply with requirements from multiple regulators. One example is 3GPP, which has enabled use of satellite communications as part of the core network. Therefore, the regulations directing 3GPP apply equally to satellite constellations, which offer services to 3GPP networks such as 5G or 6G.

Regulatory influence is also evident in governmental satellite services, including mission-critical tactical networks and high assurance communication channels. In Europe, the impact of regulation can be observed through the activities of the European Cooperation for Space Standardisation (ECSS) [60], which develops harmonised standards for European space systems. Furthermore, Consultative Committee for Space Data Sytems (CCSDS) is now upgrading Space Data Link Security Protocol [61] to enforce PQC security for space systems, which are now mandatory by regulations. CCSDS standards typically reflect regulatory expectations across multiple regions, as the organisation brings together representative space agencies such as ESA (EU), NASA (United States), and JAXA (Japan).

3.3.3 Network Security (IPsec)

Post quantum cryptography significantly affects IPsec, given that IPsec relies on public key mechanisms (DH/ECDH) vulnerable to quantum-attacks. Regulatory bodies in Finland, the European Union, the United States, and other global regions increasingly mandate migration toward quantum resilient or hybrid PQC schemes. Below, we summarize PQC impacts on IPsec and reference the specific public sources from which the information is drawn [11], [62], [63].

Finland's national posture is tightly aligned with the EU's coordinated PQC transition efforts. Finland is a signatory of the European PQC Joint Statement (2024), where 18 European cybersecurity agencies, including Traficom, highlight the urgency of transitioning to quantum resistant cryptography. The statement emphasizes the high probability of a cryptographically relevant quantum computer emerging within the next decade and recommends adopting hybrid classical-and-PQC cryptography for critical systems such as IPsec [11]. The EU Coordinated Implementation Roadmap for Post Quantum Cryptography (2025) sets out the binding framework for PQC adoption across the Union. It identifies IPsec as part of "high risk critical systems" requiring early transition due to its use in cross border, governmental, and mobile communication infrastructures. The roadmap explicitly advises prioritizing NIST standard PQC algorithms (ML KEM, ML DSA) and encourages hybrid deployments to maintain interoperability during transition [62], [64].

The United States provides the most prescriptive regulatory requirements for transitioning network security, especially IPsec, to PQC. U.S. Federal Requirements Affecting IPsec mandates government wide cryptographic inventories and PQC transition planning. Executive Order 14144 (2025) requires PQC implementation "as soon as practicable", directly affecting IPsec VPNs across federal agencies. DHS/CISA PQC Migration Guidance prioritizes network-layer cryptography and explicitly lists IPsec tunnels as high-risk, long-lifespan systems requiring early PQC adoption. Federal procurement rules are expected to enforce PQC-capable IPsec as a requirement for national security or critical infrastructure vendors [12], [19], [63].

Beyond the EU and the United States, PQC transition roadmaps increasingly target VPN and IPsec-protected communication as early migration domains globally. Global IPsec relevant PQC impacts:

- Japan (NISC, CRYPTREC): Recommends hybrid PQC adoption for secure network communication; emphasizes long term confidentiality risks [32].
- Singapore (CSA): Identifies IPsec-based VPNs as first-wave PQC transition targets in the Quantum-Safe Migration Handbook (2025) [33].
- Canada (CCCS): Advises PQC migration planning for long lifespan encrypted traffic, including IPsec, within government and critical systems [38].

- Australia (ACSC): Recommends prioritizing PQC for IPsec tunnels used in national critical infrastructure [40].
- South Korea: Promotes PQC ready IPsec deployments in government and telecom sectors; has standardized local PQC algorithms such as HAETAE, AIMer, SMAUG-T [27].

All these jurisdictions view IPsec as requiring early PQC transition due to its widespread use in mobile, enterprise, government, and defense communication systems.

3.3.4 Device management communication (TLS)

TLS plays a critical role in securing management-plane communication, including configuration updates, authentication, telemetry exchange, provisioning, and policy distribution. Because TLS relies on public key algorithms vulnerable to quantum-attacks (RSA, ECDH, ECDSA), regulators classify it, like IPsec, as an early transition protocol in the PQC migration timeline. Management traffic often contains sensitive metadata, persistent credentials, and long lived secrets, making it highly exposed to "harvest now, decrypt later" threats. The sections below outline how PQC affects TLS secured management connections across Finland, the EU, the United States, and the global regulatory environment [11], [62], [63].

Finland's national cybersecurity posture reflects its participation in the European PQC Joint Statement (2024), where Traficom joined 17 other EU cybersecurity authorities in warning that the probability of cryptographically relevant quantum computers within 10 years is non negligible. The statement highlights the necessity of transitioning public key cryptography to PQC—especially in systems handling critical management-plane data. It recommends immediate deployment of hybrid PQC mechanisms for protocols such as TLS to ensure forward secrecy even if classical keys are later compromised [63]. Because device management platforms often store long-lived credentials, Finland's regulatory interpretation places significant emphasis on the early adoption of *hybrid PQC-TLS*, combining classical X.509 authentication with PQC signatures (e.g., ML-DSA), and PQC key exchange (ML-KEM).

The EU Coordinated Implementation Roadmap (2025) identifies TLS as one of the most critical protocols for early PQC migration. This is because management-plane TLS channels often protect long-term secrets, including device identities, EMM/MDM credentials, firmware signing chains, and policy distribution mechanisms [11], [62]. EU regulators also recommend shorter certificate validity periods and adoption of hybrid Certificate Authorities combining classical and PQC signatures during the transition. This directly impacts TLS management infrastructures, which depend heavily on CA trust chains [62].

Countries outside the EU increasingly classify TLS, and especially management-plane TLS, as a priority for PQC migration domain. Given U.S. procurement influence, PQC-TLS is expected to become a de facto requirement for all vendors servicing defense, federal, and critical infrastructure markets by 2030. Across all regulatory domains: Finland, EU, United States, and global, TLS for management-plane communication is consistently ranked as a first priority PQC migration target, alongside IPsec. The global recommendation is clear; Use of hybrid key exchanges, use of hybrid certificates, shorten certificate lifetime and update [12], [19], [27], [32], [33], [38], [40], [63], [64].

3.3.5 Telecommunications

Telecommunication networks form a large and complex international system of interconnected communication systems. Equipment from different vendors, governed and operated by commercial and government-regulated actors in different sovereign nations, must be able to interoperate in order for mobile connections to be established by end users also when they have roamed into a different country far from their home network. The globally interconnected nature of telecommunication networks emphasizes the importance of international standardisation bodies, such as 3GPP and GSMA, in establishing the technical means for the networks to maintain global connectivity. As telecommunication networks are also critical infrastructure at the national level, the sector is strongly regulated.

3GPP is in the process of standardizing post-quantum cryptography into 5G, and 6G is expected to be designed to be fully quantum resistant from the outset [65]. To a large extent, the protocol layers requiring

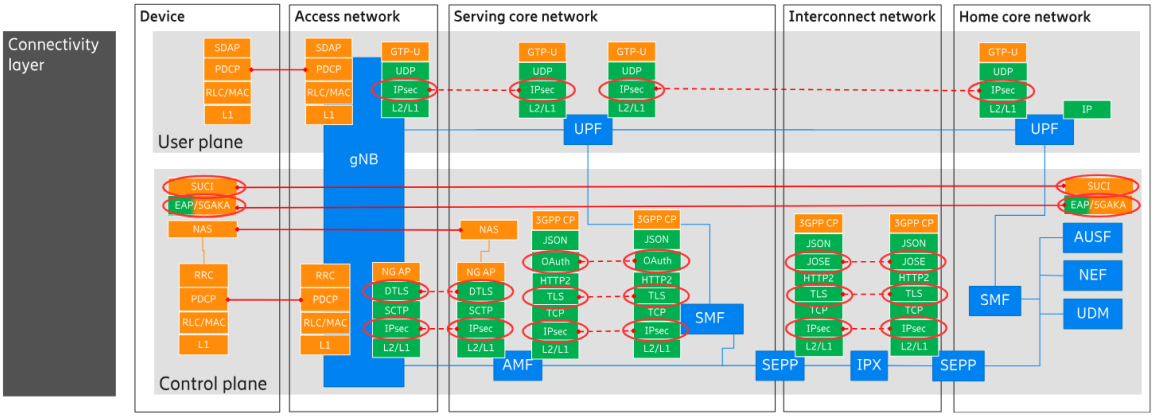

Figure 2: Upgrading the telecommunication network connectivity layer to quantum-resistant algorithms builds on underlying IETF standards [65]

updates to asymmetric cryptographic algorithms are located beneath those defined in familiar IETF RFCs, as illustrated in Figure 2.

5G relies on IETF protocols such as IKEv2, TLS 1.3, DTLS, JOSE, EAP TLS, and EAP AKA FS, as well as Public-Key Infrastructure (PKI) management mechanisms including the Internet X.509 profile, CMP, CRL, and OCSP, for nearly all uses of public key cryptography. IMSI encryption uses the SECG ECIES standard, augmented with X25519 (RFC 7748). Management and infrastructure layers also use public key cryptography in protocols such as DTLS SRTP, MIKEY SAKKE, ACE, COSE, and SSH, although management access is typically local and does not always require the same degree of interoperability.

In telecommunications standardisation, adopting a protocol relies on its specification being mature, and draft standards are generally not seen as sufficiently stable to reference. This has an impact on standardisation timelines, as 3GPP depends not only on the final NIST standards for the algorithms, but also on the stabilisation of any protocol level standards applying the new quantum-resistant algorithms.

In addition to quantum-resistance being highly visible in the network connectivity domain, very visible parts of telecommunication equipment are also long-lived hardware deployed into exposed areas. This means that the firmware updates and hardware-assisted firmware integrity protection of the equipment form a high-value target in need of quantum-resistance protection. Software and firmware signatures and remote attestation frameworks are vendor-specific solutions and are not standardized by 3GPP.

At the time of writing the report, telecommunication-specific regulation on quantum-resistant algorithms has not yet emerged, while the aforementioned general regulation promoting risk-aware security solutions applies to this area as well. National recommendations on algorithms to use and migration timelines have a strong impact on the field, as networking equipment is expected to comply to national guidelines. For example in EU, critical communication infrastructure would generally be seen as a high-risk target, and therefore would be expected to migrate by the earlier deadline of 2030.

The actual roll-out of the migration depends both on equipment vendors making the quantum-resistant algorithm solutions available, and on the operators deploying the solutions to their production environments. At a global scale, we can expect to see a combination of environments where quantum-resistant algorithms are in use, and legacy deployments that are vulnerable to quantum computers, and a need to find ways to interoperate between two different kinds of networks without compromising overall system security. Unlike enterprise IT inter-site virtual private networks, the international interconnections of telecommunication networks are not structurally compatible with adding protective point-to-point IPsec tunnels with special equipment for connecting to legacy equipment.

As systems must be able to interoperate across different geographical areas, it becomes particularly challenging to navigate any mutually conflicting cryptographical requirements, such as regional differ-

ences in algorithms, whether PKI elements are expected to use hybrid signatures or not, whether SLH-DSA is allowed as a conservative fallback algorithm or disallowed, and what secure hash algorithms are allowed for digests that are external to the largely SHA-3-utilizing algorithms themselves. Where possible, telecommunication is likely to continue to follow conservative options for security parameters: high security levels, hybridized key exchange, SHA-3 over SHA-2, stateless algorithms over stateful, hedged solutions to protect against compromised random number sources, and stable specifications over drafts and work in progress.

3.4 Media Systems

Media systems often rely on networked and cloud based infrastructures, making cryptographic mechanisms critical for protecting content throughout its lifecycle. The transition to post quantum cryptography introduces new considerations for media production, distribution, and authenticity.

3.4.1 Quantum Secure Media Delivery

This section focuses on the different needs of the enterprises and public sector for cyber-secure cloud and hybrid video service production, preparation, management, distribution and consumption in the PQC era. We will focus on European market to scope the work.

The standardisation has been touched on in the previous chapters, and it's implications can be mapped to the requirements of various organisations and their media/video value chain: production, preparation, management, distribution, consumption and retention. Within corporate environment, it is also vital for vendors to be able to "prove" their security frameworks, and this is where models like ISO 27001 become vital. Media software vendors will need crypto-agile architectures and ISO 27001 acts as a governance enforcement mechanism, whereas NIST/EU defines which algorithms to use. Furthermore, as the market is global, the algorithms must be global as well to ensure interoperability.

From organisational perspective, most media companies need to show security frameworks and compliance to ensure high quality content from major studios. ISO 27001 certification provides a good framework for this. ISO/IEC 27001 is the internationally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). While the standard does not prescribe specific cryptographic algorithms, it provides a risk-based governance framework that is highly relevant in the transition to post-quantum cryptography. Current cryptographic mechanisms such as RSA and ECC are vulnerable to quantum-attacks. Organisations must assess where these algorithms are used, regarding e.g. TLS, Digital Rights Management (DRM), and PKI, and the lifetime of protected data. This is particularly relevant for long-term media archives, sensitive public-sector video content and intellectual property in media production.

In cloud and hybrid video environments, where multiple systems and vendors interact, ISO 27001 enables coordinated action across technical, operational, and procurement domains. As a result, it is likely to be one of the primary mechanisms through which PQC adoption is implemented in both enterprise and public-sector media systems. ISO/IEC 27001 does not mandate PQC directly, but it forces organisations to act when risks are identified.

3.4.2 Impacts of PQC Technology on Media Production

In the context of this project, our focus is primarily on use cases emerging in media production, as well as on new media production standards that are being introduced. Particular attention is given to aspects that should be considered as post-quantum cryptography requirements evolve alongside the development of quantum computing. This discussion focuses mainly on electronic media production, since the methods used in text-based media production are largely similar to those used in general documentation.

For a long time, electronic media production relied on technical devices between which audio and video signals were transmitted via various cables or through separate, closed computer networks. During this period, information security received relatively little attention.

With the emergence of IP-based technologies and networked infrastructures, the challenges have increased. Initially, these challenges were mainly technical and related to digital signal processing, media transmission between devices over networks, and device control. In the de facto standards developed for these purposes, information security has not yet been particularly advanced. In recent years, more comprehensive standards have emerged. These standards are likely to remain in use for a long time, and therefore their PQC resilience should be examined more carefully.

Another important issue is that information security challenges in media production have increased significantly due to cybersecurity attacks, synthetic or misleading media, and AI-based media production. Security requirements have increased, for example with the wider adoption of ISO/IEC 27001:2022, but there have still been relatively few requirements regarding the monitoring of the internal technical architecture or structural composition of media service systems.

File-based systems have also raised concerns about media storage and encryption. Examples of high-risk content include medical records, movies, TV content, and legal material. In many cases, this content needs to be encrypted and currently various DRM platforms have been used. The industry standard providers are Google, Microsoft and Apple. It can be assumed that these vendors will find solutions for long-term PQC threats. DRM files are typically encrypted using AES (e.g. AES-128/CTR or CBC) and distribution is handled using HTTPS/TLS. The vulnerability is in license acquisition and key exchange which use RSA and ECC (ECDSA, ECDH) algorithms.

Within this project, the idea has emerged to monitor software structures and cryptographic structures in media production systems more closely using the concepts of Software Bill of Materials (SBOM) and Cryptographic Bill of Materials (CBOM). In the future, it may become common that media production system services are delivered with SBOM and CBOM documentation in a manner similar to ingredient lists on food packaging, enabling customers to track updates and changes related to information security.

3.4.3 Standards and Challenges in Media Production

As media production transitions to network- and cloud-based environments, new standards have emerged for device control, media transmission between devices, and verification of media authenticity. These standards need to be evaluated from the perspective of PQC. Below is a brief overview of relevant standards and their associated challenges.

Media Transmission: For media transmission over IP networks, traditional standardized methods have been used, including streaming protocols such as RTP, SRT, RIST, RTSP, HLS, DASH, XRTC, and WebRTC, and file transfer protocols such as FTP and HTTP. It should be noted that HLS and DASH operate over HTTP protocol, which natively support PQC via latest HTTPS3/TLS 1.3.

In live media delivery, low transmission latency is a critical requirement. This has led to the emergence of several proprietary platforms, including Zixi, LTN Network, and Haivision, which will need to adapt to post quantum cryptography.

From a standardisation perspective, the industry standard protocols Secure Reliable Transport (SRT) and Reliable Internet Stream Transport (RIST) are key technologies for reliable media transmission. A similar, partly overlapping standard is WebRTC.

SRT has gained wide acceptance among industry vendors because it provides an open source alternative for reliable audiovisual transport over unreliable networks. SRT uses AES encryption (typically AES 128 or AES 256) for payload data. Its key exchange mechanism is based on Diffie–Hellman (DH), and authentication relies on a pre shared passphrase (PSK). In the post quantum cryptography era, these handshake mechanisms represent a potential weak point and will need to be addressed.

Reliable Internet Stream Transport (RIST) is a standards-based video transport protocol developed by the Video Services Forum (VSF). It was created to enable interoperable, broadcast-grade video transport over IP networks, and is build on existing, well-understood standards (RTP/RTCP). RIST uses Datagram Transport Layer Security (DTLS) and thus provides TLS-equivalent security over UDP and strong encryption (AES-based). Stream authentication can be based on certificates similar to HTTPS/TLS. RIST's reliance on standardized security protocols (DTLS) positions it as a more future-proof candidate for post-

quantum migration compared to proprietary or custom-secured transport protocols, as it can inherit cryptographic advancements from the broader TLS ecosystem.

Device control typically relies on TCP/IP-based protocols or protocols operating over HTTPS, such as Ember+, which is used for media control, or MQ message-queue applications. In recent years, the SMPTE organisation has introduced the ST 2110 standard family for professional audio and video media transport. For media transfers, precise timing is critical and the PTP v2 is generally used in media production environments.

The SMPTE ST 2110 Standards Suite specifies the carriage, synchronisation, and description of separate elementary essence streams over IP for real-time production, playout, and other professional media applications. ST 2110 streams use the RTP protocol, which can be made relatively PQC-compatible through SRTP (RFC 3711), with the current exception of key exchange mechanisms. A similar challenge appears to exist with WebRTC. More and more media production is done in Containerised Cloud environments where media transfer delays play important role. In order to avoid delays, new architectures with Common Memory Sharing have been developed. These may possess new security and PQC challenges as the boundaries between protocols and architectures are challenged. An example of this is the MXL. MXL refers to the Media eXchange Layer of the EBU (European Broadcasting Union) Dynamic Media Facility (DMF) reference architecture.

Media Device Control: The ST 2110 standard itself does not address device discovery or device control. For this purpose, the Advanced Media Workflow Association (AMWA) has developed the Networked Media Open Specifications (NMOS). NMOS is an open-source set of protocols and associated software for discovery, registration, connection, and management of ST 2110 networks.

The NMOS standard relies on OAuth 2 authentication, which may not remain PQC-resistant over time. At the time of writing, the most commonly used media production device control protocol, Ember+, is entirely based on external security mechanisms and will likely evolve in the future.

From a PQC perspective [66], the most important aspect of media transmission and device control is monitoring the development of quantum computing. The primary requirement is that unauthorized parties must not be able to access data transmission or routing during system operation.

Media Authenticity: To address the issue of media content provenance and authenticity, the Coalition for Content Provenance and Authenticity (C2PA) initiative has been introduced as a project of the Joint Development Foundation [67]. The aim is to enable the tracking of media assets back to their original sources, including any changes made to the content.

When creating and modifying media content, *provenance data* is generated, digitally signed, and added to the media asset as metadata. The provenance data contains assertions—statements covering areas such as asset creation, edit actions, and capture device details—as well as previous provenance data [66], thereby cascading the history of the asset.

The provenance data is signed using PKI and the X.509 format. As a result, a subsequent user (a media producer, either a device or an organisation) or an end user can verify the origin and history of the content through a validation service.

It is noteworthy, within the scope of the BLimPQC project, that the current C2PA specification (version 2.3, dated January 5, 2026) permits exclusively non-PQC signature algorithms in X.509 certificates, namely RSA- and elliptic-curve-based algorithms. Although ML-DSA (and, in the future, FN-DSA) represents a PQC-compliant but currently non-deployed alternative, the BLimPQC project partners are preparing a formal communication to C2PA regarding plans for PQC compliance.

The adoption of the C2PA standard within media production chains is still at an early stage and is likely to take several years to become widespread. However, C2PA appears capable of accommodating PQC with only minor changes to the specifications. As stakeholders increasingly transition their infrastructure toward quantum resilience, partially mandated by regulation, it is important to ensure that all security mechanisms remain robust, mutually aligned, and compliant with best practices.

4 Discussion

This report has examined regulatory developments impacting the transition to quantum-resistant cryptography. At the time of writing, it has been slightly over a decade since the U.S. government set a new requirement to transition to cryptography that could resist attacks by quantum computers. NIST launched its PQC standardisation programme in 2017 as an open international effort, and finally settled on three standards in the first standardisation batch: ML-KEM for key exchange, ML-DSA and SLH-DSA for signatures. The final algorithm standards were completed in 2024. Between these milestones, a flurry of academic research, development efforts and cryptanalytic evaluation work was poured into the future of cryptography. In 2023–2024, the role of artificial intelligence in supporting side channel analysis of the new algorithms gained increased visibility in the media. During the same period discussion of side channel attacks and corresponding mitigations became an active and visible part of the algorithm standardisation process.

4.1 Regulation, Standardisation, and Market Dynamics

Regulations create binding obligations: they define who must act, when action is required, and what the legal consequences of non-compliance are. Standards, in contrast, define the technical means that make compliance feasible, including algorithm choices, parameter sets, test vectors, and interoperability profiles. In practice, regulation and standardisation are tightly coupled. Regulation is not the place for discovering new cryptographic solutions; it must rely on sufficiently mature standards that have undergone open evaluation and broad scrutiny.

In standardisation, there is a ”sweet spot” somewhere between a technology becoming mature enough for early adopters and reaching widespread use, where a well placed standard supports common adoption and protects implementations from diverging into multiple mutually incompatible branches responding to the same need. Regulators face a similar balancing act: the primary goal of ensuring sufficient security investment in society is balanced with the need to not forcefully push implementations down a road that could turn out to be a dead end. In the context of PQC, some government sectors have already imposed requirements through procurement policies, while public cybersecurity authorities have issued strong recommendations to organisations more broadly.

Market forces also play a significant role. Well-positioned industry actors, for example browser vendors or cryptographic library maintainers, may adopt new mechanisms faster than formal standardisation bodies, effectively establishing de facto standards through early and ubiquitous deployment. At the same time, legacy and embedded systems with long lifecycles may struggle to meet regulatory deadlines without costly retrofits or full replacement. As PQC migration accelerates, organisations are therefore well advised to invest in cryptographic inventories, crypto-agility, and, where appropriate, hybrid cryptographic schemes to protect their assets.

Across jurisdictions, government guidance to public institutions, industry, and society at large consistently emphasizes three core themes:

- The importance of risk-aware oversight on protection targets and their features, which is a necessity for controlled migration planning and prioritisation,
- The communication of urgency through tight and internationally aligned timelines, and
- The scoping to focus migration efforts around effective algorithms and solutions developed through an open and public evaluation process to minimize the risk of new algorithm adoption.

4.2 Regulatory Approaches and Timelines

There are two approaches to the regulation of the PQC transition. Soft guidance approaches, such as the EU PQC roadmap, rely on the self interest of states and companies to take the necessary steps to achieve quantum resilience. This approach is well suited to collaborative frameworks like the European Union,

as it allows flexibility between actors and accommodates different national starting points. It also allows companies to assess the level of investment required to meet their specific needs. However, this also implies that some companies may choose to invest less time and effort. The consequences for those entities will depend on how rapidly quantum decryption threats are realised.

In contrast, some entities, such as the U.S. federal system, are taking a hard mandate approach with binding deadlines and reporting obligations. While the requirements of the regulation formally apply to federal agencies, they effectively extend to any vendors providing services to these organisations, forcing them to take PQC capabilities seriously. As the U.S. federal government is a huge customer, this in reality requires the vendors to migrate to PQC in a competitive manner.

In addition to formal regulation, large customers can exert significant influence through procurement and contractual requirements. In sectors such as finance, telecommunications, and public services, security requirements imposed by customers often reinforce regulatory expectations and accelerate the adoption of PQC-compliant solutions across vendor ecosystems.

In Finland, PQC related regulation not only affects organisations subject to compliance requirements, but also has broader societal implications. The obligations of the NIS2 [1] directive require the use of effective encryption technologies, and based on that, Finnish National Cybersecurity Strategy and its implementation plan explicitly links cybersecurity to comprehensive national security. From this perspective, PQC migration is also a matter of security of supply and long term societal resilience.

At present, the PQC transition timeline primarily consists of preliminary actions intended to identify and align key market actors affected by the eventual failure of non PQC algorithms. As the situation matures, stronger regulatory measures are likely to emerge, granting certain national authorities (such as national CERTs) greater mandate to require and verify the use of encryption in products. As regulatory pressure increases, companies will likely respond by positioning their products as compliant solutions. In this context, PQC compliance is likely to provide a competitive advantage for companies able to deliver such solutions in a timely manner.

4.3 Supply-Chains, Dependencies, and Adoption Friction

In practice, PQC migration is shaped by complex dependencies across supply-chains. In Figure 3, we depict this by dividing vendors into ”first-tier” and ”second-tier” vendors, or vendors of building blocks and vendors who combine those building blocks into end products or services that users will interact with. This means that, in a supply-chain, second-tier vendors, who may be the direct targets of regulation, will in practice need to wait for first-tier vendors to implement the features required to fulfil regulatory demands. These dependencies contribute to delays in large-scale migrations, such as the transition to quantum resistant cryptography. Ultimately, the user at the end of the supply-chain is only able to use a quantum-resistant cryptography product once both first- and second-tier vendors have made the necessary functionality available. The end user organisation, whether public or private, or even an individual, may also be a direct target of government regulation and, in any case, bears the ultimate risk of security breaches.

In the specific case of Public-Key Infrastructures, the standardisation of NIST PQC algorithms in 2024 marked an important milestone. By early 2026, hardware security modules and PKI toolchains are in the process of integrating these algorithms and the associated protocol changes. While the technical foundations for initial deployment are emerging, the pace of adoption beyond this point is increasingly driven by organisational prioritisation, regulatory pressure, customer requirements, and risk assessments.

4.4 Global Interoperability and Crypto-Agility

The Internet and many digital services operate on a global scale, whereas regulation remains regionally bounded. This creates a persistent risk of misaligned requirements across jurisdictions, potentially threatening interoperability, for example, in areas such as PKI, where trust anchors and certificate chains often span national borders. Global vendors must therefore navigate multiple regulatory environments simultaneously, increasing the importance of crypto-agility as a design principle.

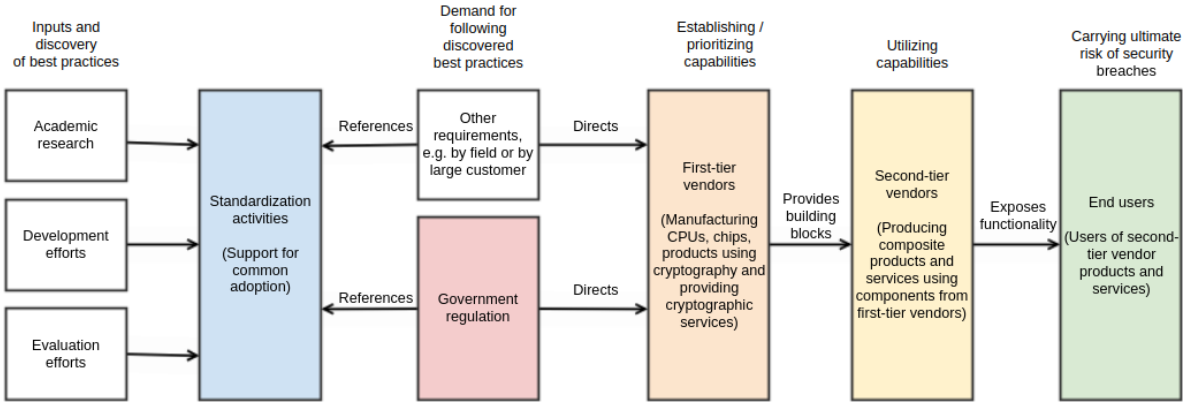

Figure 3: Summary of the impact of regulation on the infrastructure transition.

Crypto-agility enables organisations to support multiple algorithms, parameter sets, and transition strategies without repeated large-scale redesigns. It also mitigates the risk of regulatory fragmentation by allowing systems to adapt as standards evolve or diverge across regions.

4.5 Uncertainty, Legacy Systems, and Long-Tail Migration

Preparing for future threats presents a well-known paradox: If the preparation is successful, the horror-scenarios do not materialize, and more pressing matters will dominate the news cycles. Conversely, failure to prepare will lead to highly visible incidents and public scrutiny. In the case that the preparation is successful, the resources used might even look misplaced or excessive, becoming material for conspiracy theories and proof of mismanagement or government overreaction.

The appropriate level of effort for the PQC transition is difficult to determine. This is especially true for quantum threats, as they remain theoretical at the time of writing. However, the rate at which quantum capabilities are advancing indicates that the processing power required for practical attacks is drawing closer.

Uncertainty about timelines can also slow adoption. In some cases, organisations may delay deploying available PQC solutions while waiting for additional guidance, tooling, or hybridisation mechanisms, fearing that early choices may not meet future regulatory expectations. Such dynamics can paradoxically decelerate migration even when technical solutions exist.

In order to predict how long a transition will take, we can try to compare this transition to an earlier cryptographic transition. For example, SHA 1 was standardized in 1993. Since 2005 [68], it has not been considered secure against well funded opponents due to collision attacks discovered against the algorithm, and as of 2010 many organisations have recommended that it be replaced. NIST deprecated SHA 1 in 2011. In 2017, a practical attack dubbed “SHAttered,” implementing the ideas from the 2005 paper, gained high visibility as a demonstration of SHA 1 being practically breached, and major web browsers stopped accepting SHA 1 based certificates. Microsoft discontinued SHA 1 code signing support for Windows Update in 2020. NIST has announced that SHA 1 should be phased out by the end of 2030. This transition involved a theoretical attack identified more than 20 years ago, a practical attack against the hash algorithm 12 years later, and major browser rejection occurring at roughly the same time. The long tail of PKI replacements may still be ongoing. We can expect a similarly long tail for PQC replacement, although applications where security is critical are likely to apply different prioritisation.

Disclaimer

Microsoft Copilot was used to access and translate resources in Chinese, Japanese and Spanish. Official English translations by the source were preferred whenever they were available. AI was used for grammar and consistency checks at the editing phase as well.

References

[1] European Parliament and Council, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, Text with EEA relevance, Dec. 14, 2022. Accessed: Dec. 12, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[2] European Parliament and Council, *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, Text with EEA relevance, Dec. 14, 2022. Accessed: Dec. 12, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554.

[3] European Parliament and Council, *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) No 168/2013 and Regulation (EU) 2019/1020 and Directive (EU) 2020/1828*, Mar. 13, 2024. Accessed: Dec. 12, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[4] European Parliament and Council of the European Union. "Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC." Consolidated version in force as of 28 December 2024 (Text with EEA relevance), Accessed: Mar. 27, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014L0053-20241228.

[5] H. R. O. T. U. F. F. AFFAIRS and S. POLICY, *The EU's Cybersecurity Strategy for the Digital Decade*, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, Dec. 16, 2020. Accessed: Jan. 20, 2026.

[6] The European Parliament and the Council of the European Union, *Regulation (EU) 2016/679 of the european parliament and of the council*, Official Journal of the European Union, 1:1–88, May 4, 2016. Accessed: Jan. 20, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[7] The Council of the European Union, *COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information*, Oct. 15, 2013. Accessed: Jan. 20, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN.

[8] The Council of the European Union, *COMMISSION DECISION (EU) 2022/640 of 7 April 2022 on implementing rules for the roles and responsibilities of the principal security actors*, Apr. 7, 2022. Accessed: Jan. 20, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D0640.

[9] B. D. et al, *Post-Quantum Cryptography-Integration Study*, https://www.enisa.europa.eu/sites/default/files/publications/Post%20Quantum%20Cryptography-%20Integration%20Publication.pdf, version 1, Oct. 1, 2022. Accessed: Jan. 16, 2026.

[10] European Comission, *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography, Jun. 23, 2020. Accessed: Jan. 28, 2026.

[11] NIS Cooperation Group, EU PQC Workstream, *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography, version Part 1, Version 1.1, First deliverable of the NIS CG work stream on PQC; aimed at EU Member States, Jun. 11, 2025. Accessed: Dec. 12, 2025.

[12] *Public Law 117-260: To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes*, Dec. 21, 2022. Accessed: Dec. 12, 2025. [Online]. Available: https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf.

[13] The White House, *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, , Directs federal agencies to plan a transition to PQC and addresses quantum-era cryptographic vulnerabilities, May 2022.

[14] O. of Management and B. (OMB), *Memorandum M-23-02: Migrating to Post-Quantum Cryptography*, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf, Operational guidance to federal agencies for inventory and migration planning to PQC, Nov. 2022.

[15] Department of Defense Chief Information Officer. "Preparing for Migration to Post-Quantum Cryptography." Memorandum providing Department of Defense guidance and requirements for planning and coordinating migration to post-quantum cryptography, Accessed: Mar. 27, 2026. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/PreparingForMigrationPQC.pdf.

[16] E. O. of the President, *Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity*, Executive Order 14144, Federal Register, Mandates agency implementation of post-quantum cryptography, 2025.

[17] E. O. of the President, *Modification of Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity*, Executive Order Modification, Revises PQC implementation requirements with emphasis on risk-based prioritization, 2025.

[18] The White House, *Executive order 14306: Sustaining select efforts to strengthen the nation's cybersecurity and amending executive order 13694 and executive order 14144*, Executive Order, Accessed March 2026, Jun. 2025. [Online]. Available: https://www.govinfo.gov/content/pkg/DCPD-202500669/pdf/DCPD-202500669.pdf.

[19] U.S. Department of Homeland Security, "Post-Quantum Cryptography: Roadmap and Guidance for Organizations," DHS, Tech. Rep., 2023. [Online]. Available: https://www.dhs.gov/publication/preparing-post-quantum-cryptography-infographic.

[20] Cybersecurity and Infrastructure Security Agency, "Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools," CISA, U.S. Department of Homeland Security, Tech. Rep., 2024, Guidance document. [Online]. Available: https://www.cisa.govsites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf.

[21] P. Kampanakis, M. Manzano, D. Connolly, S. Jamshidi, and A. Bosarge. "International PQC Requirements." PQCC publication, Post-Quantum Cryptography Coalition (PQCC), Accessed: Feb. 6, 2026. [Online]. Available: https://pqcc.org/international-pqc-requirements/.

[22] "Next-generation Commercial Cryptographic Algorithms Program (NGCC)), Official english website." Official website providing notices, proposals, and information services on commercial cryptography standards, Institute of Commercial Cryptography Standards, Accessed: Feb. 6, 2026. [Online]. Available: https://www.niccs.org.cn/en/.

[23] M. Swayne. "China Launches its own Quantum-Resistant Encryption Standards, Bypassing US Efforts." News article, The Quantum Insider, Accessed: Feb. 6, 2026. [Online]. Available: https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/.

[24] W. Meng. "Accelerating the Deployment of China's National Standard and Industrialisation of Quantum Resistant Cryptography (PQC): Proposal for Building National Security "Double Insurance" in the Quantum Era." SSRN preprint. Posted: 2025-09-08, Accessed: Feb. 6, 2026. [Online]. Available: https://ssrn.com/abstract=5402545.

[25] Standing Committee of the National People's Congress of the People's Republic of China, *Cryptography Law of the People's Republic of China*, http://www.npc.gov.cn/englishnpc/c2759/c23934/202009/t20200929_384279.html, Order No. 35; adopted Oct. 26, 2019; effective Jan. 1, 2020, Oct. 2019. Accessed: Feb. 24, 2026.

[26] "FedRAMP Policy for Cryptographic Module Selection and Use," FedRAMP, Board-approved policy v1.1.0, Jan. 16, 2025. Accessed: Feb. 24, 2026. [Online]. Available: https://www.fedramp.gov/resources/documents/FedRAMP_Policy_for_Cryptographic_Module_Selection_v1.1.0.pdf.

[27] "KpqC Algorithms," Korean Post-Quantum Cryptography (KPQC) Research Group, Accessed: Feb. 6, 2026. [Online]. Available: https://kpqc.or.kr/contents/03_exhibit/sub_03.html.

[28] J. Kim. "'Unbreakable National Encryption with Quantum Technology'... Government Launches Pilot Project." News article, The Asia Business Daily, Accessed: Feb. 6, 2026. [Online]. Available: https://www.asiae.co.kr/en/article/2025031409333595112.

[29] "Pan-National Post-Quantum Cryptography Transition Master Plan," National Cyber Security Center (NCSC), National Intelligence Service (NIS), Ministry of Science and ICT (MSIT), Government of the Republic of Korea, Seoul, South Korea, Tech. Rep., Jul. 2023, Translated title. Original Korean title (romanized): Pan gukga Yangjanaeseong amho Jeonhwan Maseuteopeullaen (2023.7). [Online]. Available: https://www.ncsc.go.kr:4018/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=59449.

[30] M. Stubbs. "2035: Japan's NCO Sets the Timeline for Quantum Security." News article, PQShield, Accessed: Feb. 6, 2026. [Online]. Available: https://pqshield.com/2035-japans-nco-sets-the-timeline-for-quantum-security/.

[31] "Interim Summary on the Migration to Post-Quantum Cryptography (PQC) for Government Agencies," Cabinet Secretariat, National Cyber Security Center (NCSC), Government of Japan, Nov. 2025, Translated title. Original Japanese title (romanized): Seifu Kikan nado ni okeru Tai-Ryoushi Keisanki Angou (PQC) e no Ikou ni tsuite (Chuukan Torimatome). Accessed: Feb. 6, 2026. [Online]. Available: https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf.

[32] "CRYPTREC Cryptographic Technology Guidelines." Official guideline index page containing documents such as the 2024 Post-Quantum Cryptography Guideline (in Japanese), CRYPTREC (Cryptography Research and Evaluation Committees), Accessed: Feb. 6, 2026. [Online]. Available: https://www.cryptrec.go.jp/en/tech_guidelines.html.

[33] "Quantum-Safe Migration Handbook, Draft for Public Consultation," Cyber Security Agency of Singapore (CSA), Government Technology Agency (GovTech), and Infocomm Media Development Authority (IMDA), version 0.1, Oct. 23, 2025, Draft released for public consultation; produced with contributions from private and public-sector partners. Accessed: Feb. 6, 2026. [Online]. Available: 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.

[34] "Quantum Readiness Index, Draft for Public Consultation," Cyber Security Agency of Singapore (CSA), Oct. 2025, Draft version of the Quantum Readiness Index, developed with input from multiple industry and government partners. Accessed: Feb. 6, 2026. [Online]. Available: 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.

[35] WQS. "Post-Quantum Cryptography Migration Blueprint for ASEAN CISOs." Industry guidance, World Quantum Summit (WQS), Accessed: Feb. 6, 2026. [Online]. Available: https://wqs.events/post-quantum-cryptography-migration-blueprint-for-asean-cisos/.

[36] "Migration to Post Quantum Cryptography, Final Technical Report (TEC 910018:2025)," Telecommunication Engineering Centre (TEC), Department of Telecommunications, Government of India, Mar. 28, 2025. Accessed: Feb. 6, 2026. [Online]. Available: https://www.tec.gov.in/pdf/TR/Final%20technical%20report%20on%20migration%20to%20PQC%2028-03-25.pdf.

[37] "Timelines for Migration to Post-Quantum Cryptography," National Cyber Security Centre (NCSC), United Kingdom, Accessed: Feb. 6, 2026. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[38] "Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada, Management series, ITSM.40.001," Canadian Centre for Cyber Security, Accessed: Feb. 6, 2026. [Online]. Available: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001.

[39] "Preparing Your Organization for the Quantum Threat to Cryptography, Awareness series, ITSAP.00.017," Canadian Centre for Cyber Security, Accessed: Feb. 6, 2026. [Online]. Available: https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.

[40] Australian Cyber Security Centre (ACSC). "Planning for Post-Quantum Cryptography, Updated Guidance (September 2025)," Australian Signals Directorate, Accessed: Feb. 6, 2026. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2025-09/Planning%20for%20post-quantum%20cryptography%20%28September%202025%29.pdf.

[41] B. Riquelme and J. Pereyra, "Ciberseguridad poscuántica en américa latina: Desafíos y estrategias regulatorias," Post-Quantum Cybersecurity in Latin America: challenges and regulatory strategies, *Perspectivas: Revista de Ciencias Jurídicas y Políticas*, vol. Año VII, no. 12, pp. 1–19, Jul. 2025, Received: 2025-03-21; Accepted: 2025-05-01. Accessed: Feb. 6, 2026. [Online]. Available: https://repositorio.ucalp.edu.ar/server/api/core/bitstreams/c8d48784-39aa-4f84-8a29-38b399681eec/content.

[42] Africa Quantum Consortium. "Africa's Quantum Horizon: A Unified Strategy for Sovereignty and Sustainable Development. "[Online]. Available: https://africaquantum.org/whitepaper.html.

[43] E. Al Helou. "UAE Announces Approval of National Encryption Policy, Issuance of Executive Regulation," Accessed: Feb. 12, 2026. [Online]. Available: https://economymiddleeast.com/news/uae-announces-approval-of-national-encryption-policy-issuance-of-executive-regulation/.

[44] CYBER ISRAEL, "Best practices: Organizational cyber readiness to the post-quantum age (v1.85)," Israel National Cyber Directorate, Tech. Rep., 2022. [Online]. Available: https://www.gov.il/BlobFolder/generalpage/quantum_computing/he/Best%20Practices%20-%20Organizational%20Cyber%20Readiness%20to%20the%20Post-Quantum%20Age%20v.1.85.pdf.

[45] Traficom, *Siirtymä kvanttiturvallisiin salausmenetelmiin*, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat//ajankohtaista/ohjeet-ja-oppaat/pqc-kvanttiturvallinen-salaus-3, version 1, 2026. Accessed: Feb. 27, 2026.

[46] Traficom, *Suomen kansallisen kryptoryhmän linjaukset kansallisiin PQC-salaustuotearviointeihin 1.1.2026 alkaen*, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomen-kansallisen-kryptotyoryhman-linjaukset-kansallisiin-pqc, version 1, Oct. 3, 2025. Accessed: Feb. 27, 2026.

[47] "Data Security Impacts of Quantum Computing – Preparedness Recommended," National Emergency Supply Agency (Huoltovarmuuskeskus), 2024, Prepared by the National Emergency Supply Organisation's Digipool and VTT Technical Research Centre of Finland Ltd. [Online]. Available: https://www.huoltovarmuuskeskus.fi/files/3a17a4fc1889b0c36cfe61b950d14b82a36e8a59/hvk-datasecurityimpactsofquantumcomputing-2024-saavutettava.pdf.

[48] "Network code on cybersecurity for the electricity sector," Accessed: Feb. 24, 2026. [Online]. Available: https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en#network-code-on-cybersecurity.

[49] "ENTSO-E Provisional list of European and international standards and controls," Accessed: Feb. 24, 2026. [Online]. Available: https://www.entsoe.eu/network_codes/nccs/#deliverables.

[50] "NIST SP 800-53 Rev. 5," Accessed: Feb. 24, 2026. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[51] "America's Water Infrastructure Act," Accessed: Mar. 13, 2026. [Online]. Available: https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf.

[52] "Withdrawal of Cybersecurity Memorandum of March 3, 2023," Accessed: Mar. 13, 2026. [Online]. Available: https://www.epa.gov/system/files/documents/2023-10/action-memo_rescinding-cyber-memo_october-2023.pdf.

[53] "Payment Card Industry Data Security Standard, Requirements and testing procedures, version 4.0.1," PCI Security Standards Council, Accessed: Feb. 10, 2026. [Online]. Available: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf.

[54] "Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102-1 2026-01," Federal Office for Information Security (BSI), Accessed: Feb. 10, 2026. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.

[55] "G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector: January 2026, Policy paper," G7 Cyber Expert Group (CEG), Accessed: Feb. 10, 2026. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.

[56] 3GPP, "Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP," 3GPP, Technical Report TR 33.703 V0.4.0, 2026.

[57] 3GPP, "Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP," 3GPP, Work Item SP-250858, 2025.

[58] National Cyber Security Centre - NCSC, *Timelines for migration to post-quantum cryptography*, 2025. Accessed: Mar. 19, 2026. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[59] U.S. Executive Office of the President, "Migrating to Post-Quantum Cryptography," Memorandum M-23-02, 2022. Accessed: Mar. 20, 2026. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.

[60] "European Cooperation for Space Standardisation (ECSS)," European Space Agency and European Space Industry, Accessed: Mar. 27, 2026. [Online]. Available: https://ecss.nl/.

[61] *Space Data Link Security Protocol*, Consultative Committee for Space Data Systems (CCSDS), 2022. Accessed: Mar. 27, 2026. [Online]. Available: https://ccsds.org/Pubs/355x0b2.pdf.

[62] M. Ivezic, *EU Commission Roadmap Targets 2030 for Post-Quantum Cryptography Transition*, Section: Quantum Policy, Standards & Regulation News, 2025. Accessed: Mar. 19, 2026. [Online]. Available: https://postquantum.com/quantum-policy/eu-pqc-roadmap/.

[63] EU Member States, "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography," Joint Statement, 2024. Accessed: Mar. 20, 2026. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3.

[64] K. Patil, *The EU Just Released a New Post-Quantum Cryptography (PQC) Roadmap: Here's What You Need to Know*, 2025. Accessed: Mar. 19, 2026. [Online]. Available: https://securityboulevard.com/2025/07/the-eu-just-released-a-new-post-quantum-cryptography-pqc-roadmap-heres-what-you-need-to-know/.

[65] J. P. Mattsson. "Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale." IETF 123 Meeting, Host Speaker Series, Accessed: Mar. 25, 2026. [Online]. Available: https://datatracker.ietf.org/doc/slides-123-ietf-sessd-ietf-123-host-speaker-slides-00.

[66] "Content Credentials; C2PA Technical Specification," Accessed: Mar. 20, 2026. [Online]. Available: https://spec.c2pa.org/specifications/specifications/2.3/specs/_attachments/C2PA_Specification.pdf.

[67] "About coalition for content provenance and authenticity (C2PA)," Accessed: Mar. 20, 2026. [Online]. Available: https://c2pa.org/about/.

[68] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *Advances in Cryptology – CRYPTO 2005*, V. Shoup, Ed., ser. Lecture Notes in Computer Science, vol. 3621, Springer, 2005, pp. 17–36, ISBN: 978-3-540-28114-6. DOI: 10.1007/11535218_2.

A Summary of PQC migration timelines

Table 1: Summary of PQC migration timelines. If an explicit migration deadline was found for high risk systems or for overall migration, we have included it in the table.

Region	Planning	High risk systems	Full migration
European Union	Initiate national PQC transition strategy by end of 2026	2030	2035
United States (Federal)	Required migration plan, cryptographic inventories		2035
China	Ongoing national PQC standards competition, advanced in QKD		
South Korea	National plan, piloting national PQC standards		2035
Japan	Interim report, no full roadmap		2035
Singapore	Draft handbook, start planning now		
India	Technical report for PQC migration		
United Kingdom	Planning complete by 2028	2031	2035
Canada	2026 for federal non classified IT	2031	2035
Australia	Refined plan by end of 2026	2028	2030
Latin America	(No formal plans)		
Africa	(No formal plans)		
United Arab Emirates	PQC regulation in place, immediate planning		
Israel	Immediate planning		2035
Finland	Align with EU roadmap, immediate planning	2030	2035