CEPS
TASK FORCE REPORT

STRENGTHENING THE EU TRANSITION TO A QUANTUM-SAFE WORLD

Technology, market, governance and policy challenges

Rapporteurs

Lorenzo Pupillo
Swann Ashworth
Afonso Ferreira
Carolina Polito

DECEMBER 2025

CEPS is an independent think tank based in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe and the world.

This CEPS Task Force report builds on the debates of the CEPS Task Force on 'Strengthening the EU transition to a quantum-safe world'. The Task Force was composed of industry experts, representatives of European institutions and agencies, academics, researchers, civil society organisations and practitioners. The group's activity began in April 2025, meeting on five separate occasions and continuing until November 2025.

The Coordinator of the Task Force acknowledges the invaluable contributions of all the participants. Thanks also go to the members of Advisory Board: Sofia Lindskov Hansen at the Danish Ministry of Foreign Affairs, Michele Mosca at Waterloo University, Michael Osborne at the IBM Research Division in Zurich, Bart Preenel at KU Leuven and Tim Watson at the Alan Turing Institute in London. The Coordinator would also like to thank the rapporteurs Swann Ashworth Carolina Polito and Afonso Ferreira. The Coordinator also thanks Jaime Gómez García, Matthias Schunter, Kevin Reifsteck, John Mattsson and Laima Jančiūtė for their extensive comments on the draft of the report. Finally, the Coordinator also acknowledges the editing expertise of Deborah Mulhearn, Julien Libert and Daniel Cassidy-Deketelaere.

The recommendations of this report do not necessarily reflect a common position reached by all members of the Task Force. Nor do they represent, in any manner, the views of their respective institutions. A list of members, meetings and speakers are in the appendices.

Suggested citation: Pupillo L. et all. (2025), *Strengthening the EU transition to a quantum-safe world. Technology, market, governance and policy challenges*, Task Force Report, Centre for European Policy Studies, Brussels.

978-94-6138-799-8

Image credit: www.vecteezy.com

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229 39 11
email: info@ceps.eu
www.ceps.eu

CONTENTS

FIGURES

BOXES

TABLE

List of Abbreviations

3DES	Triple Data Encryption Standard
3GPP	Third Generation Partnership Project
AES	Advanced Encryption Standard
ANSSI	National Agency for Information Systems Security (France)
API	Application programming interface
AQHKE	Authenticated quantum-safe hybrid key establishment
ATM	Automated teller machine
BIS	Bank for International Settlements
BSI	Federal Office for Information Security (Germany)
C4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
CENELEC	European Committee for Electrotechnical Standardization
CEPS	Centre for European Policy Studies
CISA	US Cybersecurity and Infrastructure Security Agency
CPU	Central processing unit
CRA	Cyber Resilience Act
CRQC	Cryptographically relevant quantum computer
CV-QKD	Continuous variable quantum key distribution
DEI	Diversity, equity and inclusion
DORA	Digital Operational Resilience Act
ECB	European Central Bank
ECC	Elliptic-curve cryptography
ECDSA	Elliptic-Curve Digital Signature Algorithm
ECDH	Elliptic-Curve Diffie-Hellman
ECDHE	Elliptic-Curve Diffie-Hellman Ephemeral
EDA	European Defence Agency
EDF	European Defence Fund
EDT	Emerging and disruptive technology
eIDAS	Electronic Identification, Authentication and Trust Services Regulation

EMV	Europay, Mastercard, and Visa
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROQCI	European Quantum Communication Infrastructure
FCA	Financial Conduct Authority
FFIEC	Federal Financial Institutions Examination Council
FIPS	US Federal Information Processing Standards
FN-DSA	Fast-Fourier transform over NTRU-Lattice-Based Digital Signature Algorithm
FS-ISAC	Financial Services Information Sharing and Analysis Centre
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HQC	Hamming Quasi-Cyclic
HSM	Hardware security module
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKEV2	Internet Key Exchange Protocol Version 2
IND-CPA	Indistinguishability under chosen plaintext attack
IPSEC	Internet Protocol Security
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union – Teleco. Standardisation
KDF	Key derivation function
KEM	Key Encapsulation Mechanisms
LMS	Leighton-Micali Signature
LTS	Long Term Support
MAD	Magnetic anomaly detectors
MAD-XR	Magnetic anomaly detector – extended role
ML-KEM	Module-Lattice Key Encapsulation Mechanism

ML-DSA	Module-Lattice-Based Digital Signature Algorithm
NATO	North Atlantic Treaty Organisation
NCCOE	US National Cybersecurity Centre of Excellence
NCSC	UK National Cyber Security Centre
NGCC	Next-generation commercial cryptographic algorithms
NIS	Network and information systems
NIS2	Network and Information Security Directive 2
NISQ	Noisy intermediate-scale quantum
NIST	US National Institute of Standards and Technology
NSA	US National Security Agency
NSM-10	National Security Memorandum 10
OCSP	Online Certificate Status Protocol
ORAM	Oblivious Random Access Memory
OT	Operational technology
OTNSEC	Proprietary Security Protocol for Optical Transport Networks
PIR	Private information retrieval
PKI	Public-key infrastructure
PNT	Precision navigation and timing
PQC	Post-quantum cryptography
PRNG	Pseudo-random number generator
PSK	Pre-shared key
PSI	Private set intersection
QDNL	Quantum Delta NL
QKD	Quantum key distribution
QRNG	Quantum random number generator
R&D	Research and Development
RSA	Rivest-Shamir-Adleman Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAGE	Security Algorithms Group of Experts
SBOM	Software Bill of Materials

SD-WAN	Software-defined network
SHA	Secure Hash Algorithm
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TLS	Transport Layer Security
TQC	Transatlantic Quantum Community
TRL	Technology readiness level
TRNG	True random number generator
UK	United Kingdom
US	United States
VPN	Virtual private network
WEF	World Economic Forum
XMSS	eXtended Merkle Signature Scheme

PREFACE

This report is based on discussions of the Centre for European Policy Studies (CEPS) Task Force on Strengthening the EU Transition to a Quantum-Safe World. The Task Force was composed of industry experts, representatives of European institutions and agencies, academics, researchers, civil society organisations and practitioners (see the list of participants in Annex 1). The group's activity began in April 2025, meeting on five separate occasions and continuing until November 2025.

The report is divided into eleven parts. After the introduction that sets the stage, Parts II to VI present the major issues related to the transition to quantum safe in the European Union (EU), focusing on the technology, market, governance and policy issues. Part VII presents the comments of the Task Force to the Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, put forward in June 2025 by the Network and Information Systems (NIS) Cooperation Group. Parts VIII to X focus on the specific transition in the financial, public and defence sectors. Part XI outlines the recommendations for governments and businesses to strengthen and accelerate the transition to quantum safe in the EU.

As Coordinator of the Task Force, I would like to acknowledge the invaluable contributions of all the participants in this work. Thanks go to the members of the Advisory Board: Sofia Lindskov Hansen at the Danish Ministry of Foreign Affairs, Michele Mosca at Waterloo University, Michael Osborne at the IBM Research Division in Zurich, Bart Preenel at KU Leuven and Tim Watson at the Alan Turing Institute in London.

I also wish to acknowledge the substantial work done by my fellow rapporteurs, Swann Ashworth, Carolina Polito and Afonso Ferreira. I would further like to thank Jaime Gómez García, Matthias Schunter, Kevin Reifsteck, John Mattsson and Laima Jančiūtė for their extensive comments on the draft of the report. This work has been a collective endeavour as other Task Force participants have directly contributed their expertise by commenting on selected sections of the report. Thanks also go to the invited speakers who contributed to the Task Force discussions.

Lorenzo Pupillo
Coordinator and Rapporteur of the Task Force
Associate Senior Research Fellow and Head of the Cybersecurity@CEPS Initiative
CEPS, Brussels
December 2025

EXECUTIVE SUMMARY

In April 2025, CEPS launched a Task Force on Strengthening the EU Transition to a Quantum-Safe World. The objective of this initiative was to draw attention to the technical, market, governance, and policy challenges involved in Europe's transition to quantum safe.

The Task Force, designed as a multi-stakeholder platform, brought together eleven private organisations, eleven EU institutions and agencies, seven universities and think tanks, one national research agency, and one civil society organisation (see Annex I for the full list of participants).

The group aimed to develop practical guidelines for governments and businesses to strengthen and accelerate the EU's transition to quantum safe. Its discussions addressed the technical, managerial, and governance challenges associated with implementing this process. These efforts resulted in a set of policy recommendations aimed at EU institutions, Member States, the private sector, and the research community to guide Europe's secure transition toward quantum resilience.

The transition to post-quantum cryptography (PQC) poses an urgent strategic challenge for Europe. It requires careful coordination and long-term planning across both the public and private sectors. Quantum computers capable of breaking today's cryptographic systems may emerge as early as the next decade. Yet transitioning to PQC is a lengthy and complex process. Past experiences with security-standard migrations suggest such transformations can take 10 to 15 years.

Despite this urgency, recent surveys by the European Union Agency for Cybersecurity (ENISA) and the Information Systems Audit and Control Association (ISACA) show that most European stakeholders remain underprepared. Only a small share has begun investing in post-quantum solutions, and overall awareness remains low. At the Member State level, Germany, France, and the Netherlands have taken leading roles by issuing guidance and launching PQC pilot projects, both through national roadmaps and within the Network and Information Systems (NIS) Cooperation Group. However, progress across the EU remains uneven, and the Union still lacks a coherent, unified transition framework like that of the United States.

Against this backdrop, the Task Force calls for strengthening the EU's transition process towards quantum safety, guided by the following principles:

1) Quantum-safe transition as a systemic transformation

The shift to quantum-safe cryptography should not be viewed as a routine technical upgrade but as a **comprehensive, systems-level transformation**. Transitioning to PQC extends beyond updating cryptographic libraries: it involves integrating new product versions, modifying the application programming interface (API), adapting software development lifecycles, and, in some cases, redesigning core business processes. It also demands proactive management of supplier, customer, and ecosystem relationships. This represents a **major managerial challenge** requiring long-term planning, skilled workforce development, and sustained organisational change.

2) Moving beyond the 'Q-Day' narrative

Public discussions often refer to 'Q-Day', the hypothetical moment when quantum computers render classical cryptography obsolete. While this framing can mobilise attention, it is misleading. **Quantum capability will not arrive as a tsunami but as a gradual, uneven process**, with early machines breaking selected keys before broader capabilities develop. A more realistic perspective is that of a 'Q-period', which supports balanced and adaptive migration strategies aligned with the actual pace of quantum and standards development.

3) Post-quantum cryptography as the core of the transition

PQC forms the backbone of the transition to quantum safety. These algorithms are designed to withstand attacks from quantum computers and are widely recognised by regulators and standardisation bodies **as the only viable short- to medium-term solution.**

Other quantum technologies play more specialised roles:

- **Quantum key distribution (QKD)** is not a direct substitute for public-key cryptography but a complementary technology that can offer diverse layered protection for specific high-security environments.
- **Quantum random number generators (QRNGs)** provide certifiable entropy quality, ensuring that quantum-derived randomness can be embedded into cryptographic stacks and validated under recognised certification schemes.

4) A risk-based transition model

Migrating billions of devices to quantum-safe standards requires a structured, risk-based approach encompassing the following elements:

- **Crypto agility**: design cryptographic systems in a modular way, allowing for the easy replacement of cryptographic components.

- **Awareness of crypto dependencies**: since most organisations rely heavily on third-party vendors, understanding and managing supply chain dependencies is crucial. Organisations must engage suppliers, request clear timelines for quantum-safe capabilities, and monitor supply-chain readiness.

- **Crypto and product inventories**: effective planning starts with a comprehensive inventory of internal and external dependencies, including software, hardware, APIs, and services. Critical systems should be prioritised for early migration.

- **Hybrid solutions**: the coexistence of classical and quantum-resistant algorithms, known as hybrid cryptography, can enable interoperability and redundancy. To ensure global interoperability, hybrid solutions must be standardised through standards' development organisations. The Task Force recommends broadening the definition of hybrid solutions to encompass 'context-aware, technically inclusive approaches' that combine multiple cryptographic mechanisms for resilience, such as PQC/traditional or PQC/QKD.

When it comes to the design and implementation of a European Roadmap for Post-Quantum Cryptography (from now on the Roadmap), beyond specific contributions made to the NIS Cooperation Group Roadmap (available in Part VII of this report), the Task Force highlights the need for the following actions:

- **Integrate quantum safety into digital systems from the outset**: the European Commission and Member States should ensure that digital systems (e.g. the European Digital Identity Wallet) are designed to be quantum-safe from the start.

- **Link the Roadmap to a quantum-transition strategy and existing legislations**: a roadmap defines milestones and timelines, but a supporting strategy must clarify how Member States, vendors, and institutions will meet them.

- **Ensure alignment and coherence across roadmaps**: with multiple quantum-safety roadmaps emerging at EU and national levels, the European Commission, Member States, and standardisation bodies must coordinate efforts to ensure coherence in timelines, dependencies, and objectives. Coordination with the US and other G7 partners is equally important.

- **Introducing greater parallelisation into the Roadmap**: the Roadmap's current structure implicitly relies on a staged or linear approach, which may unintentionally create bottlenecks. This Task Force recommends introducing greater parallelisation into the Roadmap to accelerate progress and reduce systemic risk.

Finally, the report underscores the importance of promoting awareness, cooperation, and effective governance throughout the transition to quantum safety. It calls for capacity building, skills development, and the establishment of dedicated crypto-management units within organisations.

In detail, **this Task Force makes recommendations to policymakers, the private sector and the research community that are summarised as follows**[1].

1. General Recommendations

GR1. Develop crypto agility

In the pursuit of quantum-safe encryption, the transition of encryption methods of billions of devices requires a specific model, needing design from a technical, organisational and policy perspective. For such an endeavour, a risk-based approach is necessary. Such an approach should revolve around **crypto-agility principles** based on measured risks and needs.

GR2. Engage with suppliers to take care of crypto dependencies

Most organisations rely heavily on third-party products and services, and supply chain dependencies frequently define the constraints and possibilities of migration. Migration to PQC often stalls when critical products or dependencies are beyond the direct control of the organisation. Software vendors and suppliers are on staggered upgrade schedules, and many cryptographic components are buried in complex, nested dependencies. To address this, **organisations need robust engagement with suppliers**, clear requests for timelines on quantum-safe capabilities, and a mechanism for tracking supply-chain readiness.

GR3. Building and maintaining crypto and product inventories

In preparation for the shift to post-quantum cryptography, organisations are increasingly focusing on how cryptographic and product inventories are built and maintained. Developing inventories should be prioritised, focusing first on the most relevant use cases. Prioritising such an inventory will help with building a roadmap and provide context on migration activities. An inventory of cryptographic assets is an important task that, based on previous analysis, will facilitate a better understanding of the landscape of what needs to be migrated. What emerges is not a rigid blueprint, but rather a set of guiding practices,

[1] The extended version of the Recommendations is avalable in Part XI.

shaped by early planning, collaboration across technical and governance teams, and a clear understanding of what such inventories need to capture and why.

Cryptographic inventories are a detailed mapping of where and how cryptography is used across an organisation's systems. Its objectives are to identify the cryptographic algorithms in use today (Rivest-Shamir-Adleman Algorithm (RSA), elliptic-curve cryptography (ECC), Advanced Encryption Standard (AES)), their implementation context (code signing; Transport Layer Security (TLS) for communications), their quantum resistance status (legacy or PQC), and the dependencies of cryptographic modules and standards.

Product inventories focus on external products, services, and hardware that an organisation uses (i.e. third-party providers), and map the cryptographic characteristics of these products. When purchasing new software, hardware, or cloud services, organisations would require vendors to disclose the cryptographic algorithms and protocols used in their products, potentially including a roadmap for post-quantum upgrades.

GR4. Integrate quantum-safety into digital systems from the start

The European Commission and Member States should ensure that digital systems (such as the European Digital Identity Wallet) are **designed to be quantum-safe from the start**. In other terms, if new services or systems or standards are introduced that require crypto, then this crypto should be quantum safe from day one. This means integrating post-quantum cryptography into system architecture, certification, and procurement processes rather than treating it as a future retrofit.

GR5. Going beyond hype: from a Q-Day to a Q-period

Discussions of PQC are frequently animated by the spectre of Q-Day, a sudden moment when a powerful quantum computer renders classical cryptography obsolete. While useful as a mobilising narrative, this framing risks distorting the problem. Quantum capability will not arrive as a tsunami but as a gradual, uneven process. A handful of machines will first be able to break selected keys, before scaling to broader applications. Therefore, **a more realistic framing, treating the problem as a Q-period, rather than a Q-Day**, would support balanced migration strategies, paced with the actual evolution of quantum capability and standards readiness.

GR6. Linking the Roadmap for the Transition to Post-Quantum Cryptography[2] to a quantum transition strategy and to existing laws

There are significant risks in pursuing an EU quantum-safe roadmap without a coordinated, risk-aware transition strategy. A roadmap must specify what milestones are required and by when, but only a supporting strategy can define how Member States, vendors, and institutions will meet them. Without synchronised standards, certification schemes, interoperability frameworks, and testing infrastructures, regulation may outpace readiness.

GR7. Ensure alignment and coherence across roadmaps

Multiple roadmaps for quantum-safe transition are currently being developed and discussed at the EU and national levels, covering post-quantum cryptography, quantum communication, and related infrastructure initiatives. While each roadmap sets valuable priorities and indicative milestones (e.g. 2026, 2030, 2035), their coexistence risks producing fragmented or worse incompatible requirements and implementations if not properly aligned. The European Commission, together with Member States and standardisation bodies, should therefore **promote cross-roadmap coordination to ensure coherence in timelines, dependencies, and objectives**.

To ensure global coherence and avoid fragmentation, the EU should also coordinate closely with the US and other G7 economies to align roadmaps, technical requirements, and timelines for quantum-safe transitions.

GR8. Introducing greater parallelisation into the Roadmap

The Roadmap's current structure implicitly relies on a staged or linear approach, which may unintentionally create bottlenecks, particularly where progress in one area depends on completion in another. Given the complexity and heterogeneity of cryptographic systems across the EU, **we recommend introducing greater parallelisation into the Roadmap to accelerate progress and reduce systemic risk**[3].

GR9. Promoting awareness, cooperation and better governance

In cyberspace, all nations are connected across borders and depend on each other, including in this transition. Therefore, Member States **should create an environment or**

[2] Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, from now on the Roadmap.

[3] Specific, actionable suggestions for increasing parallelism while maintaining coordination and alignment are available in Part XI.

community where organisations, entities and stakeholders can share knowledge and experiences.

Member States should lead by example with transparent transition plans: publish and regularly update government transition roadmaps, including timelines, milestones and budgets, to foster knowledge sharing and best practices. Roadmaps should broaden their definition of 'stakeholder' beyond ministries, regulatory agencies and technical experts. Civil society, minority networks and grassroots diversity, equity and inclusion (DEI) organisations should be recognised as co-leaders, not simply 'consulted'.

The Roadmap for the transition to PQC should establish mechanisms (citizen assemblies, consultation panels, regular transparent updates) to ensure citizens not only receive information but can actively shape strategies. The Roadmap should **encourage joint pilot projects at the EU level to test interoperability of PQC in cross-border services before 2030.**

We suggest **establishing a public-private PQC migration observatory under ENISA** to monitor advances and recommend acceleration of timelines if necessary.

GR10. Promoting skill development and management structures

Finally, successful migration also depends on management structures and skill development. Cryptographic migration is no longer just the purview of niche technical experts; it requires cross-functional teams, transparent governance, and clear process ownership. Organisations should have a **well-established, funded, and empowered programme that starts with clear business-level priorities**. Much of the current progress is bottom-up and lacks executive support.

2. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE FINANCIAL SECTOR

FS1. Create an ad hoc PQC governance structure

Governance structures are vital. Firms should establish a PQC transition steering committee or task force. This group oversees inventorising cryptographic usage, tracking standards, and setting migration timelines in alignment with business priorities and regulatory requirements. Many large banks have already formed internal 'quantum risk' or 'crypto agility' teams for this purpose.

FS2. Enhancing collaboration with vendors and partners

The financial sector's crypto infrastructure extends beyond the walls of any single institution. It includes vendors, third-party service providers, and hardware manufacturers. It depends on these actors. A key bottleneck is the **readiness of technology providers** to support PQC. Therefore, firms should engage vendors early to ensure their roadmaps include PQC support, effectively asking for **crypto agility by design in new procurements.** Vendor incentives may be increased and fragmentation reduced if financial institutions can agree on common procurement standards.

FS3. Upgrade the financial sector underlying infrastructure

Companies need to **upgrade their underlying infrastructure** to ensure that hardware security modules (HSMs), cryptographic libraries, virtual private network (VPN) appliances, and other related components can support quantum-safe algorithms. A key recommendation is to modernise algorithms **as part of the ongoing broader IT modernisation initiative**. For example, if a bank is migrating services to the cloud or replacing core banking systems, crypto-agility considerations should be built in from the start.

FS4. Prioritise actions based on risk assessment

Given the scale of the transition, not everything can be changed at once. A risk-based approach is essential to prioritise which systems and data to secure first. This process begins with a **cryptographic inventory**. Instead of aiming for a comprehensive inventory that is costly and may become outdated once actual migrations begin, we recommend a top-down and risk-based approach that creates inventories for migrating specific parts of the business based on a business-level risk-reward analysis. While certain dependencies will need to be maintained, this ensures that the business justification and value can be identified and tracked while migrating.

FS5. Perform cost-benefit analysis of mitigation options

Not all solutions are equal: some may involve hardware changes (using hybrid solutions in hardware or deploying quantum random number generators or QKD links), while others are purely software-based (switching to PQC algorithms). The Task Force mentions that a complete crypto transition for a large bank could cost in the order of hundreds of millions of dollars. The importance of quantified risk assessments for boards and executives is essential to justify expenditures against the risk reduction achieved. **If the cost of inaction (i.e. potential fines, losses, and reputational damage from a future breach) outweighs the migration cost, the business case for PQC investment becomes clear.**

FS6. Overcome organisational and skills gaps

Financial institutions face a **shortage of cryptographic skills and awareness** at all levels. Cryptography has often been a niche domain in IT; now it must become a mainstream concern. The culture in many financial organisations has been to treat cryptography as a static utility. Changing this mindset to one of continuous cryptographic improvement is an organisational challenge.

3. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE PUBLIC SECTOR

PS1. Implement a sequenced migration plan across PKI and digital identity ecosystems

Public administrations should adopt a coordinated, risk-based approach to upgrading public-key infrastructure (PKI) and digital identity systems. Migration should begin with the **most critical and high-impact components**, such as national identity registers, cross-border authentication services, and certificate authorities that anchor public trust, before extending to dependent systems. Administrations should conduct comprehensive cryptographic inventories to map dependencies and identify areas most exposed to quantum risks. This mapping should inform **sequenced migration roadmaps** that combine hybrid cryptography for short-term continuity with long-term adoption of post-quantum standards.

PS2. Synchronise authentication layers to prevent fragmentation and service disruption

Authentication systems, roots, intermediates, browsers, and revocation services must **evolve in lockstep** to preserve trust and interoperability during the quantum transition. The European Commission and national authorities should **coordinate migration to ensure simultaneous readiness across these layers**. This includes benchmarking performance impacts, conducting interoperability and stress tests, and establishing fallback mechanisms to handle larger certificates and increased computational demands. A synchronised approach will prevent fragmented implementations and minimise service outages.

PS3. Coordinate cross-border roadmaps and align national migration strategies

The European Commission and Member States should establish a joint roadmap for quantum-safe migration, aligning national PKI upgrades, timelines, and policy frameworks. This coordination should focus on **interoperability across borders**, ensuring that trust chains, certification processes, and governance models remain consistent within the EU. Regular reporting and **shared readiness benchmarks** should be institutionalised to ensure that national infrastructures evolve in sync and maintain mutual trust.

PS4. Manage the quantum transition as a coordinated sociotechnical programme

Post-quantum migration in the public sector should be approached as a **whole-of-ecosystem effort**, not a purely cryptographic upgrade. The European Commission and Member States should establish coordination mechanisms bringing together technical agencies, regulators, standardisation bodies, and industry actors to guide the transition. Migration plans must also **account for legacy and operational-technology constraints** by scheduling upgrades and enabling parallel standards updates to prevent bottlenecks.

4. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE DEFENCE SECTOR

DS1. Develop a post-quantum transition roadmap

Defence industry stakeholders should establish a post-quantum transition roadmap that synchronises governmental policy milestones with industrial deployment. This roadmap should mandate comprehensive cryptographic inventories, prioritise mission-critical and high-risk systems, and coordinate cross-vendor testing of PQC implementations. Developing shared migration benchmarks will enhance interoperability across defence supply chains, prevent redundant efforts, and enable the modernisation of legacy command, control, and communication infrastructures without disrupting critical operations.

DS2. Support industrial coordination

Institutional stakeholders should support **industrial coordination** between defence primes, SMEs of the quantum industry, and research labs through funding mechanisms that prioritise European value chains and reduce reliance on non-EU suppliers.

DS3. Address supply-chain dependencies

Similarly, competent European institutions (e.g. the European Defence Agency (EDA), the European Commission and the European Defence Fund (EDF)) should address **supply chain dependencies**: several key quantum algorithms and hardware components currently originate in the US or Asia. European actors should prioritise developing proprietary quantum algorithms, photonics platforms, and cryogenic technologies in Europe.

DS4. Formalise public-private quantum innovation frameworks

International and European defence institutions (EDA, NATO, EDF) should formalise **public-private quantum innovation frameworks** connecting established defence contractors with start-ups and academic labs. These partnerships should include shared testbeds, classified-and-open research and development (R&D) tracks, and co-funded demonstrators to accelerate technology transfer. Priority should go to **dual-use quantum sensing and communication systems**, ensuring civil R&D (from Quantum Flagship or national programmes) is adapted to defence applications.

DS5. Establish structured pilot-to-certification pathways

To validate emerging quantum systems for operational use, the **EU and NATO** should establish **structured pilot-to-certification pathways**. Programmes such as OPENQKD should evolve into permanent **Quantum defence testbeds,** allowing companies (e.g. Thales, Leonardo, SMEs) to test prototypes under military conditions. Results should directly feed into European standardisation bodies (the European Telecommunications Standards Institute (ETSI), ENISA) to define **security and interoperability benchmarks**, thereby reducing time-to-deployment and ensuring trusted European solutions.

DS6. Incentivise research in defence quantum technologies

To incentivise **research in defence quantum technologies**, it is essential to establish secure **knowledge-sharing mechanisms** (e.g. classified research consortia, modular publications, or declassification windows) allowing academics to maintain academic career progression without breaching defence restrictions.

PART I. INTRODUCTION

The transition to quantum-safe cryptography poses a critical and urgent challenge for Europe, necessitating careful coordination and long-term planning across both the public and private sectors. While quantum computers with the potential to undermine current cryptographic standards may become available as early as the next decade, transitioning to post-quantum cryptography is far from immediate. Previous experiences with security standard migrations show that such transformations can take 10 to 15 years (e.g. the Transport Layer Security (TLS) migration[4]).

Despite this urgency, recent surveys, including the European Union Agency for Cybersecurity (ENISA)'s[5] assessment of over 1 350 organisations across 27 EU Member States, reveal that most European stakeholders remain largely unprepared: only a small fraction have started investing in post-quantum solutions, and overall awareness is low. This is not only a matter of slow uptake, as substantial portions of operators in critical sectors do not even plan to invest in quantum-safe measures at all. This acknowledgement is supported by private sector data as well (only 4% define a quantum computing strategy, including transition to quantum safe)[6]. In Europe, Germany, France, and the Netherlands have taken a leading role in issuing guidance and running post-quantum cryptography (PQC) pilot projects, both through their national roadmaps and within the Network and Information Systems (NIS) Cooperation Group. However, across the wider EU, the uptake of these roadmaps remains uneven, and the Union as a whole still lacks a coherent, unified quantum-transition framework comparable to that seen in the US.

Against this backdrop, the Centre for European Policy Studies (CEPS) Task Force on Strengthening the EU Transition to a Quantum Safe World provided a platform for dialogue among private sector representatives, European institutions, academia, and civil society. The aim is to seek consensus on technological pathways, governance mechanisms, and policy recommendations that will guide Europe's secure shift toward quantum resilience.

[4] Brat Preneel presentation 2024, https://handouts.secappdev.org/handouts/2024/bartpreneel_the-quantum-threat-and-post-quantum-cryptography-pqc.pdf.

[5] ENISA 2024 assessment, 'Only 4% of organisations have invested in Post-Quantum Cryptography', https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf.

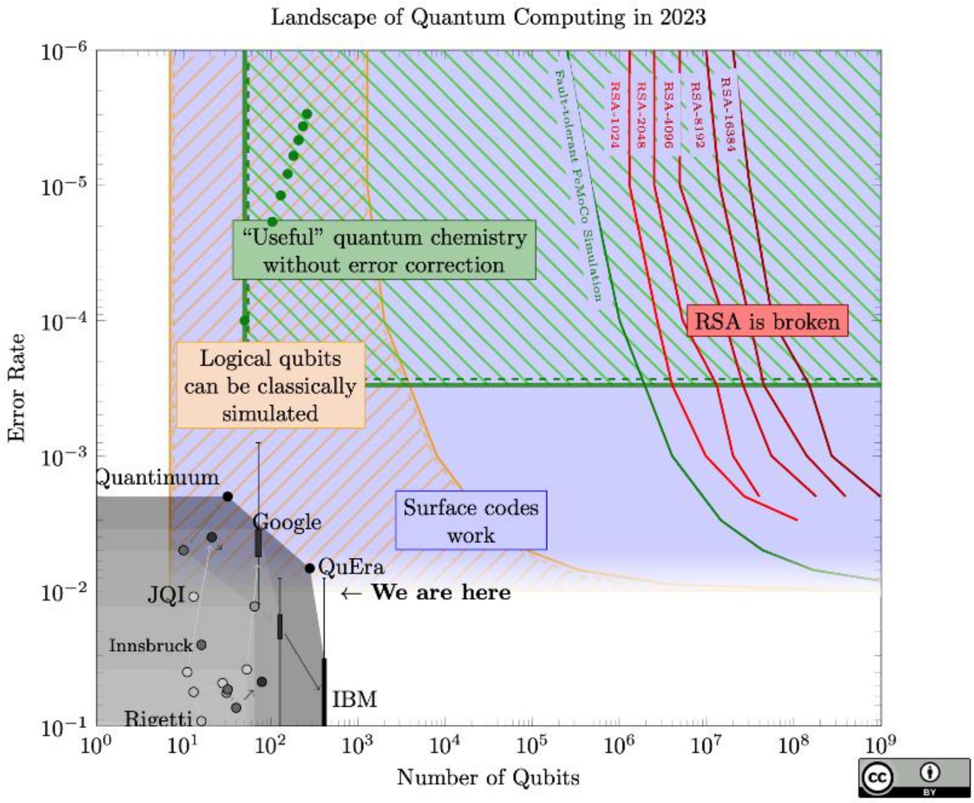
[6] ISACA study on 2 685 company members (geographics not included in dataset, some companies may not be part of the EU), https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-to-cybersecurity-and-business-stability.

While a fully functional cryptographically relevant quantum computer (CRQC) capable of breaking modern cryptography may still be years or even decades away, the magnitude of the risk and the scale of the required transition make immediate and sustained preparation essential[7]. Quantum research, particularly Craig Gidney's recent work, has steadily reduced the estimated number of **physical qubits required to break RSA-2048**, from ~20 million in 2019 to under **1 million today**, thanks to advances in error correction and algorithmic techniques. As error rates drop and codes become more efficient, this compression trend accelerates, meaning fewer qubits deliver comparable power, and risk evolves faster than hardware scales. Assuming continued improvements, each year of refinement cuts the required qubit count substantially, bringing the prospect of cryptographic attacks closer even before physical qubit milestones are reached. Samuel Jacques' CRQC timeline[8] illustrates the current state of quantum computers (small, noisy devices), their desired future direction (error-corrected, large systems), and the distance we have yet to travel to achieve cryptographically relevant quantum computers capable of breaking the Rivest-Shamir-Adleman (RSA) Algorithm (Figure 1). His timeline demonstrates a similar perspective on the amelioration of quantum computing components, bringing us closer to CRQC.

[7] 'Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography', A joint statement from partners from 18 EU Member States (2024), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5.

[8] This timeline has been used and referenced in a report by ICANN and Pr. Douglas Stebila, as well as Pr. Bart Preneel. Unofficial but updated annually, this timeline is realised by Samuel Jacques, professor at the University of Waterloo. The forecast made in 2023 is more generous than the 2025 update, due to increased error-corrected qubits (source).

Figure 1. Unofficial CRQC timeline (Samuel Jacques)



Source: Task Force resource, Samuel Jacques.

Today, major corporations, start ups, and research programmes are pursuing a diverse range of scientific approaches to develop a utility-scale quantum computer. The massive investments flowing into quantum research and development (R&D) reflect the geopolitical and economic stakes of this technological shift. National strategies are also drawn to quantum technologies as a whole, from quantum computing to sensing and communications. Several Member States, including Spain, Italy and Denmark, have recently published dedicated national quantum strategies, outlining investment priorities and mechanisms for research uptake. At the EU level, the European Quantum Technology Strategy was released in July 2025. Similarly, in the US and China[9], investments of USD 3.7 billion and up to USD 14 billion respectively signal a deep commitment to leadership in this domain. Altogether, these developments underscore how quantum technologies are emerging as central to the next-generation digital transformation.

The report will examine the distinct roles and capabilities of PQC, quantum key distribution (QKD), and quantum random number generator (QRNG) and is structured as

[9] The 14th National Economic and Social Development and Vision 2035 includes strong investments in quantum computing, but also quantum sensing (e.g. in PNT) and communications (QKD mainly for inter-city networks) (source).

follows. As an introduction, each of the approaches addresses the quantum threat from a different angle, potentially forming layers of protection: PQC through mathematical algorithms resistant to quantum attacks, QKD through physics-based key exchange, and QRNG, which ensures randomness and unpredictability in cryptographic keys.

Building on this foundation, we will propose and assess the most viable transition models that allow for phased, resilient adoption of quantum-safe solutions. These include hybrid cryptographic architectures and crypto-agility strategies, essential concepts for a migration to quantum safe. Furthermore, the report will also showcase how organisations can begin building post-quantum inventories as a prerequisite for effective risk mitigation and governance.

These models will then be evaluated in consideration of ongoing national and international efforts. The report will present an analysis of quantum preparedness across key countries, both within the European Union and internationally (i.e. the US and China), focusing on their strategy and vision. This sets the stage for the sector-specific chapters, where we will examine the particular challenges and opportunities in three strategic domains: **the financial, public, and defence sectors.**

By integrating these elements, the report aims to deliver a coherent roadmap for quantum resilience that is both technically grounded and policy-relevant. The final chapter will provide actionable recommendations based on this analysis, supporting public and private decision-makers in orchestrating a secure, scalable, and timely transition to quantum-safe cryptography.

PART II. STATUS OF PQC, QKD, AND QRNG IN A QUANTUM-SAFE CONTEXT

1. POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography is the primary method for organisations to transition to quantum safety. It consists of cryptographic algorithms that can (in theory) resist future attacks on quantum computers and classical computers. In the transition to quantum safe, PQC is regarded by regulatory bodies as the only viable option in the short to medium term[10].

From a technical perspective, post-quantum cryptography refers to new asymmetric (public-key) algorithms designed to resist quantum attacks. These can be categorised into two primary forms: Key Encapsulation Mechanisms (KEMs) and digital signature algorithms. The former is an algorithm used to establish shared secret keys, similar to the Diffie-Hellman key exchange or RSA encryption in current systems. PQC KEM can be used to protect session keys. CRYSTALS-Kyber is an example of this, having been selected by the US National Institute of Standards and Technology (NIST) as a reliable PQC algorithm. Digital signature algorithms are used for authentication and integrity, analogous to RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) signatures today.

Over the past decade, the international community converged on a first generation of standards of PQC algorithms. For instance, the US is the most prominent in standardisation for global adoption. NIST finalised three algorithms for encryption and digital signatures. In 2024, NIST finalised three standards (Kyber, Dilithium, and SPHINCS+), while Falcon and other candidates are expected to follow later. However, global fragmentation remains possible, with parallel initiatives in countries such as China and Korea, where competing standards could reduce interoperability.

The precise technical structure of PQC is an ongoing project undertaken through the development of standards by national or independent bodies. The debate now also revolves around determining the deployment of such technology across thousands of products, certificates, and infrastructures. This transition must be understood not only as an upgrade of hardware and algorithms but as a long-term governance challenge that will shape the resilience, sovereignty, and security of the digital ecosystem for years to come.

[10] US National Institute of Standards and Technology, https://csrc.nist.gov/projects/post-quantum-cryptography.

2. QUANTUM KEY DISTRIBUTION

QKD shares secret keys between two parties by exchanging signals, mainly photons but also electrons and ions, that leverage quantum effects. It is a key agreement technique, not an encryption algorithm. Using a physical link, QKD can produce shared random key material that both parties know, and guarantees that any eavesdropper trying to intercept the quantum signals will cause detectable disturbances that both parties will become aware of before the QKD protocol completes. The jointly established key material – known to both parties but nobody else – can then be used for other cryptographic schemes, such as message encryption or authentication.

Unlike key agreement based on PQC, which relies on the assumed computational hardness of mathematical problems (e.g. lattice-based schemes), QKD derives its security from the laws of quantum mechanics. Therefore, even a CRQC cannot break QKD, as the protocol does not depend on algorithmic complexity but on the physical behaviour of quantum systems[11]. Additionally, QKD systems usually enable short-lived random keys for each session, which are continuously updated over time. The absence of a longer-lived key (that may be leaked or stolen) increases the security of such systems.

2.1. QKD - LIMITATIONS AND IMPLEMENTATION MODELS

QKD links such as fibre optic cables exhibit finite losses that typically increase with distance, so photons are transmitted most efficiently over short distances. Despite its theoretical advantages, QKD currently faces practical limitations in medium- to long-range communication links, with current networks often relying on trusted nodes where losses would otherwise give rise to slow or no key generation, and complex integration into existing networks. Losses in the vacuum of space can be lower, enabling satellite QKD links to be longer, once signals have passed through the atmosphere.

The current advancements in QKD, which are at an intermediate technology readiness level (TRL) do not yet function in long-distance applications (> few 100 km) without trusted nodes. The no-cloning theorem can be part of the security of QKD, but it also means that amplifiers cannot be used as in classical networks (commercial quantum repeaters are still in development). Furthermore, a QKD channel typically generates keys at a specific rate, measured in bits per second (up to ~Mbit/s but reducing with distance). This rate can be a limiting factor when it comes to encrypting large amounts of data simultaneously, but rates are often higher than those easily generated by key agreement techniques based on computational complexity.

[11] For more information on the appliance of laws of quantum mechanics to QKD: Scarani et al., 2009.

To achieve the highest distances and rates, QKD is sometimes deployed over dark fibre rather than multiplexing with other data. This can necessitate additional infrastructure beyond what is necessary for a similar classical network. There could be significant costs and complexity involved in installing and maintaining QKD devices. However, many QKD devices are composed mainly of regular communications components, and well-designed QKD devices should be able to offer comparable reliability and operate in standard data centre environments. Calibration of individual photon-based transmission can be important for the security of some designs of QKD devices. Such considerations point to the current use of QKD in scenarios where the added security justifies the expense and effort (e.g. in government communications and inter-bank connections).

Apart from technical limitations, the strategic approach towards QKD is fragmented both within policy and financially in terms of investments by the private sector. As the maturity of some of the technology remains limited, this raises questions about investments from both the public and private sectors in the development of QKD, given the value it delivers compared to research costs.

In the context of these shortcomings, the opportunity cost of overemphasising QKD could be significant. The allocation of resources towards mature software-based PQC algorithms may yield more immediate and scalable security outcomes. This concern is pronounced in the EU, with launched initiatives such as the European Quantum Communication Infrastructure (EuroQCI), which seeks to connect European hubs with quantum communication systems. It is also essential to continually evaluate QKD capabilities and their role in the broader architecture, particularly in a layered, hybrid system that combines QKD, PQC, and classical cryptographic mechanisms.

In summary, QKD is not a drop-in replacement for public key cryptography in general networks. It is best thought of as a specialised service in particular environments that may increase security for selected scenarios. A bank might use QKD between its two primary data centres to secure its replication traffic, but it will not use QKD to ensure every customer's connection to online banking, where PQC would be a better choice. However, competition and innovation could improve technology and boost adoption. Significant areas of development include increasing the key rate, extending the distance, and miniaturising the equipment.

QKD standardisation and certification are in progress and will be key to its future implementation. They will determine how QKD can complement classical encryption and be used in hybrid communication networks. These standards would enable applications to utilise keys from a QKD device in a uniform manner, regardless of the QKD device's internal details. The network integration of QKD is another issue in building quantum networks[11]. The efforts of standard bodies, such as the European Telecommunications

Standards Institute (ETSI) and the International Organization for Standardization (ISO) (specifically the ISO/IEC JTC 1 SC 27), enable the broader adoption of this technology through the principles of harmonisation and interoperability.

3. Quantum random number generators and classical random number generators

At the foundation of secure encryption lies the generation of random numbers, values that must be truly unpredictable to withstand adversarial attacks. QRNGs represent a state-of-the-art approach to this challenge, harnessing the inherent indeterminacy of quantum phenomena such as photon behaviour and quantum phase fluctuations to produce high-entropy outputs. Unlike classical random number generators, which rely on deterministic algorithms or noisy physical processes, QRNGs offer randomness that is guaranteed by the laws of quantum physics. This positions QRNGs as a promising source of high-quality entropy for cryptographic systems. However, while QRNGs enhance the unpredictability of cryptographic inputs, they do not address the broader vulnerabilities posed by quantum computing. Even perfectly random keys can be compromised if used within cryptographic algorithms that are susceptible to quantum attacks. Therefore, QRNGs must be integrated with post-quantum cryptographic protocols to achieve true quantum resilience.

Sufficient randomness of selected inputs is vital in encryption mechanisms (see Table 1). It is essential to ensure that the generated numbers are truly random so that they cannot be predicted. In cryptography, entropy is a main concept for generating random numbers. Entropy refers to the amount of unpredictability in a system, measuring the difficulty of guessing or reproducing a value. The higher the entropy, the harder it is for an attacker to predict.

Table 1. Level of randomness

Level of randomness	Description (simplified)
1. Illusion of randomness	Patterns look random but aren't; they can be reverse-engineered with enough analysis (e.g. a subsequence of the number PI)
2. Opportunistic randomness	Relies on unpredictable but uncontrolled processes (e.g. user input timing, mouse movement)
3. Engineered chaos	Uses complex physical systems (e.g. thermal noise, radio interference) to produce randomness with unclear guarantees
4. Quantified uncertainty	Based on quantum mechanics or other physical effects; randomness is guaranteed by the laws of physics and can be quantified

Source: Deloitte study.

Most systems today use **pseudo-random number generators (PRNGs)** and **true random number generators (TRNGs)**:

- **Classical TRNGs** rely on complex classical physical phenomena such as oscillator jitter or atmospheric noise. While not algorithmic, they still rest on assumptions of unpredictability in classical systems. Over time, subtle biases or correlations may emerge and be potentially exploitable. QRNGs are TRNGs that leverage quantum phenomena, such as single-photon detection, quantum phase fluctuation, or entanglement, to generate randomness. Since quantum processes can be fundamentally unpredictable, QRNGs can offer randomness without assuming any classical complexity or noise, unlike classical TRNGs. If they meet the quality required by relevant standards, such as NIST SP 800-90A/B/c, QRNGs can offer the highest tier of randomness: quantified uncertainty.

- **PRNGs** are algorithmic and deterministic. They usually use a (truly) random 'seed' and a cryptographic PRNG algorithm to generate long sequences of seemingly random bits. **Cryptographic PRNGs** (such as NIST DRBG or Fortuna) guarantee unpredictability of the generated numbers. However, their safety depends entirely on the secrecy and quality of the seed (i.e. its entropy) and the cryptographic security of the PRNG algorithm. In practice, a hybrid approach is often used where a few true random numbers are used to generate a higher-speed stream of PRNG randomness.

The strong argument in favour of QRNGs is that, if the laws of physics hold and their effects are correctly captured in the random numbers, no hidden variable or predictive model can accurately forecast the output. Here, the system's predictability is safeguarded by physical laws.

Standards for entropy sources (such as NIST SP 800-90B and BSI AIS 31[6]) are beginning to consider quantum-derived randomness, which could facilitate the wider certification and adoption of QRNGs in the future. While we await more specialised standards, existing QRNGs may still be certifiable under existing entropy standards, which enables their deployment in regulated systems.

The overview of PQC, QRNG, and QKD underscores that there is no single or uniform pathway to achieving quantum-safe security, and that the relative maturity and applicability of each approach vary considerably. Each approach advances different aspects of the transition and faces its own trade-offs between security, interoperability, performance, cost, and operational manageability. PQC must balance algorithmic robustness and efficiency with integration into existing infrastructures and global interoperability. QKD deployments weigh key-generation rates, distance, and physical infrastructure requirements against cost and scalability. QRNG systems focus on certifiable entropy quality, while ensuring that quantum-derived randomness can be efficiently embedded in existing cryptographic stacks and validated under recognised certification schemes.

These criteria are often interdependent and sometimes conflicting. For instance, optimising for performance or ease of integration may reduce algorithmic diversity or introduce dependencies on specific hardware or network conditions. Such tensions reveal that success in quantum-safe implementation cannot be measured by a single metric but rather by how effectively systems manage these trade-offs through layered design, interoperability, and certification. An appropriately high level of security is a non-negotiable baseline. Improvements in usability, cost, or performance cannot come at the expense of cryptographic soundness or trust in key material. Achieving resilience, therefore, requires layered safeguards, such as hybrid deployments and fallback mechanisms.

PART III. Quantum-Safe Transition Model

In the pursuit of quantum-safe encryption, the transition of encryption methods of billions of devices requires a specific transition model, needing design from a technical, organisational and policy perspective. For such a large and complex endeavour, we believe that a risk-based approach is best suited for organising the individual sub-projects and sub-tasks of the transition. Such an approach should be pursued top-down: migrating the highest priority business applications and processes while deep-diving into the required technical migrations. This should aim to implement crypto-agility principles based on measured risks and needs.

1. Risk-based approach

The shift to quantum-safe cryptography is increasingly understood not as a routine technical upgrade but as a **comprehensive, systems-level transformation**. Transitioning to PQC extends far beyond updating cryptographic libraries; it typically requires integrating new product versions, modifying application programming interfaces (APIs), adapting software development lifecycles, and, in some cases, redesigning core business processes. It also includes conscious management and transition of supplier, customer, and other ecosystem relations. This process demands long-term planning, specialised workforce recruitment, and sustained organisational change over several years.

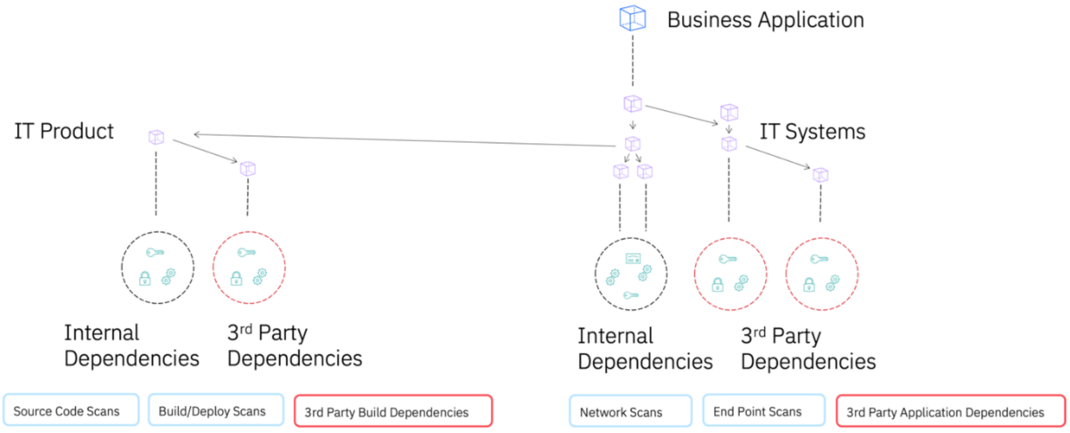
In Europe, the regulatory landscape acknowledges the need for quantum-safe cryptography but lacks a defined transition framework. Regulations such as the Cyber Resilience Act and the Network and Information Security Directive 2 (NIS2 Directive) mandate the use of state-of-the-art cryptographic measures by December 2027, particularly for critical infrastructure. However, neither provides concrete guidance or phased implementation plans for enterprises, leaving organisations without a clear roadmap to manage the complexity and scale of PQC migration.

Transition strategies must be tailored to the specific sector and system. Overly generic guidance risks causing confusion, misalignment, and unnecessary burden, particularly when regulatory obligations are not synchronised with the actual pace of technological or market readiness.

To counter this, there are specific technical and organisational elements to keep in mind. A key empirical lesson is the primacy of dependency mapping over traditional cryptographic inventories. Cryptographic inventories, although necessary for risk monitoring, are rarely complete or actionable for migration planning purposes. They tend to suffer from false positives (crypto code present but unused) and false negatives (crypto embedded in closed, third-party dependencies). In other words, an exhaustive cryptographic inventory may never be complete. The more actionable approach is to map system and software dependencies, particularly in hybrid, cloud-based, or highly interconnected environments.

Besides, most organisations rely heavily on third-party products and services, and supply chain dependencies frequently define the constraints and possibilities of migration. Migration to PQC often stalls when critical products or dependencies are beyond the direct control of the organisation. Software vendors and suppliers are on staggered upgrade schedules, and many cryptographic components are buried in complex, nested dependencies. To address this, organisations need robust engagement with suppliers, clear requests for timelines on quantum-safe capabilities, and a mechanism for tracking supply chain readiness. In this context, actionable planning begins with an inventory of internal and external dependencies, software, hardware, APIs, and services (Figure 2) so that organisations can engage suppliers, demand timelines for upgrades, and plan accordingly. This mapping is not only a technical prerequisite but also enables alignment with supply chain risk management tools that are integrated into EU regulations (e.g. Software Bill of Materials (SBOM) requirements)[12]. If supply chain partners report cryptographic details in standardised formats, it will allow for more reliable automation, compliance, and policy-making (a detailed mapping of post-quantum inventories will be developed in Part IV).

Figure 2. Crypto-dependency mapping



Source: Task Force resource, IBM.

[12] See on this the Cyber Resilience Act – Annex I Section 2 (Vulnerability Handling Requirements).

Furthermore, quantum-safe migration cannot be realistically accomplished in a single leap, because of both the phased availability of cryptographic primitives and the real-world constraints of legacy systems, regulatory cycles, and supply chain dependencies. The release and maturity of post-quantum cryptographic tools occur incrementally. KEMs are generally the first to be standardised and incorporated into products, followed by digital signatures and, eventually, full integration into more advanced protocols such as those underpinning digital identity frameworks or multi-factor authentication.

To mitigate harvest now, decrypt later risks, post-quantum KEMs should be prioritised in any risk-based quantum migration strategy. HNDL targets encrypted data with long-term sensitivity, exploiting the vulnerability of classical public key encryption to future quantum attacks. PQC KEMs offer quantum-resistant alternatives for securing data in transit and are essential for protecting communications today against decryption tomorrow. In contrast, authentication poses a lower near-term risk, as credentials are typically short-lived and easier to rotate. While both encryption and authentication must eventually transition to quantum-safe algorithms, KEMs demand immediate attention to safeguard high-value data from future compromise.

For organisations managing complex infrastructures, this staggered rollout creates immediate strategic dilemmas: migrating piecemeal as new functionalities become available may result in repeated cycles of costly upgrades, operational disruptions, and coordination overhead. However, delaying until a ‘one-shot’ migration is feasible, when the entire stack is ready and certified, risks leaving critical systems exposed for years, possibly introducing systemic dangers, as simultaneous upgrades across a large ecosystem increase the likelihood of failure, incompatibility, or missed dependencies. In this context, organisations must make informed trade-offs and adopt hybrid schemes to bridge the transition period, mapping out which business-critical applications can migrate early versus those that must wait, and building flexibility into procurement and upgrade plans to accommodate phased rollouts.

The empirical evidence from migration projects shows that poor coordination, such as treating migration as a purely technical ‘crypto update’, leads to delays, wasted resources, and sometimes stalled projects when critical dependencies are not ready (i.e. TLS migration). Instead, successful strategies are those that take a systems perspective, synchronise quantum-safe migration with regular digital transformation and IT lifecycle activities. Indeed, migration is often delayed not by lack of technical solutions but by budget cycles, operational inertia, and business priorities. Aligning quantum-safe migration with scheduled upgrades, business transformation initiatives, or regular renewal cycles yields the highest efficiency and buy-in. For most application owners, quantum-safe migration alone is a hard sell unless it is integrated with broader value, such as enhanced cybersecurity, regulatory compliance, or improved lifecycle management.

Finally, successful migration also depends on management structures and skill development. Cryptographic migration is no longer just the purview of niche technical experts; it requires cross-functional teams, transparent governance, and clear process ownership. Many organisations struggle because no single team is accountable for overseeing the transition, and the necessary skills are in short supply. Investment in education, internal centres of competence, and cross-team coordination is essential to reduce friction. A lack of immediate incentives and executive-level attention perpetuates the hesitancy to address this challenge. Organisations should have a well-established, funded, and empowered programme. Much of the current progress is bottom-up and lacks executive support.

The primary challenge in advancing cryptographic resilience isn't the lack of funding, but rather the misalignment of resources. Individuals and teams who prioritise cryptographic security often lack control over the necessary budgets, while substantial funds exist within other business areas that may not prioritise this issue. This disconnect is exacerbated by the absence of a centralised authority or programme owner dedicated to overseeing cryptographic resilience, leading to fragmented efforts and insufficient progress in securing systems against emerging threats.

2. Worst-case PQC failure scenarios: what if PQC turns out to be weak?

This section outlines two possible disruption pathways in the transition to quantum-safe, illustrating the operational necessity of crypto agility and hybrid encryptions to maintain security. It emphasises that proactive design choices (i.e. modular cryptographic architectures and fallback mechanisms) are vital for long-term resilience.

Gradual break: New mathematical insights or cryptanalysis might slowly break one PQC algorithm with classical computers. In this scenario, a proactive hybrid approach would enable encryption mechanisms to remain effective because of the layered security provided by the hybrid scheme. Suppose Kyber (a PQC algorithm) is found to be weak in five years. In that case, organisations with encryption running on Kyber would still be secured for the time being, because only one of the two hybrid encryption schemes has been broken. Furthermore, the principles of crypto agility are crucial in this context. Once a main algorithm has been broken, enterprises should be able to transition to an alternative (such as another KEM from NIST finalists) without significant difficulty. For best practice, systems with modular crypto algorithms (plug-and-play) are recommended.

Sudden break: In this scenario, a CRQC has already been developed, and malicious actors can decrypt communications protected by quantum-vulnerable algorithms, undetected. In this case, once the information is made public (if it ever is), it would be necessary to have a fallback plan. One option would be to maintain the capability to revert to full symmetric encryption in the event of an emergency. Using approaches such as trusted courier key delivery might be the smart move for increased resilience. Therefore, a fallback (sequential) hybrid system will allow for switching to an alternative method if one fails quickly. In contrast to the dual-layer hybrid, this method doesn't imply the combination of two encryption methods, but instead being agile and having backups. While Advanced Encryption Standard (AES)-256 remains secure against quantum attacks because of its large key size, it cannot function independently without a secure KEM. Post-quantum cryptography is therefore required to replace vulnerable asymmetric schemes (such as RSA or elliptic-curve cryptography (ECC)) that enable key distribution and authentication. In a sudden-break scenario, if these PQC algorithms were compromised, a fallback to pre-shared or physically delivered AES-based symmetric keys would ensure continuity of secure communications. For instance, a virtual private network (VPN) appliance might primarily use a PQC-based key exchange but have a mode to fall back to a pre-shared key or an alternate algorithm if a vulnerability is announced. Preparations such as distributing backup keys or establishing a secondary secure channel should be in place.

Both scenarios rely on crypto agility and a form of hybrid scheme, which is essential for future cryptographic design. Governments and industry should advocate for crypto-agile standards and procurement practices. Systems should avoid hard-coding a single algorithm because of possible scenarios; instead, they should build systems in a way that accommodates algorithm updates. This agility not only helps in the quantum context but also in responding to any unforeseen weaknesses (quantum or classical).

Box 1. Cryptographic agility and hybrid encryption

As defined by the NIS Cooperation Group's Roadmap for the Transition to Post-Quantum Cryptography, cryptographic agility is 'the design of cryptographic protocols and systems in a modular way that enables replacing the cryptographic components'.

Achieving agility might involve abstracting cryptographic operations in applications (so that the algorithm can be changed via configuration rather than code changes) and implementing support for multiple algorithms in libraries and hardware. It's as much a software engineering challenge as a cryptographic one.

Recent work by NIST (2025) further elaborates on these principles, framing crypto agility as a capability spanning protocols, software, hardware, and infrastructures, and emphasising the need for sector-specific strategies and common APIs to support scalable implementation. This reflects an emerging consensus that agility must be treated as an organisational and infrastructural property rather than a feature of individual algorithms.

Hybrid encryption, by contrast, involves the simultaneous use of classical (quantum-vulnerable) and PQC algorithms within the same cryptographic workflow. It is a transitional strategy widely endorsed by national cybersecurity authorities (Germany, France, Netherlands) to mitigate the risks of early PQC algorithm failure while maintaining operational continuity. The core benefit of hybrid schemes is redundancy: if one algorithm is compromised, the other can still provide security assurances. However, this approach also increases **computational complexity**, expands the **attack surface**, and raises implementation and compliance burdens, particularly for resource-constrained environments. Combinations of encryption methods can also be between symmetric and asymmetric encryption methods, post-quantum cryptography, quantum key distribution and classical encryption methods (see part 3 below on mixed encryption methods), but aren't necessarily considered hybrid encryption, as the original term implies.

The two concepts are closely related but operationally distinct. **Agility** is about maintaining the ability to switch between algorithms over time, ensuring long-term adaptability. H**ybrid encryp**tion involves running two or more algorithms in parallel to safeguard against immediate or unforeseen weaknesses. In this sense, hybrid deployment can be viewed as a transitional instrument for achieving agility, but true agility requires embedding modularity into the design of cryptographic ecosystems themselves.

A related concern is the security of composite proofs: proving that the combination of two schemes is secure if at least one of the schemes is secure. Researchers[13] are working on formal models for hybrid key exchange security (some initial proofs exist that if each component is indistinguishability under chosen plaintext attack (IND-CPA)[14]-secure, the combination is IND-CPA and so on, with some caveats around how to mix outputs properly). This work may then be translated in standards after thorough review, as with the ETSI TS 103 744 standard on quantum-safe hybrid key establishment (detailed below).

[13] Petcher and Campagna, 'Security of Hybrid Key Establishment using Concatenation', (source).

[14] IND-CPA (indistinguishability under chosen plaintext attack) means that even if an attacker can choose two messages and see the encryption of one of them, they won't be able to tell which one was encrypted.

3. MIXED ENCRYPTION METHODS

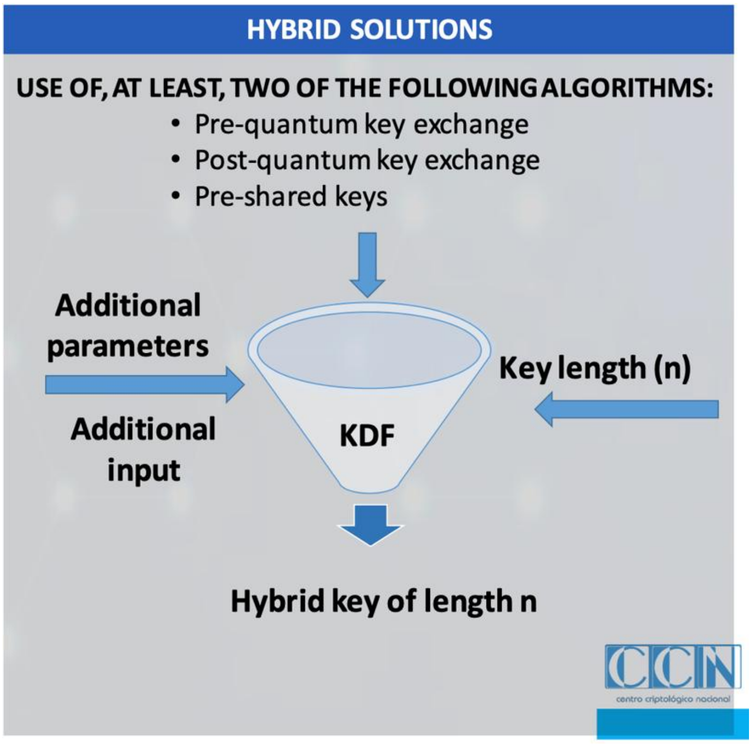
There are two types of hybrid approaches to quantum cryptography.

1) **Classical and post-quantum hybrid.** As mentioned in Box 1, classical and post-quantum hybrid schemes are recommended by many governmental and standards bodies as a short- to medium-term option for secure encryption. It means performing a cryptographic operation in parallel with both a traditional algorithm and a post-quantum algorithm and somehow combining the results. For key establishment, 'hybrid' often implies doing two key exchanges, such as an Elliptic-Curve Diffie-Hellman (ECDH) and a Kyber encapsulation, and then deriving the actual session key from both outputs. A straightforward method is to concatenate the shared secrets: secret = key derivation function (KDF) (Z_classical || Z_postquantum) (possibly including other contextual information). The ETSI TS 103 744 standard employs this approach: it concatenates the Diffie-Hellman shared point with the PQC KEM shared secret (for example, from Kyber) and an optional pre-shared secret, then inputs this concatenated input into a key derivation function to produce the final keys. The result is that an attacker would need to break both the classical and the post-quantum problem to recover the key. Even if one component is later found to be weak, the hope is that the other maintains the security. A classical+PQC hybrid also facilitates a smoother upgrade: for instance, two systems can negotiate a hybrid handshake; quantum-ready clients use both, thereby maintaining compatibility. This approach is sometimes referred to as the Post-Quantum Traditional Hybrid Schemes (PQ/T Hybrid) in the Internet Engineering Task Force (IETF). The IETF is 'driving hybrid Post Quantum/Traditional (PQ/T) schemes for both key exchange & signatures' in multiple working groups. For example, in TLS 1.3, an active standard specifies how to send two key share extensions (one for an ECDH and one for a Kyber exchange) and combine them; similarly, the Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) Protocol already defines a mechanism to perform a dual Diffie-Hellman + Kyber exchange and derive a key from both. Hybrid digital signatures are also considered (i.e. one could sign a message with both ECDSA and Dilithium, requiring both signatures to be valid). Composite certificates (containing two public keys and two signatures) are one way to implement that. The **main shortcoming of hybrid schemes** is increased computational load and larger message sizes (essentially double that of one scheme). In many cases, this is acceptable. For instance, an additional 1-2 kilobytes in a TLS handshake is not a burden, and performing an ECDH plus a Kyber KEM is easily within the capabilities of modern central processing units (CPUs).

Thus, hybrid classical+PQC is viewed as a **low-risk intermediate step to accelerate the adoption of PQC.**

2) **QKD and PQC or a multi-layer hybrid.** Another type of hybrid involves using fundamentally different mechanisms in different layers, notably by combining QKD with cryptography, either traditional or post-quantum. One proposal is to use QKD to secure lower-layer links (say between network routers or data centres), while still employing end-to-end post-quantum encryption between the endpoints. This could be viewed as a layered hybrid (Figure 3): the link is protected by quantum keys (so an attacker cannot passively eavesdrop on the fibre without detection), and simultaneously, even if one link were compromised, the data is encrypted with a PQC algorithm that is end-to-end from sender to receiver. Such arrangements can drastically reduce the risk of any single point of failure.

Figure 3. Diagram from the Spanish National Cryptologic Centre on the deployment of hybrid encryption mechanisms[15]


HYBRID SOLUTIONS
USE OF, AT LEAST, TWO OF THE FOLLOWING ALGORITHMS:
• Pre-quantum key exchange
• Post-quantum key exchange
• Pre-shared keys
Additional parameters
Additional input
KDF
Key length (n)
Hybrid key of length n
CCN
centro criptológico nacional

Source: Task Force Resource, Spanish National Cryptologic Centre.

[15] On this diagram, a key derivation function (KDF) combines multiple inputs, including a pre-quantum key and a post-quantum key, to yield a hybrid key. In practice, most systems will not use three encryption methods. Bottom line is that multiple independent keys fed into one cryptographic combination.

Box 2. Hybrid encryption methods: the Task Force's take

The term hybrid is commonly used in the context of the post-quantum transition to describe the simultaneous use of classical and quantum-resistant cryptographic primitives, most often in reference to the combination of public-key algorithms such as ECC and PQC (i.e. Kyber). Within the European Union's official policy framework, particularly the PQC Roadmap developed by the dedicated workstream of the NIS Cooperation Group, the concept of hybrid cryptography is employed in a narrow and specific sense, referring to the combination of PQC algorithms with classical public-key cryptography (i.e. RSA or ECC). The NIS Roadmap does not reference or include other forms of hybridisation, such as those involving QKD or pre-shared keys (PSKs). However, the Commission's Recommendation on a Post-Quantum Cryptography Roadmap (11 April 2024, Recital 6) and the 2024 White Paper on How to Master Europe's Digital Infrastructure Needs both refer to PQC/QKD hybridisation as part of a layered quantum-safe approach.

The Spanish National Cryptologic Centre instead defines a hybrid key as one that uses at least two of the following: a traditional pre-quantum algorithm, a post-quantum algorithm, and/or a pre-shared key. The inclusion of a PSK (a long-term secret shared out-of-band) provides an additional hedge. Even if both public-key schemes were broken, an attacker still requires the pre-shared secret. In specialised contexts, such as military communications, triple-hybrid approaches might be employed.

It should be noted, in this context, that the classical PQC hybrid model focuses on preserving existing cryptographic assurances against classical attacks while gradually introducing quantum resistance. However, hybridisation can also serve broader goals, such as diversifying trust anchors or enhancing systemic resilience. For instance, hybrid key exchanges may combine PQC with classical public-key algorithms, PSKs, or QKD-based mechanisms, not only to maintain backward compatibility but to create multi-layered defence architectures. In such architectures, QKD might secure lower-level communication links (e.g. between routers or data centres), while PQC provides end-to-end encryption at the application layer.

Because these configurations raise interoperability and coordination challenges, standardisation bodies such as ETSI, IETF, and ISO are actively defining protocol formats and negotiation schemes for hybrid use. ETSI TS 103 744, for instance, defines concrete message formats and cryptographic compositions for hybrid key establishment, including flexible extension fields to accommodate PSKs or additional algorithms. ETSI is also developing an authenticated quantum-safe hybrid key establishment (AQHKE) specification.

Against this background, we recommend using the broader term 'hybrid solutions' to denote a context-aware and technically inclusive approach encompassing all strategies that combine multiple cryptographic inputs.

4. CHALLENGES TO THE TRANSITION TO QUANTUM SAFE

In the global tech marketplace, the implementation of quantum-safe cryptography has already begun, often faster than policy development. Some organisations are deploying crypto-agile solutions in anticipation of future standards. This means that market forces and vendor initiatives are driving early adoption even without a firm regulatory push. The timeline developed by the NIS Cooperation Group foresees significant action by between 2026 and 2030, but risks being overtaken by industry realities.

Differing transition speeds across jurisdictions pose significant challenges for industry. Global enterprises and technology vendors must navigate a two-speed environment where some markets demand rapid PQC adoption, and others remain in a holding pattern. This misalignment forces difficult choices. A fragmented approach could result in duplicative development, increased costs, and potential security vulnerabilities.

Below, we outlined the key risks and constraints that arise from an uncoordinated PQC transition:

- **Two-speed transition risks**: Vendors developing cryptographic products face incompatible requirements when jurisdictions adopt quantum-resistant standards at different paces. Supporting divergent cryptographic baselines across markets is technically inefficient, increases the risk of implementation errors, and creates significant overhead in testing, updates, and certification. Maintaining separate product versions (e.g. one with PQC enabled for jurisdiction A and another without it for jurisdiction B) is rarely sustainable. As a result, many global companies are likely to adopt PQC universally only once a global minimum requirement is established. This dynamic encourages organisations to **delay implementation until harmonisation is reached**, effectively bypassing slower-moving jurisdictions. Products deployed in those markets may still include post-quantum features, but without alignment to local regulatory expectations. For the EU, a relatively cautious transition timeline risks undermining strategic autonomy, as essential infrastructure could become dependent on cryptographic systems shaped by faster-acting foreign standards.

- **Standardisation and compliance gaps**: Core internet security standards (TLS, Internet Protocol Security (IPsec), etc.) are being updated with PQC options, but regulatory timelines differ. Organisations trying to comply face a puzzle: some regulators only issue voluntary guidelines, while others plan to ban legacy algorithms by specific dates. This inconsistency fosters a troubling ambiguity in compliance, undermining clarity and accountability. A product that is 'quantum safe' enough for one country might not yet be approved in another (or vice versa).

Procurement becomes complex. For instance, an EU customer may not explicitly require PQC capability today, whereas a US government client might refuse a product that lacks it. Vendors must either meet the strictest common denominator (potentially incurring extra cost and complexity early) or risk having to retrofit solutions later for different markets, because of a lack of crypto agility. Moreover, companies worry about betting on the wrong technical standard without a clear global consensus on which quantum-resistant algorithms to use and when. Early movers could implement a scheme that certain national authorities later reject, leading to the re-engineering of technologies and incurring additional costs. For instance, if an organisation follows a non-NIST-compliant roadmap, it may later be rejected by EU regulatory bodies. At the same time, some European authorities have adopted a more diversified approach, recommending algorithms outside the NIST-selected set, such as FrodoKEM and Classic McEliece. FrodoKEM is already included in ENISA's cryptographic recommendations, showing that European regulators are exploring alternative paths towards quantum security while global consensus is still forming.

- **Operational bottlenecks:** Even with aligned policies, the practical rollout of PQC faces resource and supply challenges. The lack of a skilled workforce familiar with quantum-resistant cryptography makes it difficult to implement and audit the new algorithms at scale. This talent crunch could slow down deployments of the respective policy. Additionally, the supply chain security of PQC solutions is a concern. Many companies rely on third-party libraries (open-source or commercial) and hardware (i.e. hardware security modules (HSMs), secure chips) to enable PQC. Ensuring these components are trustworthy and integrating them without introducing vulnerabilities is essential. Early implementations require rigorous testing, as any flaw in a widely used PQC library could have global repercussions. If rushed, supply chain vetting and developing certified, standard-compliant components may become a bottleneck. The transition is a policy timeline issue and an operational challenge; it requires sufficient experts, robust tools, and secure distribution of quantum-safe technologies. These factors further underscore why a piecemeal, country-by-country transition is problematic.

PART IV. Post-Quantum Inventories

1. Approach

In preparation for the shift to post-quantum cryptography, organisations are increasingly focusing on how cryptographic and product inventories are built and maintained. What emerges is not a rigid blueprint, but rather a set of guiding practices, shaped by early planning, collaboration across technical and governance teams, and a clear understanding of what such inventories need to capture and why. The goal is to develop a shared language and operational map that allows different actors to approach their inventories not as isolated checklists, but as evolving tools supporting broader transition strategies. This framework will incorporate early planning, cross-functional coordination, and a primary goal of understanding how to approach inventories methodically and structurally. Cryptographic and product inventories are two different assessments.

Cryptographic inventories are a detailed mapping of where and how cryptography is used across an organisation's systems. Their objectives are to identify the cryptographic algorithms in use, their implementation context (code signing; TLS for communications), their quantum resistance status (legacy or PQC), and the dependencies of cryptographic modules and standards (such as Open Secure Sockets Layer (OpenSSL) and HSMs). Mapping cryptographic inventories allows one to understand the cryptographic logic and the primitives inside one's systems.

Product inventories focus on external products, services, and hardware that an organisation uses (i.e. third-party providers), and map the cryptographic characteristics of these products. This allows for determining the vendor's cryptographic roadmap: if they support PQC, what is the timeline for its transition and to what technology, the precise cryptography embedded in procured technologies like firewalls or cloud platforms, potential interoperability between systems, and compliance with standards on cryptography and certifications. Overall, the first focuses on how cryptography operates within an organisation's environment, while the second concerns products the organisation depends on, which are embedded by design.

A key theme of cryptographic inventories is **to adopt a risk-based approach** to prioritise the critical systems that need PQC first. Not all systems and data carry equal risk. Therefore, efficient inventory mapping should be **hierarchical**, focusing first on the most vulnerable assets. It is recommended that enriching existing inventories with context on the importance and sensitivity of each item be considered. Cryptographic uses protecting sensitive and long-term needed data, such as confidential archives, patents, or company proprietary systems (i.e. applications or internal software), would be at the top of the list.

Scanning the IT environment to determine where cryptography is used and adding metadata to classify the specific protected data would create a prioritised inventory. This risk-centred hierarchy guides organisations to create tiers of inventory entries (i.e. high, medium, or low risk) to allocate remediation resources effectively.

When cataloguing cryptographic assets, it is essential to be aware of the intertwined infrastructure of the systems mapped. This is particularly relevant for sectors such as telecommunications. In large networks and critical infrastructures, cryptography is embedded in interdependent components. Therefore, the organisation's product inventory must consider these external dependencies and constraints (e.g. a telecom operator's inventory uses routers or inter-provider communication protocols over which they have no control). This issue circles back to the potential risks of a two-speed transition in Part III (on challenges to the transition to quantum safe), where vendors developing cryptographic products face incompatible requirements when jurisdictions adopt quantum-resistant standards at different paces. This dynamic encourages organisations to **delay implementation until harmonisation is reached.** This time, not across jurisdictions (although it does imply this issue as well in certifications and standards), but across ecosystems; even if one organisation is ready to deploy PQ algorithms, it might need to wait for coordination between equipment vendors, partners, or customers to support them as well. Therefore, any inventory framework should capture not only internal systems but also cryptographic elements in external infrastructures they depend on, with notes on vendor roadmaps or standards timelines. This would ensure that PQ migration plans remain realistic and coordinated within a broader supply chain of a transnational network environment, avoiding situations where one component upgrades to PQ while others remain legacy encryption-based.

2. PRODUCT INVENTORIES

Organisations can use practical tools and processes for a cryptographic assessment of their product inventories. Updating the procurement guidelines to include cryptographic requirements and addressing inquiries could be an option. In other words, when purchasing new software, hardware, or cloud services, organisations would require vendors to disclose the cryptographic algorithms and protocols used in their products, potentially including a roadmap for post-quantum upgrades.

This could be facilitated through **structured vendor questionnaires**, seeking to understand what encryption algorithms are used in the product, if these are quantum-safe, and what the PQC compliance process of the organisation is. By integrating questions into the procurement and vendor management process, organisations will obtain the necessary information for their inventory mapping. This will ensure transparency from suppliers, helping to identify third-party components that use legacy cryptography, and implying that no external dependency is overlooked during the quantum transition. In practice, this means that for every significant third-party product or service in use, the inventory records the cryptographic mechanisms it relies on (for instance, 'Product X uses RSA-2048 for secure communications' or 'Cloud service Y uses TLS 1.2 with ECC, scheduled to upgrade to post-quantum TLS by 2025'). This allows for the centralisation of all cryptographic dependencies in one place, paying attention to blind spots in risk analysis by keeping a product cryptography inventory alongside the cryptographic inventory, and enabling proactive engagement with suppliers ahead of the quantum threat.

3. CRYPTO INVENTORIES

Crypto inventories need to identify, classify, and monitor cryptographic usages, which can be time- and resource-consuming. Focusing on in-house assets, the elements within a cryptographic inventory include the algorithms embedded in code, the protocols used, the configurations of cryptographic libraries, or the hardware supporting encryption processes.

The data recorded in such inventories must be granular and detailed, and include:

- the type of algorithm in use (RSA-2048, ECC, AES-128, Secure Hash Algorithm (SHA)-2, etc.)
- the functional purpose of that cryptography (i.e. authentication, confidentiality, integrity)
- the protocol context (i.e., TLS 1.2, IPsec, Secure/Multipurpose Internet Mail Extensions (S/MIME))
- the asset where it is used (i.e. firmware update signing for routers, internal APIs in applications, VPN concentrators)
- the origin of the cryptographic function (i.e. in-house developed, third-party library, OS kernel module)
- its compatibility with PQC standards, or whether it is part of a hybrid scheme
- the lifespan of the data it protects (short-term v long-term stored data)
- the sensitivity of the data it protects (proprietary, classified).

Tools such as CodeQL can identify cryptographic primitives and flag insecure or outdated usages. Used by developers and security researchers to automate security checks or to perform variant analysis, enabling one to view the languages, libraries, and frameworks of one's organisation. It may enable direct source code analysis, generate machine-readable inventory outputs, and identify insecure instantiations (such as deprecated hash functions), aligning with emerging standards of Cryptographic Bills of Materials. This enables the automated assessment of cryptographic inventories, determining the quality, origin, and expiry risk of the components within the cryptographic environment.

IBM's Crypto Discovery and Inventory tool (zCDI) offers an example of how enterprise-grade infrastructure can embed cryptographic visibility directly into system-level telemetry. It continuously scans and aggregates information about cryptographic usage across IBM Z environments, mapping libraries, key lengths, cypher modes, and usage contexts. Crucially, it associates cryptographic elements with application metadata and business processes, allowing organisations to prioritise migration not only based on algorithmic risk, but also on operational criticality and compliance needs. This system-level integration reflects the shift from passive cryptographic inventories to actionable intelligence.

Although tools may be more effective through automation, cryptographic inventories aren't simply an enumeration exercise; comprehensive scanning is often misleading and lacks prioritisation. Furthermore, a complete cryptographic mapping can divert the limited resources of a cybersecurity budget. Determining which assets need to change from a business prioritisation perspective is necessary (a hierarchical risk-based assessment is recommended, as mentioned in Part I).

Long-tail software components, open-source modules, and embedded firmware pose challenges because of slower update cycles. PQ-secure algorithm in one part of the stack can be undermined by firmware or bootloaders that are not quantum-safe. Inventories should include ageing products and plan for hybrid solutions that maintain backward compatibility while preparing for PQC rollout, assuring awareness of interdependencies within the internal networks.

Therefore, the risk-based classification system implies the mapping of cryptographic items assigned a score or tag based on their data sensitivity, algorithm vulnerability, exposure window, lifespan of protected data, update capacity, and dependencies (upon product inventory input). Within this framework, a legacy VPN using RSA-1024 with no vendor roadmap, protecting long-term archive data, and dependent on secure boot by the manufacturer would likely be flagged as high risk. Conversely, a short-lived internal session between microservices using stream cypher AES-256 may be low risk.

In that sense, cryptographic inventories serve as technical compasses guiding quantum migration, requiring both technical resources and strategic thinking to understand the value that lies within the inventory and how to prioritise it.

PART V. STATUS OF THE TRANSITION TO QUANTUM SAFE: EUROPEAN UNION (EU, FRANCE, GERMANY, THE NETHERLANDS)

1. INTRODUCTION

This section examines how the European Union and three of its Member States, namely Germany, France, and the Netherlands, are approaching the transition to quantum-safe cryptography. We begin with the EU's overarching strategy, which frames PQC and QKD within the broader agenda of digital sovereignty and the digital single market. We then turn to the selected national cases. The choice of Germany, France, and the Netherlands reflects both analytical and practical considerations. These countries represent early movers in the quantum-safe transition, each playing a leadership role at the European level. Germany has acted as a policy front-runner through the German *Bundesamt für Sicherheit in der Informationstechnik* (BSI) (Federal Office for Information Security) guidance and by co-chairing the EU roadmap process. France has integrated quantum cryptography into a comprehensive national quantum strategy, backed by substantial investment and state-led pilot projects. The Netherlands, while smaller in scale, offers a distinctive model of ecosystem-driven innovation and cryptographic agility, and it co-chairs the EU PQC working group alongside Germany and France. Together, these three cases provide a representative picture of Europe's strategic, institutional, and technical approaches to quantum-safe cryptography, while also highlighting differences in emphasis, implementation style, and reliance on state versus multi-actor coordination.

2. EUROPEAN UNION

2.1. STRATEGY AND VISION

The European Union's approach to quantum-safe cryptography centres on **coordination** among Member States and the pursuit of **digital sovereignty**. At the EU level, PQC is viewed as an urgent strategic transition that requires a synchronised timeline across all countries. In April 2024, the European Commission issued a Recommendation calling for a 'Coordinated Implementation Roadmap', encouraging each Member State to develop a comprehensive national PQC migration strategy so that Europe can move in alignment. While security and defence are largely national competencies, EU officials frame PQC readiness as integral to Europe's digital single market and therefore dependent on cybersecurity regulation.

In parallel, the EU envisions **QKD** as a complementary pillar of future-secure communications, especially for government and critical infrastructure. Under the European Quantum Communication Infrastructure (EuroQCI) programme, the EU aims to establish a **pan-European QKD network** spanning all 27 Member States via terrestrial fibre links and satellites.

2.2. Analysis

2.2.1. EU misalignments

Despite Europe's strong cryptographic research community and ambitious strategies, notable **misalignments exist between policy vision and practical execution**.

One issue is the **imbalance in funding and focus**. EU investments in quantum communication (QKD and related infrastructure) significantly exceed those dedicated to implementing post-quantum cryptography. This disproportion has led to a situation where large test networks for QKD are being built, while relatively fewer resources are allocated to help industry and governments migrate their everyday encryption to PQC. Such a gap could limit the pace and scale of practical impact because PQC upgrades, which are more immediately critical for most digital systems, may lag without sufficient funding, tooling, and personnel training. The current disparity in investments carries **potential opportunity costs**. While the development of quantum communication networks represents a valuable long-term strategic endeavour, these projects remain, for now, limited to specialised use cases. In parallel, the migration to PQC offers a more immediate and broad-based improvement to digital security, benefiting virtually all sectors that rely on public-key systems. Ensuring a balanced allocation of resources between exploratory quantum infrastructure and deployable quantum-safe measures will therefore be essential to maximise security returns during the critical transition period[16].

Technical maturity is also uneven across the quantum-safe spectrum. Symmetric cryptography (e.g. using longer AES keys) and key exchange protocols can be made quantum-resistant, and pilot implementations are underway. **PQC replacements**, however, are at an earlier stage: the leading algorithms have only recently been standardised, and integrating them into real-world protocols (such as TLS, secure email,

[16] Some Task Force participants cautioned that this interpretation might overlook the **strategic rationale behind current funding priorities**. Investments in QKD and quantum networking do not aim solely to counteract Shor's algorithm, but to advance the quantum technology agenda more broadly. This includes developing useful and usable quantum networks and securing photonic and communication-grade component supply chains. From this perspective, **quantum communication programmes and PQC efforts should be seen as complementary stages of a unified cryptographic modernisation pathway**. PQC and crypto agility represent immediate steps towards securing existing infrastructures, while QKD and symmetric-key infrastructures can provide later-stage diversification and defence-in-depth through hardware-based trust and long-term resilience. As such, the persistent framing of 'PQC versus QKD' is counterproductive. Both communities ultimately pursue certifiable, standardised, and interoperable solutions that enhance cryptographic resilience. Closer coordination could ensure that quantum-security funding not only supports research and network pilots but also bridges the gap toward deployable and certifiable cryptography, relieving pressure on under-resourced cybersecurity agencies expected to deliver this transition. In this view, PQC and QKD are not rivals but mutually reinforcing instruments for strengthening Europe's digital autonomy.

and authentication systems) is still largely experimental. There are also **gaps in standardisation and certification** for these new algorithms. Europe lacks transparent, scalable processes to **validate** PQC implementations or certify products (such as smart cards, HSMs, and VPNs) as quantum-safe. In contrast, a significant amount of effort in QKD has been devoted to devising certification schemes and standards, indicating that the 'softer' aspects of PQC (standards, compliance, training) require a similar push.

Additionally, **funding continuity and alignment** between EU programmes is not fully achieved. Horizon Europe funds a plethora of promising PQC research prototypes and methods (as noted, many algorithm candidates came from EU-funded teams). Still, the transition to deployment via Digital Europe or national projects is slow and not centrally coordinated. The European Commission has itself identified the risk here. Without better alignment, deployment programmes may 'take off' before the research has resolved key issues, resulting in either delays or investments in solutions that later prove suboptimal. In short, Europe has a strong strategic vision for quantum-safe cryptography. Still, the **implementation mechanisms** are not yet fully synchronised (from adequate funding for PQC v QKD, to consistent standardisation efforts, or synchronised research-to-deployment pipelines). This misalignment could result in fragmented efforts, with some Member States or industries forging ahead while others fall behind, thereby undermining the very unity the EU seeks.

Another misalignment arises from the EU's policy approach of using **recommendations and indirect legislation** rather than binding laws (stemming from the principle of subsidiarity in security matters). The April 2024 Recommendation on PQC provides guidance and timelines but carries no legal force: it is up to Member States to act upon it. However, the text also warns that **binding measures could follow** if sufficient progress is not achieved at the national level. Meanwhile, upcoming regulations like the Cyber Resilience Act (CRA) **implicitly** nudge stakeholders towards quantum readiness by requiring 'state-of-the-art' security practices. The Commission's 2024 White Paper, How to Master Europe's Digital Infrastructure Needs, clarifies this link, stating that compliance with the CRA 'could entail, where appropriate, the use of quantum-resistant cryptography'. In practice, this could imply that by the time the CRA is fully enforced (December 2027), using non-quantum-safe cryptography could be considered outdated. However, since PQC isn't explicitly mandated, companies might defer action, citing a lack of precise requirements. The result is a **policy gap**: the EU's strategic ambition to enable a transition to PQC is clear, but its **implementation remains cautious**, relying on voluntary coordination and national initiative. Member States have varying capacities and urgency levels. Some, such as France and Germany, are early movers on PQC, while others have barely begun. Without a binding EU-wide mandate, the speed of transition may depend on local political will and awareness, precisely what the coordinated roadmap was intended to overcome.

Finally, on the research and innovation front, there is a recognised need for **broader cross-disciplinary work** that the current structures haven't fully achieved. PQC and QKD often progress in separate silos (one in maths/computer science labs, the other in physics/engineering labs), yet the real world may use them in combination (e.g. hybrid networks). European programs highlight the importance of combining expertise, such as cryptographic algorithm design with side-channel resistance, to ensure new PQC algorithms don't introduce vulnerabilities in hardware, or integrating QRNGs to strengthen both classical and quantum crypto systems.

2.2.2. Possible risks stemming from misalignments

These misalignments carry several **risks for the EU**. One is the potential undermining of Europe's goal of technological **sovereignty**. If the transition to quantum-safe cryptography in Europe lags behind that of other global powers, European industries and governments may be forced to rely on external solutions. For instance, should US regulations mandate a particular set of PQC algorithms by 2025-2026, US companies may invest more quickly to develop technologies and may dominate the market before EU companies get started. European companies and public services would then have to adopt these products, procuring software libraries or hardware from non-European vendors, possibly **diminishing Europe's control** over the security of its information[17].

Yet there is also a risk if Europe **moves ahead on a divergent path** without global alignment. If the EU promoted a unique set of home-grown cryptographic standards that are not recognised elsewhere, European tech products might face interoperability issues or be locked out of international markets. Firms in the EU could invest in tailoring their systems to EU-specific algorithms, only to find that clients in the US or Asia require NIST-standard algorithms (or vice versa), forcing them to maintain multiple versions or lose business. Such fragmentation would hurt especially smaller European companies and startups, which have fewer resources to accommodate different standards.

Another risk stems from the **non-binding nature of EU guidance**. Without enforcement, there is a scenario wherein some **Member States procrastinate** in updating their systems. We could imagine uneven readiness across the Union by the time quantum computers

[17] Some Task Force participants noted that although a slower pace of innovation may hinder European companies, it does not necessarily compromise the EU's ability to ensure its own security. As a matter of fact, NIST algorithms are open, transparent, and shaped by significant European contributions, allowing Europe to adopt and certify them within its own regulatory frameworks. **Sovereignty, in this view, lies not in creating new algorithms but in ensuring trusted implementation, governance, and resilient deployment.**

arrive: a few states might have robust PQC and QKD infrastructure, while others still run legacy, vulnerable cryptography. This patchwork not only threatens those lagging states but also the **collective security**, since data flows across borders. A weakest-link problem emerges: an insecure node in one country's network can be the entry point for attacks affecting others. It would also politically undermine the credibility of the EU's cybersecurity agenda if, after years of warnings, a major breach occurred because of the slow implementation of PQC in some corner of Europe.

Furthermore, there are significant risks in pursuing an EU quantum-safe roadmap without a coordinated, risk-aware strategy. A roadmap must specify what milestones are required and by when, but only a supporting strategy can define how Member States, vendors, and institutions will meet them. Without synchronised standards, certification schemes, interoperability frameworks, and testing infrastructures, regulation may outpace readiness. The Roadmap should therefore be embedded in a broader EU framework that aligns national plans, industry efforts, and regulatory tools, ensuring coordination across the CRA, the Digital Operational Resilience Act (DORA), and NIS2, and guided by the institutional actors of ENISA, the Commission and standardisation bodies of ETSI, European Committee for Electrotechnical Standardization (CEN/CENELEC), to deliver a coherent, actionable transition.

3. Germany

3.1. Strategy and vision

Germany's national strategy on quantum is characterised by early acknowledgement of the quantum threat and a methodical plan to achieve quantum-safe security, both nationally and in the European context. The BSI has been warning organisations since 2020 to 'migrate to Post-Quantum Cryptography', and it has issued detailed recommendations on quantum-safe cryptography. Germany's vision aligns with the principle of 'act upon the quantum threat now'. In practice, this means that Germany aims to transition its government and critical infrastructure systems to PQC well before a cryptographically relevant quantum computer becomes available. The BSI has set interim guidance (i.e. recommending ≥ 128-bit classical security algorithms only be used until 2030-2035 unless replaced by PQC by then), consistent with the US timeline. Strategically, Germany also envisions itself as a leader in coordinating Europe's PQC efforts, as it co-chairs the EU's PQC Roadmap initiative and contributed to the 2024 EU joint statement on PQC. There is also a sovereignty angle: Germany views robust cryptography as essential to digital sovereignty (a term emphasised by German officials in the EU context), ensuring that German and European data remain secure, regardless of foreign tech dominance.

On QKD, Germany's strategy is more cautious but determined in niche areas. The government launched the QuNET initiative in 2019, a multi-year programme designed to develop secure quantum communication networks for public authorities. The vision is that by the mid-2020s, Germany would have a pilot quantum network enabling tap-proof communications between key federal agencies.

3.2. ANALYSIS

Germany's policy attitude towards quantum cryptography seeks to develop a multi-actor ecosystem that bridges government, industry, and research. BSI acts as the central authority, sharing technical requirements and certifications supported by other ministries, such as the Ministry of Interior and the Ministry of Research, Technology, and Space, for implementation and funding of R&D. Initiatives such as QuNET and PARFAIT tie federal priorities to pilot projects, which embed PQC and QKD in concrete scenarios. Internationally, Germany positions itself as a standardisation leader, ensuring interoperability and European sovereignty in the quantum-safe transition.

4. FRANCE

4.1. STRATEGY AND VISION

France's quantum cryptography strategy is embedded in its overall quantum strategy. France launched a national quantum strategy in 2021 under the France 2030 investment plan, backed by a EUR 1.8 billion commitment (including EUR 1 billion public funds). This strategy seeks to position France as a leader in quantum technologies by 2030, combining state funding, private investment and academic excellence. It encompasses quantum computing, communications, sensing and cryptography, with EUR 150 million earmarked specifically to develop cryptographic methods resistant to quantum attacks. It has five pillars, including 'developing and disseminating post-quantum cryptography' as a strategic priority. Over 80 projects have been funded, and new programmes such as PROQCIMA (for indigenous quantum computers by 2032) have been launched. In November 2022, France successfully sent its first diplomatic message encrypted with post-quantum cryptography (using FrodoKEM via the French company CryptoNext Security) between its embassy in Washington and Paris, marking a milestone in high-level government engagement with PQC.

4.2. ANALYSIS

France's political stance on the transition to quantum-safe systems is state-driven, centred on the French National Agency for Security of Information Systems (*Agence nationale de la sécurité des systèmes d'information* (ANSSI)), the, as the leading authority. The institutional body promotes hybrid cryptography as the immediate solution to the transition, through hybrid classical and PQC algorithms. France also co-chairs the EU PQC working group, alongside Germany and the Netherlands, standing for European standards, R&D efforts, and, more practically, crypto agility and hybrid schemes. State policy is reinforced by a broader quantum in defence programme, which includes promoting PQC and quantum communication methods, as part of a wider plan to develop quantum technologies for military and defence purposes. The involvement of private actors in pilot projects is privileged, as seen in the RESQUE consortium on quantum networks secured by PQC-QKD links. This includes a major telecom operator, Orange, which illustrates the strategic autonomy objectives through industrial preparation and testing.

5. The Netherlands

5.1. Strategy and vision

The Netherlands has made quantum technologies a national priority, focusing on innovation and infrastructure while integrating security considerations. In 2021, the Dutch government awarded **Quantum Delta NL (QDNL) EUR 615 million** from the National Growth Fund, a comprehensive national initiative to develop a full-stack quantum ecosystem. It supports five innovation hubs (Delft, Eindhoven, Amsterdam, Leiden, and Twente) and projects in quantum hardware, software, quantum internet, and talent development. While primarily focused on R&D and economic development, QDNL also indirectly bolsters security by advancing **quantum communication networks** (i.e. piloting metropolitan QKD links and preparing for Europe's Quantum Secure Network).

In parallel, the Netherlands relies on its national security apparatus[18] to guide cryptographic policy. The Dutch National Communications Security Agency as explicitly advised Dutch organisations to prepare now to migrate to quantum-resistant cryptography and not to delay planning for PQC. In 2024, the National Security Agency (together with CWI and TNO) released the second edition of *The PQC Migration Handbook*, providing organisations with step-by-step guidelines for transitioning to post-quantum cryptography. It outlines a three-phase approach: (1) quantum-vulnerability diagnosis: identifying cryptographic assets and assessing quantum risk; (2) planning: prioritising systems and devising a migration roadmap; and (3) execution: deploying PQC solutions and testing their integration. The handbook strongly recommends establishing **cryptographic agility** (the ability to swap crypto algorithms easily) to facilitate this and

[18] See https://www.aivd.nl/.

future transitions. Dutch agencies have also run pilot projects (in ministries and critical infrastructure) to inventory cryptography and experiment with hybrid (PQC + classical) implementations as proofs of concept.

Policy is implemented through pilots in ministries, banks, and telecoms, supported by strong public-private cooperation. Internationally, the Netherlands co-chairs the EU PQC working group with France and Germany and actively contributes to NIST and EuroQCI, positioning itself as a **bridge between cutting-edge research, standardisation, and responsible deployment**, with an emphasis on hybrid solutions and ethical governance.

5.2. 5.2 Analysis

The Dutch take a hands-on approach to the quantum transition, embedding the migration to PQC into a broader culture of cryptographic agility. Corporations can appreciate the guidance of the public sector. What the Dutch do particularly well is combining this applied experimentation with broad stakeholder inclusion: startups like QuSoft and QBird, major telecom operators and banks are brought in early, making migration a shared responsibility. By simultaneously co-chairing the EU PQC working group and contributing to NIST and EuroQCI, they ensure that national practice shapes international norms. In short, the Netherlands excels at leveraging technical credibility and ecosystem cooperation to foster collective leadership, demonstrating how to bridge policy, research, and industry in advancing quantum-safe security.

PART VI. STATUS OF THE TRANSITION TO QUANTUM-SAFE: EXTRA-EU (UK, US, CHINA)

1. INTRODUCTION

This section turns to three non-EU actors, the United Kingdom (UK), the United States (US), and China, whose strategies are particularly influential in shaping the global transition to quantum-safe cryptography. The case selection reflects their global significance. The US and China are the two main poles of technological competition in quantum technologies, with substantial resources, geopolitical ambitions, and the capacity to set de facto global standards. The UK has pioneered practical migration roadmaps and participates actively in transatlantic standardisation forums, influencing both industry practice and allied coordination. Together, these three cases provide a comparative lens on how different governance models are operationalising the quantum-safe transition, and what this implies for international alignment, sovereignty, and interoperability.

2. UNITED KINGDOM

2.1. STRATEGY AND VISION

The UK's transition strategy to PQC is shaped by the guidance of the National Cyber Security Centre (NCSC), the country's national technical authority for cybersecurity. The NCSC has set out a three-phase migration roadmap with indicative target dates. **Phase 1 (by 2028)** requires organisations to complete discovery and planning. This involves compiling a high-level cryptographic inventory, not a detailed audit of every key and algorithm, but an organisational map of where public-key cryptography is embedded across systems, services, and products. Such mapping allows engagement with suppliers and identification of long-lived sensitive data that needs early protection. The emphasis is on developing an initial migration plan, recognising that standards may evolve, algorithms may reveal weaknesses, and vendor products will change. **Phase 2 (by 2031)** calls for prioritised migration, focusing on data that must remain secure for more than a decade. The logic is to shield sensitive, long-lived information against harvest-and-decrypt risks while avoiding premature disruption to business-critical processes. Importantly, organisations are cautioned not to attempt their most critical systems first, since initial migrations are more prone to errors. Pilot projects and iterative planning are therefore essential. **Phase 3 (by 2035)** aims for full migration, ensuring all systems, services, and products have transitioned to PQC, while simultaneously taking the opportunity to strengthen overall cyber resilience, given that a wholesale review of digital infrastructure will already be underway.

The technical approach stresses **crypto agility** and staged **hybrid deployment**. Organisations are encouraged to build systems that can swap algorithms with minimal redesign, enabling flexibility if new vulnerabilities are discovered or standards evolve. **Algorithm choices largely mirror the NIST process**, with Module-Lattice Key Encapsulation Mechanism (ML-KEM) recommended for key establishment, Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for signatures, and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) reserved for long-lived anchors and firmware. While NIST's Hamming Quasi-Cyclic (HQC) was identified as a possible backup to ML-KEM, it is absent from the NCSC's published guidance.

The broader context situates PQC within the UK's National Quantum Strategy, which commits GBP 2.5 billion over ten years. PQC is recognised as a core component of this vision, not only as a defensive necessity but as part of a strategic technological capability. The NCSC has already launched a pilot programme, with eight companies offering PQC migration support, to build capacity across the ecosystem. The implementation approach relies less on hard mandates and more on procurement requirements and market nudges. For example, government contracts and defence procurement demand compliance with baseline cybersecurity frameworks, which will naturally extend to PQC as standards mature. This approach recognises that many organisations are not motivated by cryptography per se but by the products and services they procure; as vendors embed PQC into offerings, adoption will cascade.

3. United States

3.1. Strategy and vision

The US frames quantum-resistant cryptography as a near-term cybersecurity imperative. A 2022 White House National Security Memorandum 10 (NSM-10) declared that 'the United States must prioritise the transition of cryptographic systems to quantum-resistant cryptography' by 2035. This urgency stems from the recognition that current public-key algorithms (RSA, ECC, etc.) will be vulnerable to quantum attacks, and that **migrating systems takes years**.

The US strategy is encapsulated in NIST's PQC programme, which, since 2016, has led an open competition to standardise new algorithms. In 2024, NIST published the first set of PQC standards: CRYSTALS-Kyber for key encapsulation (Federal Information Processing Standards (FIPS) 203, also called ML-KEM) and CRYSTALS-Dilithium for digital signatures (FIPS 204, also called ML-DSA), along with two alternate signature schemes (FIPS 205

SPHINCS+SLH-DSA and FIPS 206 Falcon Fast-Fourier transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)). These provide quantum-safe replacements for the algorithms currently in widespread use. NIST continues to solicit additional signature schemes (on-ramp 'Round 2' candidates) to diversify options. Importantly, NIST and federal agencies have outlined a timeline for **phasing out quantum-vulnerable cryptography**: for instance, 112-bit security RSA/ECC is expected to be deprecated by 2030 and disallowed by 2035. Higher-strength classical crypto (256-bit ECC, etc.) is permitted until 2035, by which time quantum-resistant solutions are expected to be in place. This timeline aligns with NSM-10's goal of migrating US government systems by 2035.

3.2. ANALYSIS

The US treats the quantum threat as an urgent national policy. NIST's draft 'Transition to PQC' report explicitly ties its timelines to NSM-10, recommending that 112-bit security (e.g. 3K-bit RSA) be retired by 2030 and all classical public-key schemes by 2035.

NIST and US laboratories are also addressing implementation challenges. The NIST-led PQC Migration Project works with industry to tackle issues of performance, interoperability, and testing. For example, NIST's Cryptographic Algorithm Validation Program is already testing PQC candidates in its Federal Information Processing Standard (FIPS) 140 validation suite. To engage the market, the National Cybersecurity Centre of Excellence (NCCoE) is developing PQC integration guides, and the Cybersecurity and Infrastructure Security Agency (CISA) is assessing risks in critical sectors. On the R&D front, US efforts include quantum networking testbeds. The Chicago Quantum Exchange's new 'Bloch Tech Hub' plans to establish a publicly accessible quantum network testbed specifically for developing QKD and long-distance quantum communication technologies. However, US authorities remain cautious about QKD. National Security Agency (NSA) guidance explicitly states that post-quantum algorithms are 'more cost-effective and easily maintained' than QKD, and it currently does not certify QKD devices for national-security use. In practice, US deployments (in telecom, data centres, etc.) are beginning with hybrid PQC-classical modes, allowing government agencies and vendors to build and validate PQC into TLS, VPNs, and public-cloud encryption while still supporting legacy interoperability.

The US is aligning with allies through standards and policy forums. NIST and Commerce Department representatives are active in the IETF Crypto Forum Research Group and related working groups (e.g. TLS 1.3) to ensure global protocols adopt PQC algorithms. Similarly, US delegates are working in the Joint Technical Committee (JTC) of ISO and the International Electrotechnical Commission (IEC) 1/SC 27 to incorporate the NIST-selected KEMs and signatures into ISO standards. ETSI's new Security Algorithms Group of Experts

(SAGE) working group (Quantum Safe Cryptography) involves US participants and is crafting recommendations for integrating PQC into 5G/6G mobile standards. The US also emphasises 'whole-of-government' partnerships balanced by export controls and R&D protection.

The US view of QKD is that it introduces hardware dependencies (specialised equipment, trusted nodes) that could be a security liability and are not easily scalable – thus, the US is content to let others experiment. At the same time, it focuses on a solution that works over existing networks. However, the US does keep a close eye on QKD developments; if an adversary achieves an exclusive quantum-secure communication capability, the US will not want to be caught entirely flat-footed. For now, though, leadership in PQC and advancing a global migration appears to be the cornerstone of US quantum cryptography strategy

4. CHINA

4.1. STRATEGY AND VISION

China has pursued a vigorous national strategy in quantum cryptography as part of its broader ambition to be a world leader in quantum technology, by deploying quantum-proof and quantum-based cryptography at scale, and to control the standards and core intellectual property of these technologies.

On the quantum key distribution front, China's vision is unrivalled in scope; it envisages a nationwide (eventually global) quantum communication network specifically tailored for government and critical industry channels. This has been endorsed at the highest levels of leadership; President Xi Jinping emphasised the inclusion of quantum communications in China's Five-Year Plans and called it crucial for long-term strategic objectives. As a result, China became the first country to launch a quantum satellite (Micius in 2016) and to integrate satellite and terrestrial QKD into a secure communication network spanning thousands of kilometres.

Alongside this, China is also preparing for the advent of PQC. The government's cryptography authorities have been actively evaluating and standardising new algorithms in anticipation of quantum threats. China's Cryptography Law establishes a framework in which 'commercial cryptography' (used by citizens, businesses, and non-sensitive government information) must protect cyber and information security by law. This law implicitly covers PQC and QKD as future cryptographic means. In line with that, China launched the 'Next-Generation Commercial Cryptographic Algorithms' (NGCC) initiative in February 2025, a global call for new public-key, hash, and block cypher algorithms resistant to quantum attacks. This reflects a vision of self-reliance: rather than simply adopting NIST's choices, China wants domestic or globally submitted algorithms that it can evaluate and potentially standardise nationally. The emphasis is on diversity of mathematical problems (to hedge against any single point of failure) and on retaining sovereignty over core crypto technologies.

4.2. ANALYSIS

China's approach to quantum-safe cryptography is state-driven, expansive, and strategically dual-tracked. On QKD, it treats deployment as a geopolitical asset, already operating large-scale pilots (Beijing-Shanghai backbone, satellite links such as Micius) that no other country matches, translating R&D into nationwide infrastructure. On PQC, the NGCC initiative shows Beijing's intent to avoid dependence on NIST and to shape an indigenous standard portfolio, balancing technical diversity with sovereignty. In essence, China's strategy aims for a comprehensive quantum-security ecosystem under Chinese leadership or control. Geopolitically, quantum cryptography is viewed as a domain where China can leapfrog and set the rules, thereby reducing its reliance on Western crypto standards and ensuring that its own secrets remain secure.

PART VII. TASK FORCE COMMENTS ON THE NIS COOPERATION GROUP ROADMAP

1. NIS COOPERATION GROUP ROADMAP

The transition to PQC, as detailed by the NIS Cooperation Group, is a process with a Roadmap comprising three major milestones (2026, 2030, 2035), along with specific steps to ensure that all Member States become quantum safe on time.

- **Phase 1: by 31 December 2026,** Member States are expected to have laid the groundwork for PQC migration. These 'first steps' involve identifying the essential stakeholders to guide early strategy and coordination within a supply chain that includes vendors and service providers promoting PQC products. Companies shall develop and maintain their cryptographic inventories. Thereon, both suppliers and adopters of cryptographic material should collaborate in mapping out dependencies of companies' cryptographic inventories. Regulatory bodies will need to perform a quantum risk analysis, identifying the systems/data at high risk, as well as develop a timeline and implementation plan with clear priorities (prepare, plan, act phases), in alignment with the EU timeline. Furthermore, the vast array of actors should work hand-in-hand to create national awareness of the quantum threat at all levels, from C-suite executives to IT staff, and engage with EU work streams; no Member State should undertake this transition in isolation.

By the end of Phase 1, critical sectors with long data confidentiality needs or long-life systems are already experimenting with PQC solutions, ensuring a minimum level of readiness across the EU.

- **Phase 2: by 31 December 2030.,** all Member States should have implemented the following 'next steps'. The allocation of resources in the transition is necessary by both private and public actors, within a specific set of regulations that mandate quantum-safe cryptography. The adaptation of certification schemes in standards and guidelines (e.g. the EU Cybersecurity Act) to be up to date. Furthermore, the domestic and international collaboration between public, private and academia should be solid, by looking for opportunities within the ecosystem to accelerate the transition (e.g. professional training programmes, or research initiatives to support the migration). Finally, there is a need for engagement with European testing infrastructures to ensure the interoperability of systems across borders.

In this second phase, critical systems are quantum safe, and software sold from this point onwards should support such encryption by default.

- **Phase 3: by 31 December 2035**, the transition should be complete or nearly complete, with all medium- to high-use cases transitioned to PQC. This milestone represents the culmination of the coordinated Roadmap: the point at which data and communications in Europe are secured against the advancing capabilities of quantum computers.

This coordinated timeline ensures that Europe acts with urgency but also with due diligence, avoiding a rushed or chaotic migration. Following these milestones and steps will enable policymakers to safeguard security and confidentiality in the quantum computing era.

2. Task Force Comments on the NIS Cooperation Group Roadmap

2.1. Introduction

This Task Force assessed the Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography published by the NIS Cooperation Group on 11 June 2025 (from now on 'the Roadmap') and put forward the following comments.

2.2. Overall comments on the Roadmap

- We find the Roadmap very well-written and useful. In particular, we appreciate that the milestones align well with the international ecosystem, that the importance of early migration to quantum-safe software and firmware upgrades is emphasised and that the challenges of long transition periods, such as those faced by public-key infrastructures (PKIs) and long-lived devices, are clearly described, along with the need to begin migration planning for these systems as soon as possible.

- We support the EU's comprehensive approach to catalysing the transition to PQC, and we especially welcome the European Commission's commitment to engaging not only with Member States but also with industry and academia. All these stakeholders will play a critical role in helping the Commission design effective support measures for PQC.

- The Roadmap stresses the need for cryptographic inventories and dependency maps, which are essential for identifying vulnerabilities and planning migration steps.

- It recommends tailored awareness campaigns to educate stakeholders about the quantum threat and the importance of PQC migration.

- Furthermore, while it defines itself as a 'high-level concept paper', it is also very action-oriented, emphasises swift implementation and is quite specific. For instance, it prompts the Member States to start working on or updating their transition plans immediately, without waiting for the final deliverable of this work stream and to start implementing next steps in parallel with the first steps, so it tangibly strives to 'ensure a minimum level of readiness in all Member States by the end of 2026'.

- It provides concrete examples of good practice. For example, on page 11, it refers to surveys conducted in France to 'determine market readiness, identify obstacles for the PQC transition and to learn about the needs of three types of stakeholders: providers, users, and consulting companies'.

- It states that relevant regulations and technical requirements or guidance stipulated at the national level should be systematically updated, with state-of-the-art recommendations for PQC. If no such regulations or cryptographic policies exist, Member States should consider creating them, for example, by consulting other countries and the NIS Cooperation Group. Mass adoption will require both the availability of the products and an example set by institutions. Member States should consider starting to integrate PQC requirements in their future national procurement processes, and are encouraged to contact their current IT suppliers to assess their maturity on PQC (page 14).

- The Roadmap **does a good job of emphasising the importance of protecting the confidentiality and integrity of data** (page 4). However, it should also explicitly address the need to protect data during processing, as it is increasingly common to process sensitive information in the cloud. Furthermore, rather than using terms such as 'stored,' 'transmitted' and 'communication', we suggest consistently using the widely accepted formulation of 'protect the confidentiality and integrity of data in transit, at rest, and during processing.'

- **The Roadmap should also explicitly highlight the need to protect availability.** While availability is partially a consequence of integrity protection, it is important for readers to understand that PQC migration also contributes to safeguarding the availability of critical infrastructure. For most critical systems, availability is at least as crucial as confidentiality and integrity, and making this explicit will help convey the full scope of why timely PQC adoption is necessary.

2.3. TIMELINE

- The Roadmap provides a clear timeline with milestones for PQC migration, emphasising the urgency for high-risk use cases by 2030 and medium-risk use cases by 2035.

- Specifically, both the timeline completion date of 2035 and the prioritising approach used are very well chosen. Given the complexities across sectors, the varying maturity across Member States and the need to be clear without being too strict, this document and the Roadmap it describes gets the balance right.

- We support the approach to 'start now' while creating 'first steps' and 'next steps' and the timelines that are proposed by the NIS Cooperation Group.

- We appreciate that the timelines and actions (2026, 2030, 2035) are also broadly consistent with US policy.

- However, as the Roadmap leaves the initiative entirely to individual Member States, it fails to address how their approaches can be harmonised. Moreover, it remains unclear whether the EU will play a coordinating role, and the Roadmap does not specify the consequences of non-compliance.

- **We believe the Roadmap should be updated** to more clearly state that the timelines apply to deployments. For full PQC adoption in deployed systems, it is essential that standards are updated and a stable implementation is made available well in advance of those deployment milestones. The timelines for different stakeholders in the ecosystem, such as standards development organisations, equipment vendors and operators deploying the systems, are inherently different. Standards bodies need to finalise specifications early, vendors need sufficient lead time to implement, test and certify solutions and only then can large-scale deployments take place. A clearer distinction between these stages would help align expectations and ensure that all parties can plan their contributions effectively.

- We welcome the focus on piloting and learning in the field. An important aspect of these pilots should be to pilot the complete stack, since security must be rooted in a PQC-enabled infrastructure.

- We like and support the approach of pushing for PQC-enabled updates to allow continuous improvement. We suggest piloting this with hardware vendors to understand the state of the art and identify gaps to fully achieve this objective. We need to clarify how to handle systems that are not updatable (e.g. because of hardware limitations).

- Pilot use cases should: i) be 'ground up', ii) include hardware, and iii) ensure that application-level pilots are supported by PQC-enabled infrastructures and hardware.

2.4. Threats to cryptographic algorithms

'Quantum computing will be a threat to many of the cryptographic algorithms.'

'The development of quantum computers poses such a threat to cryptography which can be used to break many of the cryptographic algorithms in use.'

- It would be far more informative for the reader if it was specified that only public-key algorithms are threatened by CRQCs. Most readers are not cryptographers with deep knowledge of post-quantum cryptography and quantum attacks. The idea that symmetric algorithms with 128-bit keys are practically threatened by CRQCs is now considered a misconception [2–6]. As explained in the keynote at CHES 2024, a quantum computer breaking a single AES-128 key would require qubits covering the surface area of the Moon. Any focus on increasing symmetric key lengths diverts attention and resources from the urgent priority: migrating to post-quantum **public-key** algorithms. Such a distraction would be both costly and dangerous. Europe is already behind the US in adopting PQC, making it even more important to focus efforts where they are most needed. We therefore suggest the following improved formulations:

*'Quantum computing will be a threat to many of the **public-key** cryptographic algorithms.'*

'The development of quantum computers poses such a threat to public-key cryptography which can be used to break many of the public-key cryptographic algorithms in use.'

- In this context, it is important that the Roadmap acknowledges on page 6 that 'symmetric key methods instead of public key cryptography are worthwhile to consider, depending on the application'.

- This calls for an opportunity to elaborate more on what this can mean in practice: which use cases? Which approaches? Hybrid? The PQC-focused push is largely focused on some of the main large-scale use cases. But those who are responsible for other systems, where it is more complicated than 'just' updating to PQC algorithms, need guidance as well.

We think there are a couple of broad categories of use cases:

- For the 'higher' level applications, which are open, ad hoc, large-scale, etc, systems, PKI remains the elegant solution of choice. However, if the system being protected is critical and/or requires long-term security, it may be worth leveraging some form of 'symmetric key infrastructure' to provide defence-in-depth and higher-confidence long-term security, at least as an option (likely through PSK mechanisms in TLS, IPsec, etc).

For use cases that are smaller or less open, closer to the hardware (e.g. Proprietary Security Protocol for Optical Transport Networks (OTNsec)) or more static in terms of endpoints, etc., then symmetric key methods are more natural. One might still include public-key algorithms, but the complexity of a full PKI may not be necessary.

2.5. Hybrid solutions

'A combination of a post-quantum algorithm and a quantum-vulnerable algorithm for the same mechanism, such that the security is as high as the higher of the ingredients.'

- The definition of 'hybrid' is a bit narrow and focused on retaining our confidence in the security of pre-quantum public key cryptography against classical attacks, while benefiting from the best available security offered by PQC. We at least signal that this is a special case of what hybrid key exchange could be (there are also hybrid signatures but that is even more complicated and have their own differing objectives as well). For example, some refer to combining a PSK (others an out-of-band symmetric key) with a public key cryptography-derived key. For example BSI recommends, if using QKD keys, to combine with PQC and ECC-based keys.

'When migrating to post-quantum cryptographic solutions, it is recommended to use standardised and tested hybrid solutions, whenever feasible and suitable.'

- We believe this should be expanded and clarified. We agree that only standardised algorithms with broad international adoption by industry and government authorities should be used. However, it is important to note that no major body is currently recommending the use of hybrid solutions with hash-based signatures such as SLH-DSA. It should also be clarified that only a freely available specification should be used. Many organisations have taken a firm stance against paywalled specifications for cryptographic algorithms, viewing them as cybersecurity risks. Both the IETF and NIST are working to remove as many references to such algorithms as possible. The NIS Cooperation Group needs to likewise avoid referencing any paywalled cryptographs.

- While hybrid KEMs have been standardised by the IETF and adopted in real-world deployments, hybrid signatures have not achieved the same level of standardisation or implementation maturity. Consequently, hybrid signatures are unlikely to be ready in time to meet the EU Roadmap timelines. Currently, the only signature algorithm supported in OpenSSL 3.5 Long Term Support (LTS) for use in TLS is the standalone ML-DSA. Governments in the US and the UK have also been far more active in driving progress within open standardisation bodies, such as the IETF and ETSI, as well as in supporting the implementation of standalone ML-KEM and ML-DSA in major cryptographic libraries. It is somewhat ironic that the only standardised hybrid KEM specifications (ETSI CatKDF and CasKDF) were driven by the UK government, which now only recommends standalone ML-KEM and ML-DSA.

- The practical reality is that the only realistic migration paths today for industry are hybridised ML-KEM, standalone ML-KEM, standalone ML-DSA and, to some degree, standalone SLH-DSA. Alternative PQC algorithms (e.g FN-DSA) will not be standardised and widely implemented to meet the required timelines.

- In TLS, X25519ML-KEM has already seen massive implementation support and is the default in OpenSSL, Firefox, Chrome, Edge, Go, etc. Cloudflare reports that over 40% of all Hypertext Transfer Protocol Secure (HTTPS) client requests use PQC. OpenSSL 3.5 LTS supports ML-KEM, ML-DSA, and SLH-DSA. OpenSSH is now using ML-KEM as the default key exchange. Many IKEv2 implementations support ML-KEM. IKEv2 always uses ML-KEM in hybrid with Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE). The availability of well-tested and interoperable implementations is an essential factor for industry adoption, as it enables cost-effective, reliable and interoperable deployments

  We believe the Roadmap should be updated to fully embrace ML-KEM, ML-DSA, and SLH-DSA. These are global standards that represent years of collaborative research by leading cryptographers from around the world. Importantly, most of the authors of Kyber, Dilithium, and SPHINCS$^+$ are European researchers, many of them supported by European universities, institutes and companies. Research funding from EU Member States and the European Commission has been instrumental in making this possible. These investments have helped Europe play a central role in securing the world's digital infrastructure against future threats. This is an achievement that the NIS Cooperation Group should explicitly acknowledge and celebrate in its report.

However, we see a risk that mandating hybrid crypto could cause undue performance overhead or may not be enabled on all platforms. We suggest that this should be investigated and benchmarked in depth.

We would also like to mention that a notable difference is the EU Roadmap's strong recommendation for hybrid quantum-safe cryptography, where feasible contrasts with the US approach, more specifically the NSA, which has recommended PQC-only standards. The aim should be to offer customers a cryptographic choice where feasible, recognising that different customers will have different risk considerations. However, some cryptographic decisions – such as those at the infrastructure level – may not be configurable by customers.

2.6. INVENTORIES

'A first essential step and "no-regret" move for every entity is to create and maintain current inventories of assets that perform cryptographic operations.'

- We fully agree that creating and maintaining comprehensive cryptographic inventories is essential. Organisations that are only now starting to compile their inventories should do their inventory creation in parallel with the planning, testing and implementation of ML-KEM, ML-DSA, and SLH-DSA.

  However, we would like to mention that compiling a complete crypto inventory including the supply chain may overwhelm some organisations. We believe that performing top-down inventories and drilling down into applications and usages – guided by continuous risk assessment – may be more efficient since non-compliance of some suppliers or systems may pose a negligible overall risk while others are critical to the enterprise.

  Very few organisations have a good inventory of IT systems and assets. While it may be a good aspiration, the past few decades have shown that it is very difficult to achieve in practice. We believe it is prudent to consider how this part of the Roadmap is formulated, as it may divert organisations from other more important activities in transitioning to become quantum safe.

  Recent experience has shown that attempting to build inventory without a clear understanding of what to do with the inventory may lead to the conclusion that the effort has been wasted. It is very important to be clear on what type of inventory is required and how it can be used.

2.7. Standards

- Overall, we welcome the Commission's recognition that international standards are essential for an orderly transition, as well as its determination to complete the PQC transition for high- and medium-risk use cases in the EU in alignment with the global ecosystem. We also noticed that the timelines and actions (2026, 2030 and 2035) are also broadly consistent with US policy.

- We support a standards-based approach to build on the NIST standards for PQC that were defined through an open competition, involving the world's leading PQC scientists.

- We believe that the number of standards that need to be updated with the new cryptography is not widely understood. Only a handful of the many hundreds of protocol and industry standards have been adapted to being quantum safe. Many industries depend on these standards and will not be able to transition without these standards being updated. We suggest that a list of all impacted standards that need to be updated, together with an estimated timeline for updating them, should be formally requested, from as many standards bodies as possible. This would allow for an understanding of the current situation and help trigger action by the relevant standards bodies.

- We believe that excessive emphasis on certification may prevent the best solutions from being successful on the market. While we see a role for 'process' certification (e.g. ISO 27000) to consciously manage risk and improve systems, we believe that third-party certifications should not be the only way to prove PQC conformity and more industry-driven initiatives and tools should be supported.

- We suggest stronger alignment with the EU CRA process. This could be in the form of certification requirements that make product suppliers list the cryptography that their products contain. This would immediately raise awareness of large parts of the supply chain that organisations will depend on to provide quantum-safe solutions.

2.8. Awareness, cooperation and governance

'In cyberspace all nations are connected across borders and depend on each other also in this transition. Therefore, Member States should create an environment or community where organisations, entities and stakeholders can share knowledge and experiences.'

- We agree that all nations are interconnected, not only in cyberspace but also through trade and global markets. For European industries operating internationally, close alignment with already published global timelines and algorithm recommendations [1-15] is essential. Many European companies are already deeply engaged in the development and implementation of ML-KEM, ML-DSA and SLH-DSA in their products and services, working to meet the ambitious 2030-2035 PQC deployment timelines.

- It is not realistic to expect that each Member State can individually create communities that attract global organisations, entities and stakeholders such as the IETF, the Third Generation Partnership Project (3GPP), the US Government or major US companies. Even coordinating this at the EU level is extremely challenging. Instead, Member States should actively participate in open, global standardisation organisations such as the IETF and 3GPP, as well as in the open-source cryptographic community, to ensure alignment, influence and knowledge-sharing at the international level.
- Member States should lead by example with transparent transition plans: publish and regularly update government transition roadmaps, including timelines, milestones and budgets, to foster knowledge sharing and best practices.
- The Roadmap should broaden its definition of ‘stakeholder’ beyond ministries, regulatory agencies and technical experts. Civil society, minority networks and grassroots organisations should be recognised as co-leaders and not simply ‘consulted’.
- The integration of social clauses and community dividends into procurement, partnership and policy evaluation is vital, not just as a ‘best practice’ but as a requirement for measurable inclusion.
- Awareness campaigns and training modules should not be generic or one-size-fits-all. This CEPS Task Force is asking for a radical expansion of civic and digital education, embedding PQC awareness, quantum risk and digital rights topics not just in technical teams but across society, schools, care institutions and community centres.
- The Roadmap should establish mechanisms (citizen assemblies, consultation panels, regular transparent updates) to ensure citizens not only receive information but can actively shape strategies.
- The Roadmap should encourage joint pilot projects at the EU level to test interoperability of PQC in cross-border services before 2030.
- We suggest establishing a public-private PQC migration observatory under ENISA to monitor advances and recommend acceleration of timelines if necessary.

- As policymakers move forward with implementation, they should avoid prescriptive regulations or requirements that could create engineering or interoperability challenges, either within or across jurisdictions. We advocate for continued international dialogue on transition strategies and standards. As one potential path forward, we would welcome the G7 expanding the scope of its current quantum safety initiative in the financial sector to include a broader conversation across all sectors.

2.9. INTEROPERABILITY CHALLENGES

The Roadmap does not sufficiently address the complexities of maintaining interoperability during migration, especially for cross-border services and interdependent cryptographic systems. Close coordination between these (cross-border) organisations is critical to avoid disruptions and ensure seamless transitions.

2.10. GREATER PARALLELISATION

The Roadmap's current structure implicitly relies on a staged or linear approach, which may unintentionally create bottlenecks, particularly where progress in one area depends on completion in another. Given the complexity and heterogeneity of cryptographic systems across the EU, we recommend introducing greater parallelisation into the Roadmap to accelerate progress and reduce systemic risk. Below are specific, actionable suggestions for increasing parallelism while maintaining coordination and alignment. Instead of recommending a rigid sequence of activities (e.g. inventory → risk assessment → pilot → deployment), we suggest structuring the Roadmap into modular, composable milestone packages. These modules can be initiated independently, where conditions allow, enabling Member States, sectors and operators to move forward without waiting for all preceding tasks to be complete.

For example:

- Inventory and cryptographic asset classification can proceed in parallel with protocol readiness evaluation.
- Vendor engagement and procurement planning can begin while regulatory alignment discussions are ongoing.

We propose decomposing the Roadmap into role-specific tracks, each with its own activities, deliverables and timelines. These tracks reflect the natural division of labour across the ecosystem and allow different stakeholders to proceed in parallel:

- **Policy and regulatory track**: focused on mandates, legal harmonisation and public sector funding instruments.

- **Standards and interoperability track**: focused on profiling, conformance criteria and integrating emerging international standards.
- **Vendor enablement track**: focused on incentivising the development, certification and benchmarking of PQC-capable products.
- **Operational deployment track**: focused on asset inventories, Cryptography Bill of Materials, the migration of public services and incident response updates.
- **Oversight and metrics track**: focused on measurement frameworks, audits and maturity models.

This structure enables each stakeholder group to work on relevant tasks independently of other groups' progress.

2.11. GUIDANCE ON COST ESTIMATIONS

The Roadmap does not mention or point towards methodologies for estimating the costs of PQC migration, including hardware replacements, software updates and potential downtime. Comprehensive cost frameworks are essential for organisations to allocate resources effectively and plan their budgets.

2.12. LEGISLATIVE FRAMEWORK

While the Roadmap speaks of relevant legislative framework on page 3, it's quite odd that the General Data Protection Regulation (GDPR) is omitted. This is a central piece of legislation in the digital environment, and it does contain provisions on state-of-the-art security measures and specific references to encryption. The GDPR is extensively referred to in EU cybersecurity legislation as these are interconnected domains, and mentioning the GDPR can certainly help to make the case for PQC adoption more compelling.

On the same note, where the document states the importance of involvement of the supervisory authorities of NIS2, CRA and of the Electronic Identification, Authentication and Trust Services Regulation (eIDAS), we believe data protection authorities should certainly also be part of this process. The same goes for DORA supervisory bodies.

Similarly, for more consistency and clarity, it would be sensible to mention eIDAS on page 3, along with other legal acts, since its supervisory bodies are indicated later as relevant stakeholders.

2.13. EDITORIAL COMMENTS

The definitions section is helpful and precise. However, it arrives quite late in the document (after technical and policy content has already used the various terms). Putting them earlier in the document or summarising key terms (e.g. 'hybrid', 'quantum safe') – perhaps in a boxed glossary in the Executive Summary – would help orient readers from the start.

The phased Roadmap (2026, 2030, 2035) is one of the strongest parts of the document. It balances urgency with realism. Including references to US and UK policies (such as NSA, NIST and NCSC) also helps ground the EU recommendations within a global context. It may help to visually summarise the timeline as a Gantt chart or infographic for clarity and engagement.

The technical sections are understandable, albeit long. The references to specific risk models (e.g. PQC Migration Handbook Fig. 2.7) are helpful but some of the cross-references assume a familiarity with risk management methodologies (like ISO 27001) that might not be shared by all technical readers. A one-paragraph lay explanation of how the risk score is calculated would be useful.

PART VIII. Transition to PQC in the Financial Sector

1. Introduction

This chapter explores the transition to PQC in the financial sector. It concludes that quantum computing jeopardises core systems like payments, messaging, and identity verification. Institutions are urged to begin inventorying cryptographic assets and deploying protections for long-lived sensitive data. There is sector-wide alignment on starting now despite timeline uncertainties.

Regulatory responses differ across the EU, the UK, and the US, but share a common direction. The EU's DORA mandates cryptographic agility and awareness of emerging threats. The UK supports sector-led action via cooperation forums and a longer timeline. The US has imposed deadlines for federal systems and supports industry transition. Each jurisdiction is working towards shared standards and implementation targets around 2028 to 2030.

Three bottlenecks slow PQC adoption: technical challenges, skills shortages, and vendor dependency. Legacy systems must be retrofitted; talent is lacking; suppliers are not yet fully PQC-ready. These factors increase costs and delay action. Without coordinated efforts, organisations risk incompatibility and fragmented standards.

- Legacy systems are not crypto agile by design.
- Crypto expertise is limited across financial IT teams (and within executives).
- Vendors and standards bodies lag behind sector needs.

2. Transition to PQC in the financial sector

The advent of CRQCs poses a systemic risk to financial systems by undermining the public-key cryptography that secures payments, interbank messages, and digital identities. If sufficiently powerful quantum computers emerge, they could break the RSA, ECC, and other algorithms currently protecting payment networks (i.e. the Society for Worldwide Interbank Financial Telecommunications (SWIFT) and authentication systems), potentially compromising the confidentiality and integrity of transactions. Given the **long-term sensitivity of financial information, data being transmitted or archived now could be exposed retroactively,** eroding trust in the financial sector's foundational security.

The financial system's heavy reliance on cryptography means a quantum break could have dire consequences. Payment systems and digital banking rely on encrypted channels (i.e. VPN tunnels, TLS) and digital signatures for transactions and identity verification. In practice, **fund transfers could be tampered with and identities impersonated if current cryptographic safeguards fail.** Recognising this, regulators and central bankers have sounded alarms. The European Central Bank (ECB) President Christine Lagarde has suggested the next financial crisis could be cyber-related. Crucially, the consensus is that **financial entities must act with urgency to migrate to post-quantum cryptography**. The ECB, the Bank for International Settlements (BIS) and the Dutch PQC Migration Handbook classify banks as 'urgent adopters' that should begin transitioning as soon as possible.

An important nuance is that quantum risk combines an **unknown deadline** (the eventual arrival of a CRQC, estimated by some experts to be between 2030 and 2035) with an **immediate threat** (harvest now, decrypt later). This unique challenge requires the financial sector to balance current cybersecurity with future-proofing efforts.

In summary, the transition to PQC in finance is driven by the need to preserve stability and trust. The quantum threat for the financial system is therefore existential: it threatens not only data confidentiality but the continuity of core financial functions. This recognition underpins global calls to begin the PQC transition now, despite uncertainty in the timeline of quantum computing advances. Financial institutions are urged to inventory their cryptographic assets and identify vulnerabilities (i.e. long-lived secrets, critical transaction links) and to start **deploying quantum-safe solutions in those areas first.**

3. The current regulatory landscape (EU, UK, US)

European Union: The EU has specific regulations concerning the financial sector, notably through the DORA and its implementing regulations. DORA, which applies to a broad range of financial entities, mandates rigorous ICT risk management, which encompasses cryptographic risks. Article 9 of DORA requires firms to monitor and control the security and functioning of ICT systems and to maintain high standards of data confidentiality and integrity. Crucially, a March 2024 Commission Delegated Regulation under DORA (EU 2024/1774) **requires financial entities to have an encryption and cryptographic controls policy** that remains current with technological advancements. This policy must include criteria for selecting cryptographic techniques based on established best practices and standards, as well as provisions for updating or modifying the cryptographic technology as necessary in response to advancements in cryptanalysis. Entities unable to immediately adhere to cutting-edge crypto standards must implement compensating controls to ensure resilience against cyber threats. Most institutional stakeholders on the type or method of cryptography used (BSI, ANSSI, Commission), emphasising the importance of cryptographic agility[19]. The position of the EU effectively makes **quantum readiness part of operational resilience compliance**. Financial supervisors can point to the **'state-of-the-art'** security principle (which is embedded in the GDPR, now echoed in DORA's requirements, and will be emphasised in the CRA) to hold firms accountable for keeping cryptography up to date. However, a gap remains between these regulatory expectations and industry awareness, and even where awareness exist, it may not be clear what 'state-of-the-art' requires in all circumstances.

While DORA provides a strong regulatory driver (and covers over 20 categories of financial entities), there is a recognised need for further guidance and perhaps supervisory pressure to spur concrete PQC migration plans. Some experts have called for additional EU-level papers or roadmaps to make the quantum-safe transition *'more explicit'* as a policy goal. Nonetheless, the EU's inclusion of cryptographic agility requirements in law is a pivotal step. It means that **EU financial regulators can enforce PQC migration as part of operational resilience**.

United Kingdom: The UK's approach to PQC transition has been proactive, but so far relies on guidance and industry collaboration rather than specific new legislation. The Financial Conduct Authority (FCA) considers quantum security under its broad mandate for cybersecurity and operational resilience, treating it as another emerging risk that firms must manage. There is no new legislation solely for PQC; instead, quantum risk falls under existing regulatory expectations for firms to withstand cyber incidents and cryptoanalysis attempts. In practice, UK regulators have been working closely with industry and international bodies to shape a coherent transition strategy. The FCA-World Economic Forum 2024 white paper, Quantum Security for the Financial Sector: Informing Global Regulatory Approaches, emphasises the need for global coordination. This collaboration highlights the UK's stance that addressing quantum threats necessitates close cooperation between industry and regulators, as well as a coordinated approach across jurisdictions.

A UK timeline for the rollout of PQC has been discussed in terms of alignment with national and international goals. The UK appears less ambitious for 2028 as a target for a quantum-safe plan development compared with the EU's 2026 milestone[20], though final objectives around 2030/31 are similar. The UK's Digital Regulation Cooperation Forum which unites the FCA with other regulators, provides a venue for coordinating

[19] As defined in the NIS group report on quantum cryptography, cryptographic agility refers to 'the design of cryptographic protocols and systems in a modular manner that enables the replacement of cryptographic components'.

[20] This milestone is given out by the NIS Cooperation Group on quantum cryptography, previously proposed by German BSI. It is not yet an official map carved in policy.

cryptographic standards across sectors. In essence, the UK is ensuring that financial regulators, national security agencies, and industry bodies collaborate effectively. The Bank of England, for example, participates in G7 working groups, and UK Finance has identified quantum risk in its agendas.

While the UK has not yet issued binding rules solely on PQC, the supervisory tone is clear: firms should treat quantum vulnerability as a component of cyber risk management and overcome cyber incidents, including those enabled by cryptanalysis. **Firms are expected to undertake 'no-regret' moves now (such as cryptographic audits, inventories, upgrades) rather than wait for regulatory compulsion.** Therefore, the UK regulatory landscape is characterised by early engagement, guidance, and international collaboration. We can anticipate more explicit UK guidance once standards mature, with specific advice for the financial sector expected to come 'earlier' in the UK than elsewhere. Still, UK regulators are already actively participating in global principle setting for PQC.

United States: In the US, the push for cryptographic agility and PQC adoption in the financial sector has been driven by **both federal government directives and industry initiatives**. NIST finalised its first PQC algorithms (FIPS 203, 204, 205) in August 2024, which are now the basis for future cryptographic standards. Alongside this, NIST's NCCoE has issued Special Publication 1800-38B, which provides practical migration guidance for financial institutions, including cryptographic inventory methods and sector-specific use cases. This initiative directly involves financial actors and offers banks and market infrastructures an operational blueprint for crypto agility. At the federal level, the Quantum Computing Cybersecurity Preparedness Act of 2022 requires agencies to adopt NIST standards once they become available and compels agencies procuring ICT systems to prepare for a post-quantum transition. Further reinforcement comes from Executive Orders 14144 and 14306, which establish deadlines for the deployment of PQC-capable products across government systems. While primarily directed at the public sector, these requirements also impact the financial industry through vendor dependencies and critical infrastructure links. Financial regulators, such as the Office of the Comptroller of the Currency (p21) and the Federal Reserve, have already referenced quantum risk within their operational resilience frameworks. The Treasury, through its Financial Sector Cybersecurity Framework, has integrated quantum threats into its guidance, while the Federal Financial Institutions Examination Council has begun incorporating quantum resilience considerations into its supervisory material.

From the industry side, organisations such as the **Financial Services Information Sharing and Analysis Centre (FS-ISAC)** have taken a leading role. In October 2024, FS-ISAC's PQC Working Group released *Building Cryptographic Agility in the Financial Sector*, a comprehensive blueprint for firms to achieve crypto agility in a coordinated manner. US financial regulators have echoed this collaborative and agile approach. The Federal

Financial Institutions Examination Council (FFIEC) has added quantum risk considerations into its handbooks, and the Treasury's Financial Sector Cybersecurity Framework emphasises **cryptographic inventory and upgrade plans**. Additionally, legislation is in progress (i.e. portions of the Quantum Computing Cybersecurity Preparedness Act) to ensure that public-private coordination on quantum-proofing critical financial infrastructure continues. These initiatives align with the US National Cybersecurity Strategy of March 2023, which makes PQC a priority for both government and critical private infrastructures.

Overall, the US regulatory landscape combines top-down requirements (for federal agencies and, indirectly, their contractors, including some financial market utilities) with bottom-up industry frameworks. This results in the emergence of preparatory steps, such as **mandatory cryptographic inventories, risk assessments, and the development of migration playbooks**. Financial sector regulators, such as the Securities and Exchange Commission and the banking agencies through the FFIEC, haven't yet issued PQC-specific rules but are likely to rely on existing safety and soundness mandates. They expect banks to follow NIST standards and FS-ISAC best practices as they become available. In short, **US authorities are aligning policy with practice** by updating guidelines and fostering an ecosystem for post-quantum cryptography.

4. TRANSITION MODELS TO QUANTUM-SAFE CRYPTOGRAPHY IN THE FINANCIAL SECTOR

Transitioning to post-quantum cryptography will be a **complex, multi-year journey**. Key strategies for managing this transition include developing cryptographic agility, conducting thorough risk assessments to prioritise actions, and learning from early initiatives in the financial sector (pilot projects and experiments) to inform broader rollouts.

Rather than a one-off swap of algorithms, experts advocate for a **crypto-agile approach**: one that builds the capacity to change cryptographic algorithms and protocols **rapidly with minimal disruption**. This thereby avoids the security vulnerabilities of outdated algorithms. For example, applications should support cryptography where algorithms can be changed via configuration rather than code overhaul, and protocols should be negotiated to use the strongest standard algorithm available between parties. Agility also implies maintaining interoperability during the migration, which is deemed a necessity. A BIS Project Leap report notes that a hybrid approach (using classical and quantum-safe algorithms together) is essential 'to maintain interoperability during the migration phase', ensuring communications remain secure even if one side hasn't fully upgraded.

To implement cryptographic agility, organisations are advised to take several practical steps. **Governance structures** are vital: firms should establish a PQC transition steering committee or task force. This group oversees inventorying cryptographic usage, tracking standards, and setting migration timelines in alignment with business priorities and regulatory requirements. Many large banks have already formed internal 'quantum risk' or 'crypto-agility' teams for this purpose. Next, firms need to **upgrade their underlying infrastructure** to ensure that HSMs, cryptographic libraries, VPN appliances, and other related components can support newer algorithms. A key recommendation is to modernise algorithms as part of a broader modernisation initiative. For example, if a bank is migrating services to the cloud or replacing core banking systems, crypto-agility considerations should be built in from the start. Alongside this, staff require training with workshops for IT and security teams on the basics of quantum computing and cryptographic concepts. This upskilling ensures that the workforce can effectively implement and maintain new cryptographic solutions. Finally, **collaboration with vendors and partners** is crucial. Firms should engage vendors early to ensure their roadmaps include PQC support, effectively asking for **crypto agility by design** in new procurements.

Given the scale of the transition, not everything can be changed at once. **A risk-based approach** is essential to prioritise which systems and data to secure first. This process begins with a **cryptographic inventory**. Financial institutions should catalogue all cryptographic assets, including algorithms, key lengths, certificates, and their usage locations and methods. The inventory must also identify which assets have long-lived confidentiality requirements (for example, data that needs to remain secret for 10 years or more). Indeed, those are at higher risk from **harvest now, decrypt later attacks**. Using this inventory, firms can then **estimate the quantum vulnerability** of each asset. One approach presented in the Task Force is to calculate the probability that a given asset's encryption will be broken within a particular time frame, based on projections of quantum computing progress. To determine this timeline, applying **Mosca's theorem** can be helpful[21].

Crucially, risk assessment must consider **both cryptographic strength and business impact**. Not all systems carry equal risk; one must prioritise the critical systems that need PQC first. High-impact assets, such as payment clearing systems or PKI that underpin interbank authentication, with long security lifespans, should be migrated early. Additionally, some data or processes might be less sensitive or have short-term confidentiality needs and could be migrated later. Several frameworks have emerged to

[21] Mosca's approach considers the remaining lifetime of sensitive data, the time expected for quantum computers to break current encryption, and the time needed to transition to PQC. If the sum of the data's required secrecy duration and migration time exceeds the estimated quantum 'break' date, immediate action is warranted.

guide this process. The Dutch PQC Migration Handbook and research by the Netherlands Organisation for Applied Scientific Research have introduced structured risk models combining *quantum weakness scoring* of algorithms, *impact levels* of different data, and the *effort required* for migration. Similarly, the ECB has developed a *'five-domain'* risk and readiness framework: (1) **Knowledge** (threat awareness, technical expertise); (2) **Planning** (effort estimation and roadmap); (3) **Discovery** (cryptography use-case inventory, data at risk); (4) **Third parties** (vendor and legal considerations); and (5) **Risk management** (updating risk registers and prioritising mitigations). Each domain has maturity levels to assess an institution's progress. Using such models, a firm can identify its current position and pinpoint the gaps it needs to address. For instance, if a bank finds that its *'discovery'* domain is weak (no comprehensive crypto inventory yet), that becomes a near-term action item.

Another aspect of risk management is performing a **cost-benefit analysis** of mitigation options. Not all solutions are equal: some may involve hardware changes (using hybrid solutions in hardware or deploying QRNGs or QKD links), while others are purely software-based (switching to PQC algorithms).

It is reported that a complete crypto transition for a large bank could cost in the order of hundreds of millions of dollars. The importance of quantified risk assessments for boards and executives is essential to justify expenditures against the risk reduction achieved. **If the cost of inaction (i.e. potential fines, losses, and reputational damage from a future breach) outweighs the migration cost, the business case for PQC investment becomes clear.** Regulators, too, are interested in these analyses. The World Economic Forum (WEF)-FCA roadmap encourages regulators to 'conduct a cost-benefit analysis of different approaches to quantum risks (…) to take decisions accordingly'.

Risk-driven prioritisation means identifying which cryptographic exposures to tackle first, devising a timeline (often multi-phase) for upgrades, and ensuring resources are allocated efficiently. This approach enables a phased transition, allowing for quick wins (i.e. swapping algorithms in software that supports new standards) to be achieved early. In contrast, more complex changes (i.e. replacing or refactoring legacy systems that cannot handle new key sizes) are planned with sufficient lead time.

Overall, the financial sector should focus on a risk-driven prioritisation of cryptographic material as part of a broader strategy meant to upgrade IT processes. The cost of a transition can be very expensive; therefore, including C-suite level executives in the transition is essential, showcasing the cost of inaction **(i.e. potential fines, losses, and reputational damage from a future breach)**, with specific teams or a task force in charge of the transition.

5. INITIATIVES IN THE FINANCIAL SECTOR

The abstract nature of the PQC transition is being made concrete by several pioneering projects and collaborations. These **case studies provide insight** into how to transition in practice and the status of progress:

- *Central bank experiments:* Several central banks have run quantum-safe pilots. **Project Leap**, led by the BIS Innovation Hub with Banque de France and Deutsche Bundesbank, demonstrated a quantum-safe VPN for interbank connections. In 2023, Project Leap's first phase established a site-to-site IPsec tunnel secured with hybrid cryptography (traditional RSA combined with NIST PQC algorithms) to carry ISO 20022 payment messages between Paris and Frankfurt. The project evaluated cryptographic agility (the ability to swap algorithms in the VPN), performance impacts, and integration challenges. This project demonstrated that migrating to new protocols necessitates changing the entire set of cryptographic protocols well in advance. It also highlighted operational issues, such as staffing, noting that specialists in quantum-safe crypto are scarce. The BIS had to specially train a team, stating the lack of workforce with the specific skills in this area. Phase 2 of the project is now planned to explore more network architectures and to incorporate additional layers of the payments value chain. In parallel, central banks in Israel, Canada, and others have held workshops and provided recommendations. Banca d' Italia, under the 2024 G7 presidency, hosted a conference ***'Building a quantum-safe financial system: what role for authorities and private sector?'***. One output was a G7 statement calling for early planning and a common roadmap for quantum resilience across countries. This top-down encouragement is prompting each central bank to develop its own transition plan for critical systems, such as real-time gross settlement payment networks (i.e. the ECB's TARGET services). In fact, the ECB has already formed a dedicated task force (with itself and major national central banks) to devise an 'internal transition roadmap' for Eurosystem infrastructures.

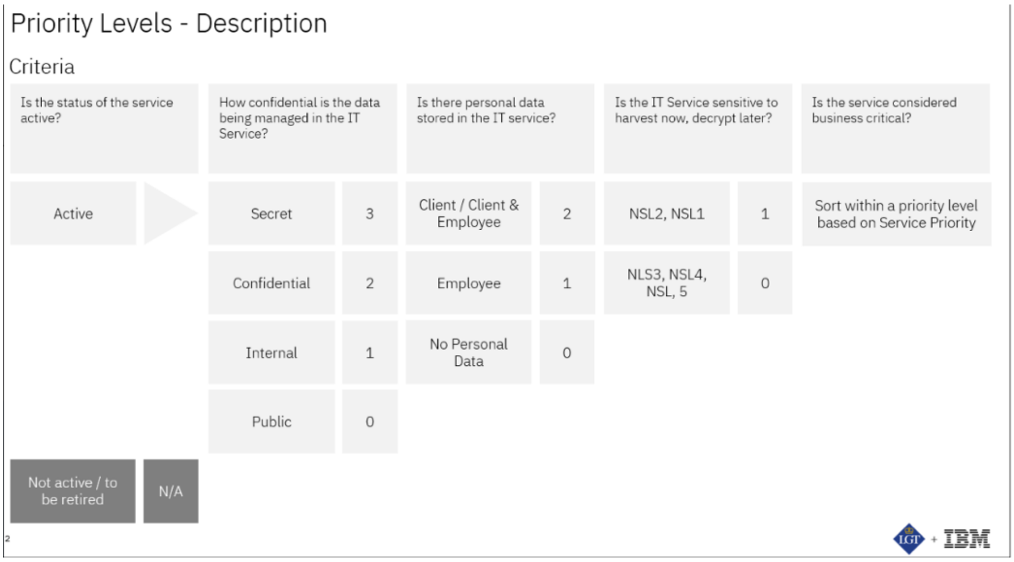
- *Commercial banks and pilot networks:* In the private sector, banks such as Santander and LGT have been early movers. Santander has a dedicated quantum security team and has participated in industry pilots blending PQC with QKD. In 2023, Santander conducted a test with MadridQCI of a hybrid PQC-QKD network for secure communications. In this setup, a software-defined network (SD-WAN) delivered keys to IPsec routers, where classical pre-shared keys were combined with QKD-delivered keys (per the ETSI TS 103 744 standard) to establish VPN tunnels. The test confirmed that such a hybrid IPsec is feasible even with multi-vendor QKD sources (Cisco, QoolNet, ID Quantique devices, Luxquanta). The

conclusions from Santander's pilot were encouraging: a software-defined networking based key management approach can support early quantum-safety in IPsec networks at scale and enable interoperability among different key exchange mechanisms. This is a practical demonstration of crypto agility and hybrid cryptography in action, suggesting that even before full PQC standards are finalised, networks can be made quantum safe (i.e. dual algorithms or additional QKD layers).

Similarly, **LGT Private Bank** (Liechtenstein) was reported to be experimenting with quantum-safe communications, for example, by using QKD links between its data centres, although details are sparse. The fact that private banking and wealth management firms are exploring such technologies suggests that concerns about client confidentiality are driving the early adoption of these technologies. One prominent element of their approach to quantum cryptography was the elaboration of a hierarchical prioritisation of materials, through questionnaires (this way of proceeding was elaborated with IBM, see Figure 4).

- *Industry consortia and forums:* Collaborative initiatives are helping guide the transition. FS-ISAC's Post-Quantum Working Group produces guidance and fosters information sharing among banks globally. Another is the **Quantum Safe Financial Forum**, which operates under the supervision of Europol. Led in part by industry, this forum is pushing for cross-sector threat intel sharing and joint pressure on vendors. It recognises that vendors of core banking software, automated teller machine (ATM) hardware, cloud services, and other related products need precise requirements from the financial industry to prioritise PQC in their product roadmaps. On the standards front, organisations such as **ETSI** and **ISO** have been active. A consortium of nine organisations, including startups, academics, and the banking industry, has developed quantum communication two-point networks between two data centres of Denmark's Danske Bank under the CryptQ project. The Technical University of Denmark used continuous variable quantum distribution (CV-QKD), with the financing and technological help of consultancy firm KPMG, to create and share secure encryption keys on standardised telecom fibre optics. This showcases how this technology can be implemented in other critical infrastructure. The project was built on the basis of Horizon 2020 initiatives, funded under the OPENQKD call for tender (EU funding), and the Danish project CryptQ, with investments of the Innovation Fund Denmark of 22.5 million Danish Krone.

Figure 4. LGT's cryptographic priority levels



Priority Levels - Description

Criteria

Is the status of the service active?		How confidential is the data being managed in the IT Service?		Is there personal data stored in the IT service?		Is the IT Service sensitive to harvest now, decrypt later?		Is the service considered business critical?
Active		Secret	3	Client / Client & Employee	2	NSL2, NSL1	1	Sort within a priority level based on Service Priority
		Confidential	2	Employee	1	NLS3, NSL4, NSL, 5	0	
		Internal	1	No Personal Data	0			
		Public	0					
Not active / to be retired	N/A							

2

Source: Slides from ETSI conferences, 2025.

These initiatives suggest that many financial organisations are at a proof-of-concept or early implementation stage of the PQC transition. There are no widely deployed production quantum-safe interbank networks yet, but the building blocks (PQC algorithms, hybrid protocols, vendor support in hardware) are quickly materialising. Regulators are monitoring these pilots closely. For instance, the Monetary Authority of Singapore issued an advisory in 2024 addressing the cybersecurity risks of quantum. Along with the Bank of England and others, it participates in international quantum risk discussions, ensuring lessons from one project (like Project Leap or Santander's test) inform the broader global approach. Therefore, the 'how' of transition is being refined through these ongoing initiatives: blending PQC algorithms into existing protocols, using hybrid classical-quantum approaches to mitigate risk during a long migration, but also developing next generation approaches (e.g. Santander's PQC and QKD networks) and coordinating via forums so that, eventually, the whole financial sector can move in step when the time comes to flip the switch to quantum-safe encryption.

6. BOTTLENECKS IN THE FINANCIAL SECTOR'S PQC TRANSITION

Despite growing momentum, **significant obstacles are delaying the financial sector's transition to PQC**. These bottlenecks are technical, organisational, and infrastructural and must be addressed to accelerate progress.

- **Technical challenges:** A major technical hurdle is integrating new cryptographic algorithms into legacy systems. Financial IT environments are rife with legacy protocols and hard-coded cryptography. For example, many VPNs or secure messaging systems assume RSA or ECC for key exchange; upgrading them to lattice-based KEMs may require new protocol extensions, message formats, and error-handling logic. Ensuring interoperability between upgraded and non-upgraded entities further complicates matters. Performance is another concern: PQC algorithms generally have larger key sizes or signature sizes, and some (like lattice-based schemes) have slower operations. In high-throughput trading systems or low-latency payment switches, these performance hits need careful benchmarking. Initial tests show, for instance, that PQC handshakes can add a few seconds to the delay in session setup, which can be tolerable for some uses, but potentially problematic for others. **Tuning systems for PQC performance and stability** is non-trivial. There's also the matter of algorithm uncertainty: while NIST has selected initial standards (i.e. CRYSTALS-Kyber, Dilithium), additional algorithms (for signatures and specific use cases, such as FIPS 140-3 compliance) are still being evaluated. Some firms are hesitant to deploy one set of algorithms before the standards are fully finalised (including stateful hash signatures or future round algorithms), lest they guess wrong. **As the Bank of Italy's report noted, the absence of universal agreement on standards and a roadmap makes it challenging to design migration plans.** This fragmentation risk means that technical teams must possibly implement more than one PQC option or be prepared to pivot if an algorithm is later found to be weak (as happened with some NIST Round-3 candidates). All these issues heighten the complexity and cost of the transition.

- **Organisational and skills gaps:** Financial institutions face a **shortage of cryptographic skills and awareness** at all levels. Cryptography has often been a niche domain in IT; now it must become a mainstream concern. The culture in many financial organisations has been to treat cryptography as a static utility. Changing this mindset to one of continuous cryptographic improvement is an organisational challenge. This indicates an **awareness gap**, where boards and executives may not yet prioritise quantum risk amidst more immediate concerns. **Without executives' awareness, the budget and resources for PQC projects are limited.** On the other hand, as awareness grows, a new challenge arises: the overestimation or misallocation of effort. If too many uncoordinated initiatives start (each business line doing its own thing), it could lead to duplication or inconsistent approaches. The need for a unified strategy within firms is paramount (hence calls for internal governance such as steering committees). The **crypto-inventory process** itself can be an organisational hassle, as it may require cooperation across departments and outside of the organisation (i.e. software and hardware providers, see further below). Discovering all uses of cryptography in a large bank is akin to an audit that can take many months. **Many banks have tens of thousands of applications; scanning these for cryptographic dependencies is an immense coordination effort.** Limited skilled manpower, competing priorities, and the need for cross-functional collaboration are slowing the transition on the human side.

- **Infrastructure and vendor dependencies:** The financial sector's crypto infrastructure extends beyond the walls of any single institution. It includes vendors, third-party service providers, and hardware manufacturers. A key bottleneck is the **readiness of technology providers** to support PQC. Financial firms report that they cannot upgrade certain systems until vendors (of core banking software, HSM devices, network gear, cloud platforms, etc.) offer compatible, certified solutions. Suppose the IT sector is not on the same timeline as the financial sector. In that case, it might put the industry at risk of having to choose between potentially unreliable technology and delaying the transition. This is why there is pressure on vendors: US agencies, for instance, have set **expectations on IT vendors** to incorporate PQC, effectively nudging the whole market forward. But not all vendors have moved at the same speed. Smaller vendors or niche software providers may lack the resources or incentive until customers demand it. There's also the issue of certification and compliance. Banks require FIPS-certified cryptography or Europay, Mastercard, and Visa (EMV) standards for cards; these standards bodies are still updating their specs for PQC, which in turn delays vendor implementations. Another infrastructural bottleneck is **device limitations**. Some HSMs or smart card chips in use have fixed algorithm support (like RSA/ECC only) and limited processing power or memory for larger PQC keys. Replacing or upgrading these secure elements (which number in the millions across ATM networks, payment cards, mobile secure elements, etc.) is a massive logistical exercise. In payment systems, even such protocols as EMV or ISO 8583 would need revisions to accommodate PQC, which involves global coordination. Until standards and infrastructure catch up, **many institutions are reluctant to move first, fearing incompatibility. This is why regulatory fragmentation across different markets is a significant concern (risk of misalignments across jurisdictions)**.

Harmonising standards (which is ongoing in organisations like ISO and the G7) is slow but necessary work to remove this bottleneck.

- **Cost and complexity of migration:** Underlying all the above is the sheer cost and complexity, which can be bottlenecks in themselves. The **transition is costly**, not only in monetary terms but also in terms of operational impact. If not mandated or clearly revenue-linked, such spending is hard to justify internally until the risk is imminent. Moreover, unlike some IT projects, a cryptography migration has no immediate business upside (customers won't see new features; it's about reducing downside risk), so it often gets deferred. Complexity also makes planning difficult: institutions must consider backward compatibility, data that are currently encrypted (how to re-encrypt archives?), and coordination with counterparties. For example, two banks that regularly exchange signed messages will have to switch to new signature algorithms in a synchronised fashion. Indeed, the sector has undergone prior cryptographic transitions (i.e. Triple Data Encryption Standard (3DES) to AES, SHA-1 to SHA-256, RSA-1024 to RSA-2048), and each time it has been *more complex and time-consuming than the last. It is an endless cycle and becoming unsustainable*, which is why a different approach (agility) is now needed. But achieving that agility itself is complex: it requires significant re-engineering. Gartner's '5 R's' (Rehost, Refactor, Revise, Rebuild, Replace) are often cited as strategies to deal with legacy applications that can't easily handle new crypto. Choosing and executing these strategies on a case-by-case basis (should an old payment platform be replaced entirely, or can it be refactored to use a crypto-agile API?) is a detailed undertaking, creating analysis paralysis in some organisations.

PART IX: Transition to Quantum Safe in the Public Sector

1. Introduction

This chapter examines **the transition to PQC of PKIs and digital identity systems in the public sector**. PKIs form the backbone of digital trust, enabling secure authentication and communication across government services. The advent of quantum computing, however, threatens the classical cryptographic algorithms on which these systems rely, requiring a coordinated shift to quantum-resistant alternatives.

Different bottlenecks define the public sector's PQC migration: technical complexity in upgrading vast authentication systems, organisational adaptation across interdependent actors, and institutional fragmentation in standardisation and governance. The transition of this specific sector is far from being merely technical. While algorithmic choices, hash-based, lattice-based, or hybrid, present their own trade-offs, the broader challenge lies in adapting the entire trust ecosystem, from certificate authorities to revocation systems to hardware modules. The case of the EU Digital Identity Wallet illustrates both the potential and the risk; without PQC integration from the outset, Europe risks locking itself into obsolete cryptography.

In this context, this Task Force highlights several priorities for action:

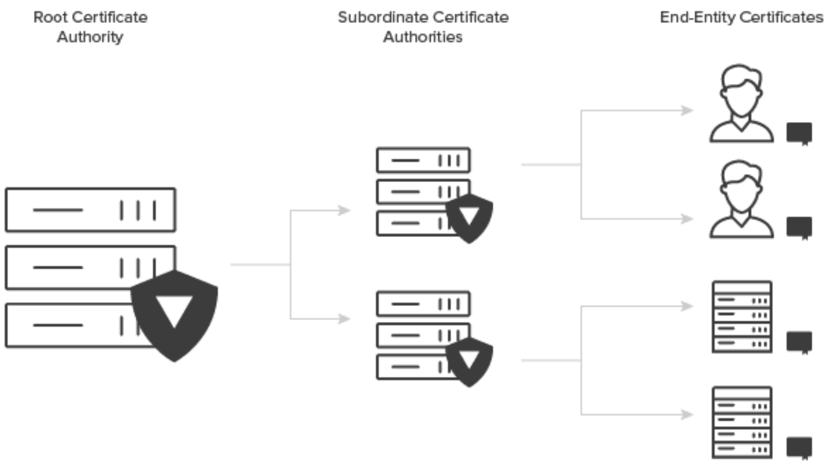
- implement sequenced migration plans for PKI and digital identity systems
- synchronise authentication layers to prevent fragmentation and service disruption
- coordinate cross-border roadmaps and align national migration strategies
- integrate quantum safety into digital identity from the start
- manage the quantum transition as a coordinated sociotechnical programme.

2. Transition to PQC in the Public Sector

PKIs are the backbone of digital trust in modern administrations. PKI is a governance and technical framework that issues and manages digital certificates so people, organisations, services, and devices can prove who they are online. They provide the framework through which public and private keys are issued, managed, and validated, ensuring that digital communications, services, and identities can be authenticated and verified.

PKIs are typically hierarchical (Figure 5); a small number of protected 'root' authorities act as trust anchors. Those roots authorise 'intermediate' authorities to operate on their behalf in specific domains (e.g. a ministry, a department, or a sector). Those intermediates (typically) then issue the actual certificates to the 'end entities': people, servers, apps, or devices. PKIs, therefore, rely on a chain of trust: a root certificate authority serves as the trust anchor, intermediate authorities distribute trust across specific domains or sectors, and end-entity certificates are issued to users, organisations, or devices. This layered architecture underpins essential services such as secure email, authentication for government systems, and digital signatures used in administrative procedures.

Figure 5. PKI Infrastructure


Root Certificate Authority
Subordinate Certificate Authorities
End-Entity Certificates

Source: https://www.keyfactor.com/education-center/what-is-pki/.

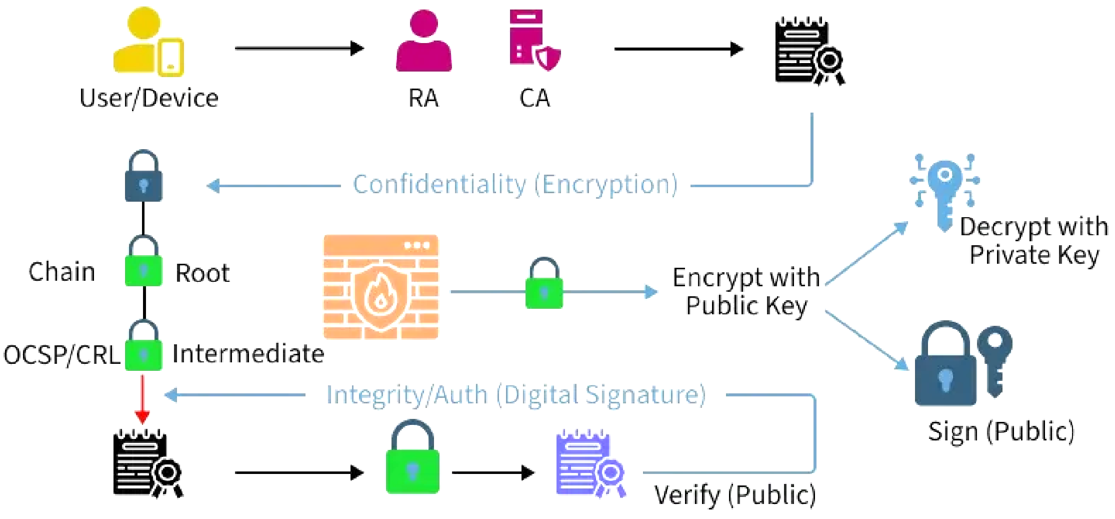
Certificates underpin secure communication between parties by ensuring that information is exchanged with the right counterpart and remains protected from interception or tampering. Certificates have defined lifecycles, often 10 years for root authorities, several years for intermediates, and a shorter period for end entities, requiring constant renewal, revocation, and oversight to maintain security and reliability.

However, the advent of quantum computing **challenges the very foundations of this trust model.** Current PKIs rely on classical public-key algorithms, such as RSA or elliptic-curve cryptography, to secure communications and guarantee authenticity through digital signatures. Once large-scale quantum computers become viable, these algorithms could be efficiently broken, undermining both encryption and authentication mechanisms.

In response, **efforts to transition to PQC are already underway, though progress varies across the different layers of Internet security**. The confidentiality layer, which protects the secrecy of communications through ephemeral, unauthenticated key exchanges, has advanced the fastest. Between 2014 and 2016, major actors such as Google, Mozilla, Cloudflare, Fastly, and Akamai piloted and have now deployed hybrid post-quantum key exchanges in TLS, enabling classical and quantum-resistant algorithms to operate in parallel. This evolution has been largely driven by the harvest now, decrypt later threat, and empirical evidence suggests that for most users, performance impacts remain minimal, aside from some latency in older devices and middleboxes.

By contrast, **the authentication function** (Figure 6)**,** which ensures endpoints are genuine and certificates are valid, remains a major bottleneck. This asymmetry reflects the relative simplicity of upgrading (ephemeral and unauthenticated) key exchange between two parties compared with migrating the entire multi-actor PKI trust fabric. Here, the transition to PQC affects the entire certificate hierarchy and lifecycle management.

Figure 6. Confidentiality and authentication on PKI



Source: https://www.geeksforgeeks.org/computer-networks/public-key-infrastructure/.

This complexity has made the selection of suitable post-quantum algorithms particularly consequential for PKI design and deployment. Each candidate family presents a different balance between performance, operational complexity, and security assurance. The main options currently under evaluation illustrate these contrasts.

- **SLH-DSA (stateless hash-based signatures)**: these are built on well-understood security properties, making them among the most conservative and robust choices. The drawback is their very large signature sizes, which inflate certificates and chains, straining bandwidth and storage.

- **eXtended Merkle Signature Scheme (XMSS) and Leighton-Micali Signature (LMS) (stateful hash-based signatures)**: also based on well-established security assumptions, these can produce very small signatures and public keys, which is attractive for certificate size. However, they require state management. This makes operational procedures, backups, and recovery more complex.

- **ML-DSA + ECDSA (hybrid)**: pairing a lattice-based signature with a classical scheme offers a 'safety net': as long as one component remains secure, trust is preserved. The hybrid also keeps signature and public-key sizes moderate, since the ECDH portion adds little overhead. Yet adoption/support across the ecosystem is still uncertain.
- **ML-DSA (pure)**: a lattice-only option avoids the complexity of managing two algorithms and is likely to enjoy wide adoption across software and hardware platforms. Sizes for signatures and keys are moderate, making it practical for many deployments. Still, reliance on structured lattice assumptions remains an open question in terms of long-term confidence. The IETF has published RFC 9881, which specifies algorithm identifiers for ML-DSA in the context of the X.509 PKI. This development marks an important step towards ecosystem-readiness of the pure ML-DSA variant, as it formalises how ML-DSA-44/ML-DSA-65/ML-DSA-87 parameter sets map into certificate structures. Nonetheless, that does not automatically resolve all questions about deployment maturity, vendor support or long-term confidence in structured-lattice assumptions.

Overall, European authorities and national agencies, such as BSI, are **actively promoting hybrid certificates**. Hash-based signatures, such as stateful LMS/XMSS, have been proposed as candidates for trust anchors because of their conservative security basis and compact size. These recommendations are being fed into European Commission channels as part of broader policy guidance. At the same time, concerns emerge about the **fragility of stateful schemes such as XMSS and LMS**. Because each key can only be used once, operational errors in state or backup management could lead to catastrophic failures. While national authorities expressed confidence in managing such schemes at the root level, they recognised the risks of mandating them for intermediates, where mistakes are more likely.

The transition, however, affects the **entire trust ecosystem**. This includes the mechanisms used to validate certificates, the procedures for introducing new trust anchors, the business processes of certificate authorities, and the supporting infrastructure, such as hardware security modules and certificate-management systems. This is, therefore, a systemic exercise that requires coordination across root and intermediate certificate authorities, certificate transparency log operators, revocation and Online Certificate Status Protocol (OCSP) responders, HSM vendors, certificate lifecycle management systems, and application-level verifiers. Each of these **actors must adapt simultaneously for a consistent chain of trust to function.**

Standards such as the International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T) X.509 now enable the use of PKI software that is capable of handling post-quantum certificates. However, this shift has so far translated into sector-specific procurement expectations rather than formal, binding mandates. Post-quantum cryptography is also being **built into widely used software libraries** (e.g. Botan, BouncyCastle, OpenSSL). Interoperability is tested at international events, such as IETF hackathons, where experimental PQ certificates are exchanged between systems.

Notably, the PQC transition is also **an opportunity to redesign potential structural weaknesses of PKI**. Intermediate certificates, already heavily cached by browsers, could be streamlined or removed to reduce chain length and overhead. Privacy shortcomings in certificate status checking, such as leaking user browsing patterns to third-party CT or revocation services, could be addressed by integrating privacy-preserving cryptography, leveraging recent production-ready advances in private information retrieval (PIR), private set intersection (PSI), and oblivious RAM (ORAM). These primitives, many of them lattice-based and thus PQC-compatible, allow verification without exposing user behaviour. By embedding such enhancements into the migration, PKI could **emerge more resilient, efficient, and user-protective than its current form**.

The implications of this transition extend beyond secure communications to the very systems that rely on PKI for identity assurance. Digital identity infrastructures inherit PKI's trust architecture to authenticate users, validate credentials, and enable cross-border interoperability. **Digital identity systems in Europe are, thus, built on a PKI-based trust framework**, where credentials are issued and validated through certificate chains that prove 'who issued what to whom'. These credentials range from simple identity assertions (e.g. 'holder is John Doe') to more complex, attribute-based claims (e.g. 'holder is over 18' or 'resident of Member State X').

Three properties drive digital identity systems design choices: **interoperability** (credentials must verify across heterogeneous systems and sectors), **trustworthy** issuance, both cryptographic soundness and correct binding to the right person/organisation, and **cross-border usability**. Cross-border use requires shared APIs, harmonised certificate profiles, and mutual recognition of trust anchors; otherwise, one country's weak or incompatible scheme undermines confidence in credentials issued elsewhere. Coordinated timelines and mutually recognised post-quantum roots are therefore a precondition for cross-border identity. More advanced identity applications, such as age or eligibility proofs, also introduce privacy requirements. Users should reveal only the necessary information, which calls for privacy-preserving cryptographic tools like selective disclosure, unlinkability, and zero-knowledge proofs. **These techniques exist in PQC forms but are not yet as mature or efficient as classical solutions.**

In digital identity systems, quantum risks differ by cryptographic function. For encryption, the harvest-now, decrypt-later threat means that any stored encrypted data could be compromised once quantum computers become viable, making post-quantum protections urgent. **For digital signatures**, the risk lies in future forgeries that could allow counterfeit credentials, meaning **migration could and should still occur on time.**

Box 3. The EU digital wallet case

Under the revised eIDAS framework, every Member State must make available at least one European **Digital Identity Wallet** and have it certified and notified by the end of 2026. Wallets must be open-source, implement the common architectural reference and profiles published by the Commission, and pass assessment by an accredited conformity assessment body before being recognised. The Commission maintains trust lists for issuers and a registration process for relying parties, so citizens can verify both 'who issued' and 'who is requesting' data across borders. **The wallet is a general purpose container for verifiable credentials** (personal identification data, mobile driving licence, education records, disability cards, social security entitlements, digital travel credentials, etc.). Benefits cluster around simplification, standardisation of common data and protocol profiles, and cross-compatibility. Several Member States (e.g. Italy, Portugal, Poland, France, Austria, and Germany) are advancing national apps towards wallet compliance, pending certification and full alignment with EU profiles. Demonstrated use cases include strong customer authentication for payments, venue/airport check-in, hotel onboarding, and proximity ID checks.

The **provisions for the Digital Identity Wallet** mandate that personal identification data and keys must be protected (through assurance levels, HSMs, or secure elements), but, importantly, **do not mandate post-quantum cryptography**. In practice, this means current deployments will still rely on classical algorithms. At the same time, the hardware and assurance frameworks provide the infrastructure to host PQ or hybrid schemes once standards and certifications mature. Against this backdrop, the risk is that a wallet rolled out without PQC capabilities will remain in operation well into the 2030s, **effectively locking Europe into outdated cryptography due to ecosystem inertia and the high cost of retrofitting**.

For this reason, there is a **strong case to embed PQC considerations at the design stage rather than treating them as a future 'swap'**. In other terms, a European digital identity wallet should embed PQ algorithms. A forward-looking approach would require crypto-agile interfaces (to allow smooth algorithm and profile updates), PQ-capable secure elements and HSMs, and footprint-aware cryptographic choices so that verification remains performant on end-user devices. As the revised **eIDAS framework** provides the legal scaffolding for European digital identity and wallets, its **emphasis on unlinkability and cross-**

border trust could be directly mapped to post-quantum requirements: preserving unlinkability against future quantum adversaries argues for PQ-by-design today.

In this context, Europe should define **common PQ defaults for identity** (e.g. a lattice KEM/signature pair for transport and credential signing, with hash-based options for trust anchors), **publish shared API and profile specifications, and coordinate procurement and conformity testing**. Clear guidance from EU bodies (e.g. algorithm suites and profiles for citizen-facing services, combined where possible to reduce implementation complexity) will minimise fragmentation and reduce implementation risk. More **specific and immediate actions include**: design the wallet and credential formats to be PQ-native and crypto agile; adopt hybrids; select an algorithm suite that covers both KEM and signatures while reserving hash-based signatures for long-lived trust anchors; **run EU-level pilots to measure performance on real devices and networks**; and publish prescriptive guidance to align Member States on profiles, APIs, and assurance. Without these steps now, the ecosystem's inertia risks missing the 2030 high-risk migration horizon.

3. TECHNICAL BOTTLENECKS IN THE PUBLIC SECTOR'S PQC TRANSITION

This section summarises the main technical bottlenecks currently facing the public sector's migration to PQC. The most immediate challenge in the public sector transition to PQC lies in the migration of existing infrastructures. The main risk is the structural difficulty of migrating complex authentication systems in time, given the **scale and intricacy of existing PKIs**. For public administrations, this risk is particularly acute: hundreds of thousands of certificates and multiple layers of certificate authorities must be updated.

Besides this, while confidentiality layers have advanced, the **authentication layer is a critical bottleneck**. Authentication depends on an **entire trust fabric of roots, intermediates, and end entities**. If certificate authorities issue PQ-capable chains but browsers lack PQC verification, interoperability collapses. Besides, CT logs must handle larger certificates, while revocation systems need to manage higher computational and bandwidth loads.

Another important technical bottleneck, as mentioned, is that **PQ algorithms also introduce significant performance trade-offs**: larger key and signature sizes increase message lengths, verification time, and storage requirements. Notably, although these effects are minor for end-users, they accumulate across large-scale identity systems, especially where millions of credentials and transactions are processed daily.

Box 4. The TLS 1.3 case

TLS 1.3, the latest version of the TLS standard published by the IETF in 2018, ensures the privacy and integrity of Internet communications. It also **illustrates the depth of the authentication challenge in the post-quantum era**. While key exchange can be upgraded through a single hybrid handshake, authentication depends on multiple signatures and certificate validations per session, including those of the handshake itself, each certificate in the chain, and certificate transparency logs. In practice, a single TLS connection may involve half a dozen signature verifications.

Post-quantum algorithms significantly increase signature and key sizes, which can cause packet fragmentation, retransmissions, and degraded performance, particularly for constrained devices or weak network links. Empirical studies have confirmed such effects, though comprehensive measurements across the full certificate chain remain limited.

Although most Internet authentication relies on PKI-issued digital certificates, **other approaches exist**. Some protocols use PSKs or password-based authentication, while an emerging proposal, KEM-TLS, employs KEMs for both encryption and authentication, reducing the need for large post-quantum signatures and improving efficiency. Yet large-scale adoption of these alternatives would require redesigning core Internet infrastructure and ensuring interoperability across browsers, servers, and certificate authorities. As a result, these methods are viewed as complements rather than replacements, and **upgrading the existing PKI remains essential for achieving post-quantum security**.

Importantly, the IETF has already taken concrete steps on key exchange. The working group published a draft specifying hybrid groups (X25519MLKEM768 and SecP256r1MLKEM768) combining a classical ECDHE algorithm and a module-lattice-based KEM.

4. CHALLENGES TO THE TRANSITION FROM A SOCIOTECHNICAL PERSPECTIVE

The transition to post-quantum PKI is **not only a cryptographic challenge but a whole sociotechnical transformation.** While much attention is devoted to algorithms, key sizes, and certification frameworks, the more difficult part of the migration lies in aligning technical, organisational, and societal dimensions.

A change at the cryptographic layer inevitably cascades across organisational processes, regulatory frameworks, and even end-user practices. The analogy with agricultural mechanisation is instructive: the introduction of the tomato harvester in post-war California was not just a technical substitution but reshaped entire communities, labour markets, and even the tomato itself. Similarly, PQC migration implies **redesigning the surrounding ecosystem**, reconfiguring certification bodies, training auditors, adapting vendor supply chains, and convincing reluctant operators to modify hardware or replace legacy systems. The technical challenge is therefore embedded in a wider reorganisation of the trust infrastructure.

Recognising PKI as critical societal infrastructure, the Dutch HAPKIDO consortium has pioneered methods to **map risks across sectors** such as government, banking, and telecom. Their societal risk assessment highlights how quantum threats manifest differently across domains. For instance, business-to-government exchanges often involve data with medium-term sensitivity, while government-to-citizen or intergovernmental data flows require far longer protection horizons. This assessment **encourages organisations to move beyond narrow compliance and ask: what is the societal impact if our digital infrastructure fails under a quantum attack?** The organisational **readiness models and a growth model-based roadmap also** help to stimulate internal discussions and embed quantum migration in broader security governance. The growth model outlines the initial awareness stage, assessment stage with cryptographic inventories ('no-regret moves'), to the full adaptation stage. Crucially, discontinuities between stages show points at which organisations cannot progress further without ecosystem-level conditions being met (e.g. standardisation updates, vendor product availability, or regulatory mandates). This highlights that migration is not linear but punctuated by dependencies that require policy and governance solutions as much as technical fixes.

The sociotechnical complexity of PKI transition stems, first and foremost, from **multi-actor interdependencies**. Certificates must chain back to trusted roots; conformity assessment bodies must validate implementations; vendors must supply updated HSMs and cryptographic libraries; regulators must certify; and users must be able to verify across borders.

These dense interdependencies are further compounded **by institutional fragmentation in the governance of post-quantum standards**. Implementation speeds differ across regions and sectors, and coordination between standardisation bodies, regulators, and industry consortia remains uneven. Open-source communities have already introduced PQ algorithms (e.g. ML-KEM) in protocols such as Secure Socket Shell (SSH), showing that adoption can occur outside formal standardisation channels. This diversity risks algorithm sprawl and regional fragmentation: different actors may implement incompatible algorithm sets, undermining interoperability. Without coordinated profiles, certification guidance, and cross-institutional policy alignment, the public sector could face a 'tower of Babel' scenario in PQ PKI deployment, threatening global trust continuity. Besides, a recurring concern is that **standards bodies may lag behind organisational needs**.

Notably, many of the standards underpinning eIDAS and European identity wallets remain untouched with respect to PQC. If organisations must wait for standardisation to trickle down before launching pilots, migration will become a sequential and lengthy process. Instead, experts emphasise the need for parallel action: **prompting standards organisations to map quantum impacts**, updating cryptographic profiles early, and ensuring that guidance evolves dynamically. Overall, this underscores the need for **ecosystem-wide coordination**, shared repositories of knowledge, and continuous learning. Critically, this also entails ensuring multilingual resources, shared glossaries, and plain-language summaries so that stakeholders at every level, governments, SMEs, auditors, and citizens, can engage.

PQC also involves dealing, from a sociotechnical perspective, **with path dependencies**. Indeed, with PQC, **legacy constraints are particularly acute**. Many industrial control systems, payment terminals, embedded IoT devices, and national identity infrastructures rely on cryptographic primitives implemented in hardware or firmware decades ago. Updating these components is costly, disruptive, and in some cases technically impossible without replacing entire infrastructures. The analogy with railway gauges is illustrative: Australia is still burdened by incompatible track widths decided a century ago. Likewise, cryptographic design choices made twenty years ago now block straightforward upgrades. These dynamics are especially acute in operational technology (OT), which underpins critical national infrastructure. Unlike enterprise IT, **OT environments often rely on decades-old equipment**, proprietary protocols, and resource-constrained embedded devices. Here, the overriding priority is availability: outages are unacceptable in sectors such as energy, transport, or healthcare. PQ algorithms, with their larger key sizes and higher computational demands, can easily overwhelm such devices. Migration pathways, therefore, range from deploying gateways and scheduling upgrades within controlled maintenance windows to wholesale hardware replacement. For legacy bespoke systems, organisations may be forced to pursue in-house updates (despite the risks of 'rolling their own crypto'), re-platforming, or retiring services entirely. Where none of these are viable, risk acceptance remains the only option. **Knock-on effects further complicate the picture.** Replacing cryptographic algorithms in one layer of a stack may cause failures elsewhere. A bank that migrates its TLS endpoints to PQC may find that embedded payment terminals can no longer interoperate. A government that mandates PQC certificates may disrupt cross-border e-signatures until standards bodies coordinate. Global supply chains magnify these risks: a blockage in one protocol or certification process can ripple across multiple industries, much as the temporary obstruction of the Suez Canal disrupted automotive manufacturing in Europe.

Looking through these lenses reveals that the PQC transition is not merely about replacing cryptographic algorithms. If the frame is limited to Shor's algorithm[22], the response is narrow and reactive. If the frame expands to the broader ecosystem, then a richer set of risks and strategies emerges. This perspective urges policymakers and technical communities to resist reductionist framings and to view PQC migration as a systemic transformation that touches sovereignty, privacy, and global equity as much as it does cryptographic mathematics.

Box 5. A sociotechnical perspective on PQC beyond 'Q-Day': the role of hype

Discussions of PQC are frequently animated by the spectre of 'Q-Day', a sudden moment when a powerful quantum computer renders classical cryptography obsolete. While useful as a mobilising narrative, this framing risks distorting the problem. Quantum capability will not arrive as a tsunami but as a gradual, uneven process. A handful of machines will first be able to break selected keys, before scaling to broader applications. In parallel, algorithms such as Grover's accelerate brute-force password guessing long before Shor-capable devices exist.

Hype can be both enabling and distorting. On the one hand, alarmist framings help mobilise investment, as seen in the rapid growth of PQC research consortia, pilot projects, and standards processes. On the other hand, over-reliance on the Q-Day metaphor risks premature or misaligned investments. Past examples illustrate this tension: after the Snowden revelations, symbolic actions such as webcam covers became widespread while deeper structural reforms lagged behind. In the PQC context, there is a risk that organisations spend resources on headline-grabbing migrations without addressing subtler but equally pressing challenges such as long-term confidentiality of stored data or crypto agility in supply chains. A more realistic framing, treating the problem as a Q-period, not a Q-Day, would support balanced migration strategies, paced with the actual evolution of quantum capability and standards readiness.

[22] Shor's algorithm is a quantum algorithm developed by Peter Shor (1994) that factors large integers and computes discrete logarithms using a quantum computer. Its polynomial-time performance for these tasks stands in contrast to classical algorithms. This is why Shor's algorithm underpins concerns about the vulnerability public-key cryptosystems.

PART X. TRANSITION TO QUANTUM SAFE IN THE DEFENCE SECTOR

1. INTRODUCTION

Quantum technologies are reshaping the strategic landscape of defence and security. For the European Union and its allies, the challenge lies not only in adopting these innovations but also in ensuring technological sovereignty and interoperability across a rapidly evolving global ecosystem. Their integration into defence systems promises to enhance situational awareness, resilience, and operational superiority, but also introduces new vulnerabilities, as quantum computing threatens existing cryptographic standards.

Governments, research institutions, and defence industries are converging to accelerate R&D while preparing quantum-safe transitions. Yet, as quantum technologies blur the boundary between civil and military domains, they also raise governance and ethical challenges, particularly around dual-use research, intellectual property, and security classification.

2. QUANTUM TECHNOLOGIES IN DEFENCE

Modern quantum technologies can be grouped into three core categories: quantum sensing and metrology, quantum communications/networking, and quantum computing. Each of these domains is at a different stage of maturity in defence applications. Related technologies include quantum radar/imagery and QRNG.

2.1. QUANTUM SENSING AND METROLOGY

Quantum sensing exploits quantum states for precise detection of physical quantities (magnetic/electric fields, acceleration or time). In defence applications, these technologies are more efficient than classical ones. The main domains of applications include:

- **Precision Navigation and Timing (PNT):** Quantum-enhanced atomic clocks provide valuable time references, improving Global Positioning System (GPS)-independent navigation (e.g. a technique used by submarines to avoid detection). Quantum accelerometers are under development to enable aircraft and submarine navigation without satellite signals.

- **Sensors and detection:** Quantum gravimetry and magnetometry are forms of quantum sensing that are considered for deployment on platforms and vehicles to detect underground structures, detect potential camouflage aircraft (air), localise unexploded objects (ground), or search for ships (underwater). Magnetic

Anomaly Detectors (MADs) have long been used to detect submarines by identifying the disturbances their metal hulls create in Earth's magnetic field. To illustrate, traditional MAD arrays (often towed or on patrol aircraft) have a limited range of a few hundred metres because the magnetic signals attenuate with distance. A private Canadian company was able to develop a quantum magnetometer with a 1.2 km range. This showcases the drastic difference between traditional and quantum technologies[23].

- **Metrology and timing**: Beyond navigation, quantum sensors improve timing synchronisation across military systems. Secure clock distribution via quantum links is perceived as an essential part of future quantum networks for increasing coordination of operations against spoofing or jamming[24].

With the increasing number of applications of quantum sensing (from quantum clocks to magnetometers), these technologies are expected to be deployed among the first quantum innovations in warfare.

2.2. QUANTUM COMMUNICATIONS

Modern militaries rely on secure communications for command and control, intelligence sharing, and coordination of forces. Quantum communication technologies seek to provide ultra-secure links that can withstand even quantum-computer-enabled eavesdropping. The driving concern is that once quantum computers mature, they could rapidly break the public-key encryption (RSA, Diffie-Hellman, elliptic curves) used to secure most military communications. Quantum communication differs from PQC in that it is based on physics rather than the computational difficulty of mathematical problems. The leading technology of this domain is QKD. Key developments include:

- Operation QKD systems: Quantum-safe communication links are being piloted. Trusted-node QKD networks are already in use, with China investing heavily in this technology. For instance, in 2016, it built a 2 000 km QKD fibre backbone between Beijing and Shanghai, linking multiple cities via quantum-encrypted links. In Europe, the EuroQCI initiative is deploying both terrestrial fibre networks and quantum satellites for secure communications (Security And cryptoGrAphic:

[23] See CAE MAD-XR (Magnetic Anomaly Detection-Extended Role), https://www.youtube.com/watch?v=btn288Y8G84.

[24] Unlike jamming, which causes signal loss, spoofing tricks systems into trusting false data. Spoofing can be used to divert autonomous vehicles, mislead drones, falsify timestamps in financial transactions, or disrupt synchronisation in telecom networks, (Source).

SAGA). Defence companies are involved: Leonardo has built a **quantum metropolitan area network (QMAN)** in Rome, connecting its sites via QKD.

- Quantum-safe networks: The final goal of quantum communications is transitioning from point-to-point QKD links to integrated quantum networks. Future entanglement-based networks (quantum repeaters) could eliminate the need for trusted relays, enabling long-range QKD. These networks would distribute quantum sensing and computing across forces, sharing quantum states securely.

2.3. QUANTUM COMPUTING

In defence, quantum computing is a double-edged sword for both offensive and defensive implications. A powerful quantum computer could break most of today's encryption protocols, endangering military communications and data security. To counter the cryptanalytic threat, militaries and governments are urgently developing and deploying PQC to resist attacks from both quantum and classical computers.

Future quantum computers might solve complex optimisation, simulation, or Artificial Intelligence problems much faster, offering advantages in logistics, encryption/decryption, or materials science for defence. Military logistics and operational planning involve extremely complex optimisation problems that can include routing, scheduling, resource allocation, and others, all of which must be accomplished under budgetary, geographic, technological, and human constraints. Quantum algorithms, such as Grover's search or quantum annealing methods, can tackle specific optimisation tasks more efficiently than classical heuristics. For example, route planning for supply convoys, optimal scheduling for air forces, or the efficient allocation of spare parts across the battlefield could be accelerated by quantum computing. In electronic warfare, quantum optimisation would help sift through frequency-hopping patterns or optimise jamming techniques. These possible implementations are still theoretical as they depend on having enough qubits. Quantum computing capabilities are also suited for simulations in quantum-mechanical systems. In a defence context, this may assist in designing new materials or understanding physical processes like high-temperature superconductivity for sensors.

Quantum sensing offers the most immediate operational advantages, with systems like Magnetic Anomaly Detector-Extended Role (MAD-XR) already deployed across allied navies and quantum gravimeters demonstrating battlefield utility in tunnel detection. Quantum communications present a more complex landscape, with China aggressively deploying QKD infrastructure while Western allies remain sceptical, preferring algorithmic post-quantum solutions. Quantum computing remains primarily a long-term capability requiring cloud-based access rather than battlefield deployment. Together with Artificial Intelligence, quantum tech is identified as a disruptive innovation for defence; one that North Atlantic Treaty Organisation (NATO) and EU strategists include in critical capability domains for 2030 and beyond.

3. RELEVANT STAKEHOLDERS AND QUANTUM DEFENCE INITIATIVES

3.1. OVERVIEW OF QUANTUM IN DEFENCE

Quantum technologies applications to defence involve a broad ecosystem of stakeholders from the public/private sector and international bodies, pursuing divergent approaches based on varying technical assessments and strategic priorities.

3.2. KEY PLAYERS AND INITIATIVES

Globally, defence planners recognise quantum technology as a strategic frontier, and many entities are mobilising to avoid falling behind. The landscape is characterised by a mix of military agencies setting requirements, industry developing solutions, and partnerships bridging the two.

In terms of **government and alliance stakeholders**, NATO and the EU have explicitly prioritised quantum tech in their innovation agendas. Quantum technologies are identified as an emerging and disruptive technology (EDT) by NATO. These technologies are considered transformative, and therefore NATO aims to foster the adoption of quantum technologies by allies as well as to protect the Alliance against the adversarial use of quantum technologies. NATO aims to foster the adoption of quantum-resistant cryptography and secure communications in the face of potential quantum challenges and threats. In terms of funding, NATO's **Innovation Fund** (a EUR 1 billion multi-national venture fund) and the DIANA accelerator programme include quantum tech in their priority areas, aiming to invest in startups and dual-use technologies that could benefit the overall security of the Alliance. By doing so, this means NATO contributes to the development of an allied quantum innovation ecosystem (e.g. companies working on quantum encryption or sensors) to ensure the Alliance keeps pace with quantum developments. The Transatlantic Quantum Community (TQC) plays a crucial role in this context. The TQC is a unique, flexible and voluntary-based community of 24 allied nations' government and industry stakeholders and academia. The TQC is used to find approaches on how to promote and scale quantum technologies within the Alliance.

The European Defence Agency (EDA) has taken a leading role within the EU to drive quantum technology adoption for defence. The EDA launched a project (ANQUOR) to explore military applications of quantum communication. The aim is to leverage civilian quantum R&D (e.g. EU Quantum Flagship results) and demonstrate use cases under military conditions, testing QKD-specific military requirements for feasibility and benefits in operations. Such projects show the EDA's approach of *dual-use innovation*: adapting civil quantum tech for defence needs. Individual initiatives from Member States (e.g. France with the Quantum in defence strategy) often encourage their defence primes to collaborate with startups and academic labs. On the **industry side**, traditional defence contractors and specialised quantum tech firms are increasingly collaborating. Industry consortia and networks are forming to share knowledge and accelerate development. Coordination through bidding alliances helps avoid duplication and promotes interoperability of these technologies across allies. Such insights push European stakeholders to stay competitive and avoid reliance on foreign quantum technologies.

Globally, the US, China, and others are also major stakeholders driving quantum tech, which influences the defence landscape globally. The US Department of Defense has multiple programmes (e.g. service labs) exploring quantum clocks, inertial sensors for GPS-denied navigation, quantum radio frequency receivers, as well as collaborations with companies such as IBM, IonQ, and Microsoft for quantum computing research. China has heavily invested in quantum communications (with Micius, for example). In April 2025, China announced a breakthrough in quantum magnetometers with the testing of a coherent population trapping atomic magnetometer, which may offer an advantage in specific operational environments, such as low-altitude regions where traditional magnetometers face challenges; it showcased its ability to detect the tail waves of enemy vessels.

Public-private partnerships are crucial in this domain, given that much quantum innovation originates in universities or small companies rather than within government labs. Startups provide the technology, and defence actors see how to integrate the technology. The public sector needs to emphasise these partnerships. In Europe, organisations such as the EDA and NATO are similarly encouraging such collaborations through funding calls and working groups. In the US, companies such as Lockheed Martin and Northrop Grumman have internal quantum research or investments (Lockheed was an early investor in D-Wave quantum annealing systems). These examples illustrate a growing defence-industrial base around quantum, where traditional defence contractors and cutting-edge quantum firms collaborate.

A notable point is that industry often works closely with the government on **pilot projects** to prove quantum tech in real conditions. For example, Thales participated in the European OPENQKD testbed. Such demonstrations help develop standards, security certifications, and operational concepts.

It is also worth noting the **international dimension** of stakeholders: the race in quantum tech is not only commercial but geopolitical. The US and China dominate patent filings in areas like PQC, accounting for over two-thirds of global patents between 2012 and 2024. NATO has launched research initiatives and multi-national projects, and there is transatlantic cooperation (e.g. US-EU dialogues on quantum standards and security). Rapid evolution by other global powers (e.g. China's achievements in quantum communication) act as a spur for NATO and EU members to coordinate their efforts.

4. Quantum-safe transition in the defence sector

The **transition to quantum-safe cryptography** in the defence sector is a coordinated effort spanning policy (mandates and timelines set by organisations such as NSA, EDA, NATO), technology development (by defence industry and cybersecurity firms), and implementation planning (inventorying vulnerable systems and developing migration plans). The overarching goal is to **prioritise communications security in anticipation of future threats**, ensuring that when quantum computers do emerge, adversaries cannot cripple military systems of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) or decrypt years' worth of sensitive data. Notably, a **PQC patent landscape study** presented at the EDA showed the US and China accounting for over two-thirds of global patent families in post-quantum cryptography. This transition is already underway: pilot projects are testing PQC in real-world scenarios (e.g. the US Army contracting a quantum-resilient communication solution for tactical networks), and alliance-wide guidelines are being issued. The challenge ahead lies in updating a vast array of legacy systems in time and managing the change without disrupting current operations: a challenge that stakeholders are addressing now so that militaries remain secure in the quantum era.

Defence industry players are crucial in this transition, since they manufacture the communication systems, software, and hardware that will need upgrading. Indeed, the industry has adopted crypto-agility principles with in-house expertise. Leonardo has been working on practical integration issues, such as migrating VPN protocols (e.g. WireGuard), to use PQC for authentication, integrating PQC into TLS secure communications, and combining QKD with PQC for layered security. These efforts are perceived within the industry.

Quantum technologies are rapidly transitioning from research to deployment, redefining the foundations of defence capability and strategic autonomy. Quantum sensing will likely deliver the first operational advantages, quantum communications will reshape information security, and quantum computing, although longer-term, will transform decision-making and cryptographic paradigms!

PART XI. RECOMMENDATIONS

This Task Force believes that the shift to quantum-safe cryptography should be understood not as a routine technical upgrade but as a **comprehensive, systemic transformation**. Transitioning to PQC extends far beyond updating cryptographic libraries; it typically requires integrating new product versions, modifying APIs, adapting software development lifecycles, and, in some cases, redesigning core business processes, including the supply chain. This process represents a **managerial challenge** that calls for long-term planning, specialised workforce recruitment, and **sustained organisational change** over several years.

Against this backdrop, this Task Force puts forward the following recommendations to policymakers, the private sector and the research communities on how to strengthen the transition to quantum safe in the EU.

This section is structured to first present the **general recommendations**, followed by the **sector-specific recommendations**. It should be noted that the sector-specific recommendations are intended as an additional layer to the general recommendations outlined in the following section. They do not replace or stand apart from the overarching measures, but rather complement them by addressing risks, implementation challenges, and operational practices that are unique to each sector.

1. GENERAL RECOMMENDATIONS

GR1. Develop crypto agility

In general, cryptographic systems may be weakened and may need to be replaced by updated versions. The migration to quantum-safe encryption is just one imminent instance of this update. In the pursuit of quantum-safe encryption, the transition of encryption methods of billions of devices requires a specific model, needing design from a technical, organisational and policy perspective. For such an endeavour, a risk-based approach is necessary. Such an approach should revolve around **crypto-agility principles** based on measured risks and needs.

Cryptographic agility is the design of cryptographic protocols and systems in a modular way that enables replacing the cryptographic components. Rather than a one-off swap of algorithms, the crypto-agile approach entails building the capacity to change cryptographic algorithms and protocols rapidly with minimal disruption. This thereby avoids the security vulnerabilities of outdated algorithms. For example, applications should support cryptography where algorithms can be changed via configuration rather than code overhaul, and protocols should be negotiated to use the strongest standard algorithm available between parties. It's as much a software engineering challenge as a cryptographic one. Agility also implies maintaining interoperability during the migration, which is deemed a necessity.

GR2. Engage with suppliers to take care of crypto dependencies

Most organisations rely heavily on third-party products and services, and supply chain dependencies frequently define the constraints and possibilities of migration. Migration to PQC often stalls when critical products or dependencies are beyond the direct control of the organisation. Software vendors and suppliers are on staggered upgrade schedules, and many cryptographic components are buried in complex, nested dependencies. To address this, **organisations need robust engagement with suppliers**, clear requests for timelines on quantum-safe capabilities, and a mechanism for tracking supply chain readiness. In this context, actionable planning begins with an inventory of internal and external dependencies, software, hardware, APIs, and services so that organisations can engage suppliers, demand timelines for upgrades, and plan accordingly. This mapping is not only a technical prerequisite but also enables alignment with supply chain risk management tools that can be integrated into EU regulations. If supply chain partners report cryptographic details in standardised formats, it will allow for more reliable automation, compliance, and policy-making.

GR3. Building and maintaining crypto and product inventories

In preparation for the shift to post-quantum cryptography, organisations are increasingly focusing on how cryptographic and product inventories are built and maintained. Developing inventories should be prioritised, focusing first on the most relevant use cases. Prioritising such an inventory will help with building a roadmap and provide context on migration activities. An inventory of cryptographic assets is an important task that, based on previous analysis, will facilitate a better understanding of the landscape of what needs to be migrated. What emerges is not a rigid blueprint, but rather a set of guiding practices, shaped by early planning, collaboration across technical and governance teams, and a clear understanding of what such inventories need to capture and why. The goal is to develop a shared language and operational map that allows different actors to approach their inventories not as isolated checklists, but as evolving tools supporting broader transition strategies. This framework will incorporate early planning, cross-functional coordination, and a primary goal of understanding how to approach inventories methodically and structurally. Cryptographic and product inventories are two different assessments.

Cryptographic inventories are a detailed mapping of where and how cryptography is used across an organisation's systems. Its objectives are to identify the cryptographic algorithms in use today (RSA, ECC, AES), their implementation context (code signing; TLS for communications), their quantum resistance status (legacy or PQC), and the dependencies of cryptographic modules and standards. A key theme of cryptographic inventories is to **adopt a risk-based approach** to prioritise inventories for the critical systems that need PQC first. When cataloguing cryptographic assets, it is essential to **be aware of the intertwined infrastructure of the systems mapped.**

The data recorded in such inventories must be granular and detailed, and should include:

- the type of algorithm in use (RSA-2048, ECC, AES-128, SHA-2, etc.)
- the functional purpose of that cryptography (i.e. authentication, confidentiality, integrity)
- the protocol context (i.e. TLS 1.2, IPsec, S/MIME)
- the asset where it is used (i.e. firmware update signing for routers, internal APIs in applications, VPN concentrators)
- the origin of the cryptographic function (i.e. in-house developed, third-party library, OS kernel module)
- its compatibility with PQC standards, or whether it is part of a hybrid scheme
- the lifespan of the data it protects (short-term v long-term stored data)
- the sensitivity of the data it protects (proprietary, classified).

Product inventories focus on external products, services, and hardware that an organisation uses (i.e. third-party providers), and map the cryptographic characteristics of these products. Organisations can use practical tools and processes for a cryptographic assessment of their product inventories. Updating the procurement guidelines to include cryptographic requirements and addressing inquiries could be an option. In other words, when purchasing new software, hardware, or cloud services, organisations would require vendors to disclose the cryptographic algorithms and protocols used in their products, potentially including a roadmap for post-quantum upgrades.

GR4. Integrate quantum safety into digital systems from the start

The European Commission and Member States should ensure that digital systems (such as the European Digital Identity Wallet) **are designed to be quantum-safe from the start**. In other terms, if new services, systems or standards are introduced that require crypto, then this crypto should be quantum safe from day one. This means integrating post-quantum cryptography into system architecture, certification, and procurement processes rather than treating it as a future retrofit. EU bodies should coordinate conformity testing, fund **pilot deployments to assess performance across devices and networks**, and issue prescriptive technical guidance to prevent fragmentation. Embedding these principles now will secure Europe's digital infrastructure for the next decades and avoid costly, disruptive upgrades after deployment.

GR5. Going beyond hype: from a Q-Day to a Q-period

Discussions of PQC are frequently animated by the spectre of Q-Day, a sudden moment when a powerful quantum computer renders classical cryptography obsolete. While useful as a mobilising narrative, this framing risks distorting the problem. Quantum capability will not arrive as a tsunami but as a gradual, uneven process. A handful of machines will first be able to break selected keys, before scaling to broader applications. In parallel, algorithms such as Grover's accelerate brute-force password guessing long before Shor-capable devices exist.

Hype can be both enabling and distorting. On the one hand, alarmist framings help mobilise investment. On the other hand, over-reliance on the Q-Day metaphor risks premature or misaligned investments. In the PQC context, there is a risk that organisations spend resources on headline-grabbing migrations without addressing subtler but equally pressing challenges, such as long-term confidentiality of stored data or crypto-agility in supply chains. **A more realistic framing, treating the problem as a Q-period, rather than a Q-Day, would support balanced migration strategies**, paced with the actual evolution of quantum capability and standards readiness.

GR6. Linking the Roadmap for the Transition to Post-Quantum Cryptography[25] to a quantum transition strategy and to existing laws

There are significant risks in pursuing an EU quantum-safe Roadmap without a coordinated, risk-aware transition strategy. A Roadmap must specify what milestones are required and by when, but only a supporting strategy can define how Member States, vendors, and institutions will meet them. Without synchronised standards, certification schemes, interoperability frameworks, and testing infrastructures, regulation may outpace readiness. The Roadmap should therefore be embedded in a broader EU framework that aligns national plans, industry efforts, and regulatory tools, ensuring

[25] Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (the Roadmap).

coordination across DORA, CRA, and NIS2, and guided by the institutional actors of ENISA, the Commission and standardisation bodies of ETSI, CEN/CENELEC, to deliver a coherent, actionable transition.

GR7. Ensure alignment and coherence across roadmaps

Multiple roadmaps for quantum-safe transition are currently being developed and discussed at the EU and national levels, covering post-quantum cryptography, quantum communication, and related infrastructure initiatives. While each roadmap sets valuable priorities and indicative milestones (e.g. 2026, 2030, 2035), their coexistence risks producing fragmented or, worse, incompatible requirements and implementations if not properly aligned. The European Commission, together with Member States and standardisation bodies, should therefore **promote cross-roadmap coordination to ensure coherence in timelines, dependencies, and objectives.** This alignment is particularly critical across standards development, vendor implementation, and large-scale deployment phases, which operate on different time horizons.

To ensure global coherence and avoid fragmentation, the EU should also coordinate closely with the US and other G7 economies to align roadmaps, technical requirements, and timelines for quantum-safe transitions.

GR8. Introducing greater parallelisation into the Roadmap

The Roadmap's current structure implicitly relies on a staged or linear approach, which may unintentionally create bottlenecks, particularly where progress in one area depends on completion in another. Given the complexity and heterogeneity of cryptographic systems across the EU, **we recommend introducing greater parallelisation into the Roadmap to accelerate progress and reduce systemic risk**. Below are specific, actionable suggestions for increasing parallelism while maintaining coordination and alignment. Instead of recommending a rigid sequence of activities (e.g. inventory → risk assessment → pilot → deployment), we suggest structuring the Roadmap into modular, composable milestone packages. These modules can be initiated independently, where conditions allow, enabling Member States, sectors and operators to move forward without waiting for all preceding tasks to be complete.

For example:

- Inventory and cryptographic asset classification can proceed in parallel with protocol-readiness evaluation.
- Vendor engagement and procurement planning can begin while regulatory alignment discussions are ongoing.

- We propose **decomposing the Roadmap into role-specific tracks,** each with its own activities, deliverables and timelines. These tracks reflect the natural division of labour across the ecosystem and allow different stakeholders to proceed in parallel.
- **Policy and regulatory track**: focused on mandates, legal harmonisation and public sector funding instruments.
- **Standards and interoperability track:** focused on profiling, conformance criteria and integrating emerging international standards.
- **Vendor enablement track:** focused on incentivising the development, certification and benchmarking of PQC-capable products.
- **Operational deployment track:** focused on asset inventories, Cryptography Bill of Materials, the migration of public services and incident response updates.
- **Oversight and metrics track:** focused on measurement frameworks, audits and maturity models.

This structure enables each stakeholder group to work on relevant tasks independently of other groups' progress.

GR9. Promoting awareness, cooperation and better governance

In cyberspace, all nations are connected across borders and depend on each other, including in this transition. Therefore, Member States **should create an environment or community where organisations, entities and stakeholders can share knowledge and experiences**'.

For European industries operating internationally, close alignment with already published global timelines and algorithm recommendations is essential. Many European companies are already deeply engaged in the development and implementation of ML-KEM, ML-DSA and SLH-DSA in their products and services, working to meet the ambitious 2030-2035 PQC deployment timelines. It is not realistic to expect that each Member State can individually create communities that attract global organisations, entities and stakeholders such as the IETF, 3GPP, the US government or major US companies. Even coordinating this at the EU level is extremely challenging. Instead, **Member States should actively participate in open, global standardisation organisations such as the IETF and 3GPP, as well as in the open-source cryptographic community**, to ensure alignment, influence and knowledge-sharing at the international level.

Member States should lead by example with transparent transition plans: publish and regularly update government transition roadmaps, including timelines, milestones and budgets, to foster knowledge sharing and best practices. The Roadmap should broaden its definition of 'stakeholder' beyond ministries, regulatory agencies and technical experts. Civil society, minority networks and grassroots DEI organisations should be recognised as co-leaders, not simply 'consulted'. The integration of social clauses and community dividends into procurement, partnership and policy evaluation is vital, not just as a 'best practice' but as a requirement for measurable inclusion.

Awareness campaigns and training modules should not be generic or one-size-fits-all. **This CEPS Task Force is asking for a radical expansion of civic and digital education, embedding PQC awareness, quantum risk and digital rights topics not just in technical teams but across society, schools, care institutions and community centres.**

The Roadmap should establish mechanisms (citizen assemblies, consultation panels, regular transparent updates) to ensure citizens not only receive information but can actively shape strategies. The Roadmap should **encourage joint pilot projects at the EU level to test interoperability of PQC in cross-border services before 2030.**

We suggest **establishing a public-private PQC migration observatory under ENISA** to monitor advances and recommend acceleration of timelines if necessary.

We advocate for continued international dialogue on transition strategies and standards. As one potential path forward, we would welcome the G7 expanding the scope of its current quantum safety initiative in the financial sector to include a broader conversation across all sectors.

GR10. Promoting skill development and management structures

Finally, successful migration also depends on management structures and skill development. Cryptographic migration is no longer just the purview of niche technical experts; it requires cross-functional teams, transparent governance, and clear process ownership. Many organisations struggle because no single team is accountable for overseeing the transition, and the necessary skills are in short supply. Investment in education, internal centres of competence, and cross-team coordination is essential to reduce friction. A lack of immediate incentives and executive-level attention perpetuates the hesitancy to address this challenge. Organisations should have a **well-established, funded, and empowered programme that starts with clear business-level priorities.** Much of the current progress is bottom-up and lacks executive support.

2. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE FINANCIAL SECTOR

FS1. Create an ad hoc PQC governance structure

Governance structures are vital. Firms should establish a PQC transition steering committee or task force. This group oversees inventorying cryptographic usage, tracking standards, and setting migration timelines in alignment with business priorities and regulatory requirements. Many large banks have already formed internal 'quantum risk' or 'crypto agility' teams for this purpose.

FS2. Enhancing collaboration with vendors and partners

The financial sector's crypto infrastructure extends beyond the walls of any single institution. It includes vendors, third-party service providers, and hardware manufacturers. It depends on these actors. A key bottleneck is the **readiness of technology providers** to support PQC. Therefore, firms should engage vendors early to ensure their roadmaps include PQC support, effectively asking for **crypto agility by design in new procurements.** Vendor incentives may be increased and fragmentation reduced if financial institutions can agree on common procurement standards.

FS3. Upgrade the financial sector underlying infrastructure

Companies need to **upgrade their underlying infrastructure** to ensure that HSMs, cryptographic libraries, VPN appliances, and other related components can support quantum-safe algorithms. A key recommendation is to modernise algorithms **as part of the ongoing broader IT modernisation initiative**. For example, if a bank is migrating services to the cloud or replacing core banking systems, crypto-agility considerations should be built in from the start.

FS4. Prioritise actions based on risk assessment

Given the scale of the transition, not everything can be changed at once. A risk-based approach is essential to prioritise which systems and data to secure first. This process begins with a **cryptographic inventory**. Instead of aiming for a comprehensive inventory that is costly and may become outdated once actual migrations begin, we recommend a top-down and risk-based approach that creates inventories for migrating specific parts of the business based on a business-level risk-reward analysis. While certain dependencies will need to be maintained, this ensures that the business justification and value can be identified and tracked while migrating.

For creating an inventory for a specific project, financial institutions should catalogue all cryptographic assets, including algorithms, key lengths, certificates, and their usage locations and methods. The inventory must also identify which assets have long-lived confidentiality requirements (for example, data that needs to remain secret for 10 years or more). Using this inventory, firms can then **estimate the quantum vulnerability** of each asset. Crucially, risk assessment must consider **both cryptographic strength and business impact**. Not all systems carry equal risk; one must prioritise the critical systems that need PQC first. High-impact assets, such as payment clearing systems or PKI that underpin interbank authentication, with long security lifespans, should be migrated early.

FS5. Perform cost-benefit analysis of mitigation options

Not all solutions are equal: some may involve hardware changes (using hybrid solutions in hardware or deploying QRNGs or QKD links), while others are purely software-based (switching to PQC algorithms). The Task Force mentions that a complete crypto transition for a large bank could cost in the order of hundreds of millions of dollars. The importance of quantified risk assessments for boards and executives is essential to justify expenditures against the risk reduction achieved. **If the cost of inaction (i.e. potential fines, losses, and reputational damage from a future breach) outweighs the migration cost, the business case for PQC investment becomes clear.**

FS6. Overcome organisational and skills gaps

Financial institutions face a **shortage of cryptographic skills and awareness** at all levels. Cryptography has often been a niche domain in IT; now it must become a mainstream concern. The culture in many financial organisations has been to treat cryptography as a static utility. Changing this mindset to one of continuous cryptographic improvement is an organisational challenge.

3. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE PUBLIC SECTOR

PS1. Implement a sequenced migration plan across PKI and digital identity ecosystems

Public administrations should adopt a coordinated, risk-based approach to upgrading PKIs and digital identity systems. Migration should begin with the **most critical and high-impact components**, such as national identity registers, cross-border authentication services, and certificate authorities that anchor public trust, before extending to dependent systems. Administrations should conduct comprehensive cryptographic inventories to map dependencies and identify areas most exposed to quantum risks. This mapping should inform **sequenced migration roadmaps** that combine hybrid cryptography for short-term continuity with long-term adoption of post-quantum standards. To ensure sustainable implementation, new procurements for digital identity and trust services must include crypto agility and PQ-readiness requirements, ensuring systems can evolve alongside standards. This coordinated and risk-informed approach will help avoid fragmented upgrades and ensure that essential authentication and signing services remain operational throughout the transition.

PS2. Synchronise authentication layers to prevent fragmentation and service disruption

Authentication systems, roots, intermediates, browsers, and revocation services must **evolve in lockstep** to preserve trust and interoperability during the quantum transition. The European Commission and national authorities should **coordinate migration to ensure simultaneous readiness across these layers**. This includes benchmarking performance impacts, conducting interoperability and stress tests, and establishing fallback mechanisms to handle larger certificates and increased computational demands. A synchronised approach will prevent fragmented implementations and minimise service outages.

PS3. Coordinate cross-border roadmaps and align national migration strategies

The European Commission and Member States should establish a joint roadmap for quantum-safe migration, aligning national PKI upgrades, timelines, and policy frameworks. This coordination should focus on **interoperability across borders**, ensuring that trust chains, certification processes, and governance models remain consistent within the EU. Regular reporting and **shared readiness benchmarks** should be institutionalised to ensure that national infrastructures evolve in sync and maintain mutual trust.

PS4. Manage the quantum transition as a coordinated sociotechnical programme

Post-quantum migration in the public sector should be approached as a **whole-of-ecosystem effort**, not solely a cryptographic upgrade. The European Commission and Member States should establish coordination mechanisms bringing together technical agencies, regulators, standardisation bodies, and industry actors to guide the transition. Migration plans must also **account for legacy and operational-technology constraints** by scheduling upgrades and enabling parallel standards updates to prevent bottlenecks.

4. ADDITIONAL SECTOR-SPECIFIC RECOMMENDATIONS FOR THE DEFENCE SECTOR

DS1. Develop a post-quantum transition roadmap

Defence industry stakeholders should establish a post-quantum transition roadmap that synchronises governmental policy milestones with industrial deployment. This roadmap should mandate comprehensive cryptographic inventories, prioritise mission-critical and high-risk systems, and coordinate cross-vendor testing of PQC implementations. Developing shared migration benchmarks will enhance interoperability across defence supply chains, prevent redundant efforts, and enable the modernisation of legacy command, control, and communication infrastructures without disrupting critical operations.

DS2. Support industrial coordination

Institutional stakeholders should support **industrial coordination** between defence primes, SMEs of the quantum industry, and research labs through funding mechanisms that prioritise European value chains and reduce reliance on non-EU suppliers.

DS3. Address supply-chain dependencies

Similarly, competent European institutions (e.g. the European Defence Agency (EDA), the European Commission and the European Defence Fund (EDF)) should address **supply chain dependencies**: several key quantum algorithms and hardware components currently originate in the US or Asia. European actors should prioritise developing proprietary quantum algorithms, photonics platforms, and cryogenic technologies in Europe.

DS4. Formalise public-private quantum innovation frameworks

International and European defence institutions (EDA, NATO, EDF) should formalise **public-private quantum innovation frameworks** connecting established defence contractors with start-ups and academic labs. These partnerships should include shared testbeds, classified-and-open R&D tracks, and co-funded demonstrators to accelerate technology transfer. Priority should go to **dual-use quantum sensing and communication systems**, ensuring civil R&D (from Quantum Flagship or national programmes) is adapted to defence applications.

DS5. Establish structured pilot-to-certification pathways

To validate emerging quantum systems for operational use, the **EU and NATO** should establish **structured pilot-to-certification pathways**. Programmes such as OPENQKD should evolve into permanent **Quantum defence testbeds,** allowing companies (e.g. Thales, Leonardo, SMEs) to test prototypes under military conditions. Results should directly feed into European standardisation bodies (ETSI, ENISA) to define **security and interoperability benchmarks**, thereby reducing time-to-deployment and ensuring trusted European solutions.

DS6. Incentivise research in defence quantum technologies

To incentivise **research in defence quantum technologies**, it is essential to establish secure **knowledge-sharing mechanisms** (e.g. classified research consortia, modular publications, or declassification windows) allowing academics to maintain academic career progression without breaching defence restrictions.

ANNEX I. LIST OF TASK FORCE MEMBERS AND INVITED SPEAKERS

Coordinator and rapporteur: Lorenzo Pupillo, CEPS

Rapporteurs: Swann Ashworth, CEPS, Afonso Ferreira, CNRS, Carolina Polito, CEPS

Advisory Board

Sofie Lindskov Hansen, Danish Ministry of Foreign Affairs

Michele Mosca, Waterloo University, Canada

Michael Osborne, IBM Zürich Research Center

Bart Preneel, KU Leuven

Tim Watson, Alan Turing Institute, London

Companies

Deloitte, Barbara Wellmann, Tommaso Stranieri

E&Y, Sarah Ampe, Sourav Sinha

Ericsson, John Mattsson

Intel, Riccardo Masucci, Matthias Schunter

Inveriant, Alessandro Luongo

KPMG, Bent Dalager

Microsoft, Kevin Reifsteck

Qualcomm, Sabrina Stanislas-Boumier

Quantinuum, Duncan Jones, Marion Lemasson

Santander, Jaime Gómez García

Sparkle, Antonella Sanguineti

European institutions and agencies

European Parliament, Brando Benifei, Angelica Petrov

European Commission, Fabiana Da Pieve

ENISA, Philippe Blot

EDA, Georgios Stamatoukos, Isidoros Monogiudis

ECCC, Rodica Tirtea

ESA, Massimo Panzeri

ETSI, Martin Ward

EIB, Harld Gruber, Désirée Ruckert

EU Quantum Flagship, Enrique Sánchez Bautista

BSI, Ehlen Stephan

Research institutes

Istituto Italiano di Tecnologia, Camilla Coletti, Antonio Rossi

Academics/think tanks

GMF, Astrid Ziebarth

I-COM, Antonio Manganelli

University of Amsterdam, Laima Jančiūtė

University of Malaga, Javier Lopez

University of Primorska, Nastja Cepak

University of Salento, Antonio Ficarella, Alessandro Lazari

University of Utrecht, Federica Russo

Civil society

Humanity of Things Agency, Marisa Monteiro Borsboom, Dirk Bloem

Invited speakers

Simona Autolitano, BSI

Frederic Barbaresco, Thales

Olivier Blazy, Ecole Polytechnique

Mirko Calvaresi, European Commission

Sofia Celi, Brave

Karen de Winter, IBM

Mauro De Santis, Italian Central Bank

Massimiliano Dispenza, Leonardo

Angela Dupont, Bank for International Settlements

Alex Ferrazzini, GovStrat

Edoardo Giglio, Deloitte

Francisco Herrera, European Central Bank

Ini Kong, TU Delft

Stravos Kousidis, BSI

Kaan Sahi, NATO

Aviram Shemesh, Microsoft

Michael Silverman, FS-ISAC

Pieter Vermaas, TU Delft

Johannes Verst, QBN

Fern Watson, Financial Conduct Authority, UK

ANNEX II. Glossary

Cold atoms: atoms cooled at very low temperatures, generally with techniques using lasers and the Doppler effect. They are used in certain types of quantum computers called cold atom quantum computers. The atoms used are neutral atoms (not ionised) and quite often rubidium, an alkali metal.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Cryogenics: cooling technology. Very low temperature cryogeny is used with superconducting and electron spin qubit computers. The temperatures required to stabilise qubits and reduce their error rate are very close to absolute zero: around 15 mK. The most commonly used systems are dilution refrigerators that use helium-3 and helium-4. Cryogenics is also used for photon generators and photon detection systems, but at a higher temperature situated between 2K and 10K.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Cryptographic agility: as defined by the NIS Cooperation Group Roadmap, the design of cryptographic protocols and systems in a modular way that enables replacing the cryptographic components.

Source: NIS Cooperation Group (2024), Roadmap for the Transition to Post-Quantum Cryptography.

Cryptographic Bill of Materials: CBOM is an object model to describe cryptographic assets and their dependencies. It is an inventory or list of all cryptographic assets used in a product or system, including algorithms, key lengths, certificates, and their usage.

Source: IBM, ETSI Quantum Safe Cryptography Conference 2024.

Cryptographically Relevant Quantum Computer: a CRQC is a quantum computer powerful enough to break or significantly weaken modern cryptographic systems. In other words, a CRQC is a quantum computing system capable of executing attacks (like Shor's algorithm) that would be infeasible on classical computers, thereby undermining widely used public-key encryption and digital signature schemes.

Source: CEPS Task Force Report.

Entanglement: a quantum phenomenon where two quantum objects are related to each other in a way that a measurement done on these two objects generates a correlated (but random) value. This process is used to link qubits together through two or three-qubit quantum gates in quantum computers. It is also used in quantum cryptography and telecommunication systems based on entangled photons in QKDs.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Entropy: measures the degree of disorder and randomness of a physical system.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Gate-based quantum computing: the broader category of quantum computing systems based on qubits and quantum circuits implementing quantum gates on 1, 2, and 3 qubits at a time.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Grover (algorithm): a quantum algorithm for finding an element in a non-indexed array or a unique element for which an oracle function returns 1.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Hardware security module: an HSM performs cryptographic operations to secure data and provides certain functions to use these operations on an external physical interface.

Source: BSI, VS-Anforderungsprofile 2024.

Hybrid encryption: to denote a context-aware and technically inclusive approach encompassing all strategies that combine multiple cryptographic inputs.

Source: Task Force report.

Ion: non-neutral atom, which has a positive or negative electric charge. It is negative if its number of electrons exceeds the number of protons (anions) and positive in the opposite case (cations).

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Key encapsulation mechanism: a KEM is a set of algorithms that, under certain conditions, can be used by two parties to establish a shared secret key over a public channel. A shared secret key that is securely established using a KEM can then be used with symmetric-key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication.

Source: NIST FIPS 203.

Logical qubit: an assembly of physical qubits implementing hardware and software quantum error correction. Seen from the software developer's point of view, it creates a virtual logical qubit with a very low error rate. The fidelity of logical qubits depends on the number of physical qubits they contain, the quality of the error correction codes and the qubits' fidelity stability with the increase in the number of physical qubits.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Noisy intermediate-scale quantum: NISQ is a name for current and near-future gate-based quantum computers, which are intermediate in terms of number of qubits (a few tens to hundreds) and subject to quantum noise that limits their capabilities. This acronym was created by John Preskill.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

No-cloning theorem: prohibits the identical copy of the state of a quantum. Therefore, it is impossible to copy the state of a qubit to exploit it independently of its original. Any copy destroys the original.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Photon: quantum of energy associated with electromagnetic waves ranging from radio waves (long waves, low frequencies) to gamma rays (very short waves, very high frequencies) through visible light. Its mass is zero. Its spin is 1, and it is therefore part of the bosons. Photons are absorbed and emitted by atoms during energy level changes.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Post-quantum cryptography: PQC is cryptography resistant to quantum computer-based codebreaking algorithms. It is based on the use of public keys that are not decomposable with conventional or quantum computers.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Private key: key used in private key encryption systems. Keys are exchanged beforehand by the parties using an encryption algorithm, often a hash or Diffie-Hellman algorithm.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Public key: an encryption system that involves sending a public key to an interlocutor who will use it to encrypt a message sent in the other direction. The elements used to create this public key are used to decrypt the message sent. It is normally impossible or very difficult to decompose the public key to find the elements that were used to create it. PQCs are based on public keys.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Quantum key distribution: a secure protocol for sending symmetrical keys via an optical link based on quantum entanglement (fibre or satellite). These keys are tamper-proof, or at least an interception of the key is detectable.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Quantum random number generator: QRNGs are the optical random number generators used in quantum cryptography, like those of the Swiss IDQ.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Quantum advantage: occurs when a quantum computer executes some processing faster than its optimum equivalent adapted to a supercomputer, with a useful algorithm. This advantage can be declined on an aspect other than the duration of the calculation. For example, a quantum energy advantage relates to energy consumption instead of computing time.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024

Qubit or physical qubit: the elementary unit of information in quantum computing in quantum computers and quantum telecommunication. It stores a quantum state associating two distinct states of a particle or of a quantum system (electron spin, energy level of a superconducting loop, energy level of a trapped atom or ion, polarisation or other property of a photon).

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

RSA: a public key encryption system based on the difficulty of factoring a public key formed by multiplying two very large prime numbers. This factorisation is theoretically possible with Shor's quantum algorithm. However, it requires a very large number of qubits to break the most common RSA keys at 1 024 or 2 048 bits. For 2 048-bit keys, 20 million physical qubits with a 99.9%+ fidelity are required, which is very long term in quantum computer roadmaps.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Shor (algorithm): integer quantum factorisation algorithm invented by Peter Shor in 1994. It would theoretically allow breaking RSA public keys by decomposing them into prime numbers.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

Software Bill of Materials: SBOM is a formal record that lists all components and dependencies contained in a software product, along with their origin. It is essentially an 'ingredients list' for software, covering open-source libraries, modules, and other third-party or proprietary components that are included in the software. SBOMs facilitate easier updates and compliance by making software composition explicit.

Source: CISA.

Symmetry: refers to situations where physical properties remain unchanged when a specific transformation is applied to a system, like spatial rotations, translations, reflections, time inversions, and more. Symmetry is deeply linked to the conservation laws in physics, where the invariance of certain quantities such as energy, momentum, and angular momentum under specific transformations leads to the conservation of those quantities.

Source: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

PRINCIPLES AND GUIDELINES FOR THE TASK FORCE

The Task Force process is a structured dialogue among experts, (former) politicians, diplomats, policymakers, NGOs, academia and think tanks who are brought together for several meetings. The Task Force report is the final output of the research carried out independently by CEPS and its partners, and in the context of the Task Force.

Participants in a Task Force

- The Chair is an expert who steers the dialogue during the meetings and advises CEPS as to the general conduct of the activities of the Task Force.
- Members provide input as independent experts.
- Rapporteurs are CEPS researchers who organise the Task Force, conduct the research independently and draft the final report.

Objectives of a Task Force report

- Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on available data, literature, and views.
- Reports seek to provide readers with a constructive basis for discussion. They do not seek to advance a single position or misrepresent the complexity of any subject matter.
- Task Force reports also fulfil an educational purpose and are drafted in a manner that is easy to understand, without jargon, and with any technical terminology fully defined

Drafting of the report

- Task Force reports reflect members' views.
- However, there does not need to be consensus or broad agreement among Task Force members for every recommendation that features in the report. Recommendations which triggered significant dissent are marked accordingly.
- Task Force reports feature data that are considered both relevant and accurate by the rapporteurs. After consultation with other Task Force members, the rapporteurs may decide either to exclude data or to mention these concerns in the main body of the text.

CENTRE FOR EUROPEAN POLICY STUDIES
Place du Congrès 1
1000-B Brussels
Belgium