HAPKIDO

Navigating the Transition to Quantum-Safe PKI

HAPKIDO Handbook

NWO

HAPKIDO

Navigating the Transition to Quantum-Safe PKI

HAPKIDO Handbook

Table of contents

Foreword

As Director CIO Rijk, I notice both political and societal attention being paid to issues in the field of digitalisation. Although quantum-safe cryptography is, for most people, a technical subject that feels far removed from everyday life, this topic has taken off. There is increasing attention for it; see, for example, the recent report by de Algemene Rekenkamer (the Netherlands Court of Audit).

Quantum-safe cryptography is not only about technology; it affects the systems that people rely on every day. It concerns secure payments, the protection of medical data, and the availability of the government.

The fact that our cryptography works well today, does not automatically mean that this will remain the case.

As a society, we are standing on the threshold of the quantum computer era. This new form of computing power offers opportunities. Complex problems can be studied, and perhaps solved, more effectively with this technology. Think of the development of new medicines or technology that contributes to our safety.

It is the task of government to provide room for innovation, but also to identify risks in a timely manner. And those risks are real. For example, when it comes to the cryptography we currently use to pay by card, to chat, or to log in. If we do not act, this technology will eventually be unable to withstand the computing power of quantum computers.

Many scenarios consider the period around 2030 as the moment when quantum computers may be able to break today's cryptography. That moment is referred to as 'Q-day'. When it will happen exactly, we do not know. But it is clear that we must prepare for this now.

For it is essential that the digital foundation of our society remains secure after that point as well. So that people can continue to trust that their data is well protected.

That is why the transition to Post-Quantum Cryptography is simply a necessity. In 2023, the Quantum-Safe Cryptography programme was launched to support (central) government organisations in this transition.

The programme does not stand on its own. In recent years, various public–private initiatives have been launched to develop knowledge and gain experience. HAPKIDO is a good example of this. Bringing together expertise from government, academia, and industry is essential to shape this transition in a careful and practical manner.

I already notice that the topic of quantum-safe cryptography is being discussed more frequently in board rooms, but this is not yet sufficient. More attention is still needed for this topic. This transition requires insight, analysis, and preparation. In short: it requires your professional expertise. It is your work that makes clear where the risks lie and which choices are necessary.

The handbook before you provides concrete guidance for this purpose. I hope that you will use it as a tool within your own organisation and in collaboration with partners. This transition requires joint effort. Only together we can ensure a digitally secure foundation for the future.

Art de Blaauw
Director CIO Rijk

Ministry of the Interior and Kingdom Relations

Executive Summary

The development of quantum computing poses a fundamental threat to today's digital trust services. Public Key Infrastructures (PKIs)—which form the backbone for authentication, integrity, confidentiality, and non-repudiation across government, finance, telecom, healthcare, and other sectors—depend on cryptographic protection that will no longer hold once a cryptographically relevant quantum computer becomes a reality. This handbook provides organisations, policymakers, and PKI operators with a consolidated, research-based guide for navigating the transition towards quantum-safe PKIs, based on the research done in the HAPKIDO consortium.

A quantum powered adversary introduces two primary risks. The store-now-decrypt-later threat is already active: encrypted data with long confidentiality requirements can be harvested today and decrypted later. The real-time access threat—expected once quantum capabilities mature—would undermine digital signatures, allow impersonation, and disrupt critical digital processes. The societal impact assessments conducted in HAPKIDO show that compromised PKI-dependent services could trigger cascading failures: from social unrest in government services to economic instability in financial systems and communication breakdowns in telecom infrastructures.

Global policy developments underscore the urgency of the transition, but execution varies significantly. The U.S. mandates strict migration timelines; the EU coordinates a phased roadmap; the Netherlands advances through a national quantum-safe communication programme; and the UK emphasises risk-based guidance. Meanwhile, Asia pursues cryptographic sovereignty with independent PQC competitions and standards. The need for hybrid solutions remains contested, centring on whether the additional security benefits of a two-layered approach justify the increased implementation effort. Despite these differences, three recurring themes emerge across the various policies: universal recognition of the quantum threat, reliance on the NIST PQC process, and a shared emphasis on early cryptographic inventory and agility.

Transitioning to quantum-safe PKI is complex: there are many components, interactions, and dynamics to consider. Transition challenges include interdependencies, uneven sector urgency, limited availability of certified hardware and software and in-house expertise, and unclear governance responsibilities—especially in decentralised ecosystems. Many standards supporting hybrid cryptography remain under development, and supporting infrastructure (*e.g.*, HSMs, crypto-libraries, certificate formats) is still maturing. Nevertheless, recent progress—such as the finalisation of several NIST algorithms and emerging hybrid certificate formats—enables organisations to begin gaining practical migration experience.

To support transition planning, HAPKIDO introduces a five-stage growth model for quantum-safe transition, spanning awareness, assessment, preparation, implementation, and ecosystem-wide adaptation. Each stage requires alignment across intra-organisational (individual organisations), inter-organisational (government agencies, sectors), and ecosystem (regulatory and international standard bodies) levels. Facilitating collective action and establishing clear decision-making structures are essential for maintaining interoperability during the transition.

Drawing from multidisciplinary research, this handbook offers actionable guidance. Organisations should begin by conducting a quantum-vulnerability diagnosis, mapping cryptographic dependencies, and understanding business impacts. During planning, dedicated migration teams should prioritise urgent assets—particularly long-lived certificates and PKI trust anchors—and initiate early testing with PQC and hybrid solutions. Execution requires careful implementation to avoid introducing new vulnerabilities and to maintain interoperability with legacy systems. Hybrid approaches, also used for backwards compatibility, are recommended in the near-term for risk-mitigation while PQC algorithms mature. Across all phases, cryptographic agility is critical to future-proof systems.

At inter-organisational and ecosystem levels, coordinated transition plans are needed to avoid fragmentation and non-interoperable systems. Shared guidelines, testbed consortia, sector-specific migration strategies, and cross-organisational communication channels will help align timelines, dependencies, and technical standards. Policymakers play a key role in shaping

mandates, promoting interoperability, and guiding the development of supporting infrastructure. A call to action is given to improve technical standards and implementations necessary to complete this transition.

In summary, the shift to quantum-safe PKIs represents a strategic, multi-actor transformation rather than a simple technical upgrade. While the exact timeline for quantum computing remains uncertain, its impact is inevitable, and long-term confidentiality is already at risk. Organisations must therefore move decisively from awareness to action and adopt continuous cryptographic agility. PKI being the foundation of most cryptography, deserves early attention. This handbook, based on scientific analysis and practical application, provides the analytical foundation and practical tools needed to navigate this transition of PKI responsibly and effectively.

1. Introduction

The HAPKIDO project[1] (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations) is a research initiative aimed at guiding digital society's transition towards quantum-safe Public Key Infrastructures (QS PKIs). As advances in quantum computing threaten to break current cryptographic systems, HAPKIDO focuses on developing the organisational, technical, and governance foundations needed to secure digital trust even after the emergence of a cryptographically relevant quantum computer. The project brings together multidisciplinary expertise to design migration architectures, hybrid PKI models, and transition tools that help organisations prepare for and adopt quantum-safe solutions.

HAPKIDO places strong emphasis on understanding the societal impact of the quantum threat. Many currently deployed secure messaging and digital signature standards, which are supported by PKI backbones, are expected to become breakable within the next decades. As a result, sectors that rely heavily on PKI—such as government services, banking, healthcare and telecom—face significant risks to privacy, security, and the continuity of critical digital services. Research conducted within the HAPKIDO project on the societal impact of this threat highlights the need for early preparation, cross-organisation collaboration, and informed decision-making to ensure a smooth and secure transition to quantum-safe trust services.

This handbook connects the contributions and outcomes of the research conducted by HAPKIDO's multidisciplinary streams of work (work packages) into one book that helps navigating the complexities of transition towards QS PKI. This handbook has two main goals: 1) to **educate** and create **awareness** on topics related to the transition to QS PKIs; and 2) to support discussion of next steps through **actionable insights**.

This handbook is written with a broad audience in mind. Nevertheless, specific groups may benefit more from each of this handbook's goals.

GOAL 1: EDUCATION AND AWARENESS. On education and awareness, we identify organisations in general as the main concerned group, in particular their **executive leadership** (*e.g.*, Chief Information Officer, Chief Information Security Officer, Data Protection Officer, among others). Faced with such a novel and pervasive threat, this group is confronted with a dilemma: having to decide between pioneering in the transition in order to align efforts to regulatory requirements and suggested timelines, but potentially transition before best practices are solidified; or transitioning later to leverage from lessons learned by the community, however having to devise potentially costlier internal transition plans with more stringent timelines to avoid compromising digital services. Executive leadership can use this handbook to understand the flavours of quantum threat, how they impact business processes, how to conduct risk assessments, and which factors influence timelines and indirectly the costs[2] of a transition. They can use this handbook to make informed decisions.

GOAL 2: ACTIONABLE INSIGHTS. The actionable insights offered in this handbook are tailored to support two other groups: **PKI operators and architects**, as well as sector regulators. The first group is directly concerned as the typical owners of the assets affected by quantum threats. PKI operators and architects are also well positioned to inventorise cryptographic assets. They may leverage from the recommendations and insights arising from our research to, for example, define deprecation timelines, assess the need for early revocation, and devise migration roadmaps. Sector regulators, on the other hand, will play a central role avoiding fragmentation at inter-organisational PKIs and mandating migration deadlines to ensure a timely sector-wide threat mitigation. This group will need to account for the role that overarching regulations will play within the

1 HAPKIDO: for quantum-safe Public Key Infrastructures - HAPKIDO (https://hapkido.tno.nl/)

2 There is currently no consensus or framework regarding the cost of migration to QS PKI. Costs can be elaborated using experience of migrating away from deprecated technology or migrating to a new PKI vendor.

constraints of their sector, considering themes of interoperability, alignment of hybrid policies, and orchestration. We invite sector regulators[3] to appraise the insights offered by this handbook.

While organisational needs and constraints vary across sectors, a number of *no-regrets steps* exist that provide clear guidance for the transition towards quantum-safe cryptographic systems. A key reference literature in this topic is The PQC Migration Handbook (Amadori, et al., 2024), authored by TNO, CWI, and AIVD (the first two also being partners in the HAPKIDO project). The present HAPKIDO Handbook does not replace the PQC Migration Handbook, instead it provides tools that support its application to the specific case of PKI migration.

We leverage on multidisciplinary research done in HAPKIDO to elaborate on the proposed migration phases as follows:

Table 1: Handbook outline

Migration Phase	Addressed section in PQC Migration Handbook	Elaborated further in the present document	Topics
Phase 1: Diagnosis	2.2, 1.5, 5	2, 3	Quantum Threat, Regulations and policies
Phase 2: Planning	3.2	4, 5	Transition challenges and growth model
Phase 3: Execution	4	6, 7	Migrating primitives and protocols

Phase 1: Perform a Quantum-Vulnerability Diagnosis, which includes a number of "no-regret" moves that will enhance an organisation's cyber resilience regardless of the quantum threat. Examples include making an inventory of all cryptographic assets. This means identifying every system, application, and process that uses public-key cryptography. This is often the most challenging step, as cryptographic dependencies can be hidden deep within legacy systems or third-party products.

Phase 2: Plan for migration to PQC. It is important to form a dedicated team to oversee the migration and to ensure that all business processes are in place to facilitate a smooth transition. Pay attention to so-called urgent adopters: organisations that need to start the PQC migration as soon as possible because the impact of a breach in cryptography within the coming decades would be unacceptable. Moreover, it provides tools to assess an organisation's readiness and maturity for a PQC migration.

Phase 3: Execution step of the PQC migration. During this phase, organisations must be careful not to introduce new vulnerabilities. The Revised PQC Migration handbook provides guidance on how to carry out the migration for different types of cryptography and the various strategies developed during the planning phase. Moreover, cryptography will continue to evolve in the future. For instance, new algorithms or vulnerabilities may be discovered and advancements in cryptanalysis may warrant larger cryptographic keys. Therefore, it is important to establish or maintain a form of cryptographic agility. Cryptographic agility enables organisations to quickly modify or replace deployed cryptographic primitives without significantly disrupting organisational processes. This is especially important when cryptographic protocol improvements or new vulnerabilities are

3 We name the regulators for four critical sectors in the Netherlands: *De Nederlandsche Bank* (DNB) for the financial sector, *Rijksinspectie Digitale Infrastructuur* (RDI) for telecommunications, Logius, as the digital government service agency for the Dutch government, and *Inspectie Gezondheidszorg en Jeugd* (IGJ) for the digital healthcare services.

identified. The Revised PQC Migration handbook offers direction on how cryptographic agility can be integrated into existing change management processes.

By raising awareness, this handbook aims to foster dialogue among industry and policymakers, and to support stakeholders navigate organisational complexity, sector and system constraints, and governance challenges that are helpful to address in support to essential migration efforts.

1.1 Context

Cryptography provides the mathematical backbone of digital trust. Typical questions which cryptography addresses are: 1) How can we be sure that we are communicating with the bank when trying to transfer money? 2) How can we be sure that the transaction is not altered in transit? 3) How can we be sure that others cannot see how much money is transferred, and to who? Cryptography is generally used to ensure confidentiality, integrity, authentication and non-repudiation of data. Confidentiality means that information can only be accessed by those it was meant for. Integrity means that information is accurate, complete and trustworthy and cannot be altered by unauthorised parties. Authentication ensures information comes from the expected party. Finally, non-repudiation refers to the inability to deny having performed certain digital actions and ensures accountability in the digital domain.

Authentication, which ensures that in this example we have connected to the real bank's server, not some imposter's, can be enforced using digital signatures. The same digital signature methods can be used to digitally sign documents to attest to the validity of such documents, for example an ownership transfer of a house or a loan. Oftentimes, it is also important to digitally attest the time at which an event happened in a way that cannot be altered. These are examples when non-repudiation can be enforced through digital signatures.

If we can trust we are communicating with the right party, confidentiality of our conversation can be ensured through encryption. This applies to all kinds of data transfers, such as transaction information, health records and criminal records. In almost all cases where encryption is applied – including the internet - public-key cryptography is required. In public-key cryptography, each party has a private key and a public key. The private key must remain private at all costs, otherwise anyone can learn the contents of the conversation. The public key can be shared publicly without any negative consequences. In fact, the public key will need to be sent around in order to start a secure communication channel. This process is called a key exchange, where the goal is for two parties two obtain the same encryption key without anyone else learning anything about it, even if they were listening to all the messages during the exchange. This key is then used to encrypt the messages that the two parties want to send to each other. For an eavesdropper observing the network, the messages that the two parties send to each other will not be useful.

With digital signatures, there is also a public key and a private key. The private key is used to create a digital signature, and the public key is used to verify that the digital signature is valid. The main challenge with public keys is, how to verify that a given public key belongs to a specific entity?

1.1.1 PKI Services and Standards

Certificates are the digital documents that are used in a Public Key Infrastructure (PKI) to bind public-keys (*e.g.*, for digital signature schemes, and public-key encryption schemes) to entities. Certificates contain information such as the identity of its owner (a person, organisation, or other types of legal/virtual entities), the issuer of the certificate, validity period, and the public key. Certificates are signed by their issuer, and so ultimately provide authenticity of public-keys.

PKIs come in many flavours, but for hierarchical PKIs we can identify a generic set of components that can be used to represent PKIs.

An overview of such components and their technical interdependencies can be found in HAPKIDO deliverable 6.1 (Amadori, Marcus, & Spagnuelo, 2024).

A minimal PKI structure consists of just one root Certificate Authority (CA). In this minimal example, the root CA is responsible for all PKI services, including the processing of Certificate Signing Requests (CSRs), issuing and re-issuing certificates, and tracking revocation information in case a certificate is revoked before its natural expiration date. Some of these responsibilities can, for example, be delegated to other intermediate CAs that process CSRs and issue certificates, a registration authority (RA) that validates information about the certificate requestor, or a validation authority (VA) that communicates revocation information to PKI users.

A deeper analysis of common PKI services is provided in HAPKIDO deliverable 6.2 (Marcus & Amadori, 2025).

1.1.2 PKI Migration and Interdependencies

With the approaching arrival of the quantum computer there is, however, an eminent threat to PKIs and digital trust. Such computers can potentially solve hard mathematical problems that underpin public-key cryptography. While classical computers cannot reasonably break these systems, a sufficiently powerful quantum computer could compromise them within hours or days, undermining core functions like digital signatures, secure key exchanges, and encrypted communications. This risk is amplified by the "store-now-decrypt-later" scenario, where adversaries collect encrypted data today to decrypt once a cryptographically relevant quantum computer becomes available. Although building such machines remains challenging, experts agree they are feasible, making the transition to quantum-safe cryptography (interchangeably called Post-Quantum Cryptography, or PQC, in this book) an urgent priority.

For a technical migration, several concepts are important. The first one is the notion of *hybrid* solutions—as currently recommended by European institutions—, which combine both classical and post-quantum cryptography to ensure that if one is later found vulnerable, the other remains to ensure security. The notion of security hierarchies is also relevant, which states that Certificate Authorities that are higher up the hierarchy should have stronger cryptographic controls. Traditionally, this meant that the key length should be equal or larger, but this is less trivial to interpret with regards to post-quantum cryptography, since there are various different algorithms and different modes (purely post-quantum or hybrid) to consider. This makes the comparison more complex. Apart from such policy requirements, there are other dependencies that are important to consider with regards to migration to post-quantum and hybrid PKIs, including but not limited to standards - both sector-specific as well as national and international - as well as software and hardware availability, hardware limitations and externally managed services.

These topics are covered in greater detail in HAPKIDO deliverable 6.2 (Marcus & Amadori, 2025).

Different PKIs are likely to follow different migration routes due to several reasons, we highlight:

- *Sector-specific needs*: policies for specific sectors will differ and have varying timelines. For example, DORA[4] is the leading regulation for the financial industry. Other sectors follow their own regulations, which will need to be updated to include PQC migration timelines and tailored guidance.
- *Tailored migration plan*: PKIs have different structures and can offer different PKI services. Sometimes certain PKI services are outsourced, leading to a strong dependency for the migration. It is therefore necessary for each PKI to understand how their services depend on external factors and how they can influence the migration timelines.
- *Lack of streamlined migration*: In many organisations, technology updates are structured through change management. Specifically for PKIs, life cycle management processes can be utilised to migrate certificates. Migration to a post-quantum PKI can often be integrated into such life cycle management processes, but not always. For example, CA migration is often done by running the new generation in parallel with the old and only issuing new certificates on the new generation CA, resulting in a natural retirement of the old CA. However, this strategy is not always possible.
- *Physical constraints*: The hardware that is used within PKIs varies. For ecosystems that use PKI to support embedded hardware, such as smartcards, it is not yet clear what the post-quantum alternative should be. Most of the standardised algorithms are too demanding in terms of memory usage and performance to work on small embedded systems, so new hardware and appropriate algorithms need to be selected, and the physical hardware needs to be re-issued.

4 Regulation - 2022/2554 - EN - DORA - EUR-Lex (https://eur-lex.europa.eu/eli/reg/2022/2554/oj)

2. Understanding Quantum Threats

2.1 Developments in Quantum Computing

Quantum computing marks a major shift from classical computing, utilising qubits that can exist in superposition and entanglement, that have the potential to enable powerful new ways to store and process information, although —currently— still fragile and prone to information decay (Gidney & Ekerå, 2021) (Smart, 2016) (Joseph, et al., 2022).

Quantum algorithms built on these principles may potentially accelerate, by a significant amount, problem-solving for certain fields (World Economic Forum, 2022b). The technology has made steady progress, with engineering advances in scaling quantum hardware (National Academies of Sciences & Medicine, 2019). Industry and academic institutions are working to build more stable processors, increasing qubit counts and improving quality and connectivity (World Economic Forum, 2022a).

Recent demonstrations show promising lab results that quantum devices can perform tasks considered difficult for classical supercomputers (Kim, et al., 2023). So far, these tasks are contrived, but this development shows the potential for transformative impact, possibly in materials science, drug discovery, and optimisation. While the impact to these fields remains speculative, quantum computing poses a well-understood threat to current encryption systems (Mavroeidis, Vishi, D., & Jøsang, 2018).

The arrival of a "cryptographically relevant quantum computer" (CRQC), known as Q-day, will break currently used (public-key) cryptography. Though the timeline is uncertain (Alagic, et al., 2025), experts generally agree on the feasibility of such a machine. Substantial scientific and engineering obstacles remain, like error-correction, quantum decoherence and qubit interconnectivity, before a universally programmable CRQC becomes feasible (Gambetta, Chow, & Steffen, 2017), and any prediction remains an educated guess, but the optimistic voices suggest Q-day could occur within 10–20 years (Mosca & Piani, 2024).

Despite the uncertainties, preparing for the quantum transition remains essential, as an undetected compromise of cryptographic foundations would have profound consequences across our digital ecosystems. Because digital infrastructures evolve, and cryptography is deeply embedded in long-lived physical and operational systems, early action is critical. The quantum threat is well understood, and with timely preparation and coordinated effort, organisations can significantly reduce the likelihood that these risks will ever materialise.

2.1.1 Background on Quantum Algorithms

While the engineering of quantum computers has a relatively younger history, research on quantum algorithms has matured building on the theoretical foundations of quantum. Researchers have developed algorithms that exploit quantum properties to challenge existing cryptographic systems. Grover's algorithm accelerates brute-force attacks on symmetric cryptography like AES by theoretically halving the key space (Grover, 1996), although practical effect is predicted to be significantly lower (ETSI, 2025) (Bootsma & Vries, 2024). To counter this, doubling key lengths is generally considered sufficient for protection against CRQCs.

Public-key infrastructures based on asymmetric cryptography—such as RSA and Elliptic Curve Cryptography (ECC)—face greater risks. RSA relies on the difficulty of factoring large numbers, and ECC on solving the elliptic curve discrete logarithm problem, both of which are computationally hard for classical machines (Smart, 2016) (National Academies of Sciences & Medicine, 2019).

Shor's algorithm revolutionised quantum computing by enabling polynomial-time solutions to these problems (National Academies of Sciences & Medicine, 2019), leveraging quantum superposition and interference (Gidney & Ekerå, 2021). A CRQC could use Shor's algorithm to break RSA and ECC within hours or days (Joseph, et al., 2022). More specifically, the availability of a CRQC capable of executing Shor's algorithm would undermine core cryptographic functions—digital signatures,

secure key exchanges, and encrypted data—threatening the integrity of digital communications (Mulholland, Mosca, & Braun, 2017) (Grimes, 2019).

Public Key Infrastructure (PKI) as the trust mechanism used to couple identities to cryptographic keys, extensively uses asymmetric cryptography, and will therefore be heavily affected. The security of PKIs largely relies on the security of digital signatures. Almost all deployed PKIs make use of classical digital signatures, which could be forged in a short amount of time by an adversary with access to a CRQC. Although building such a machine remains a monumental challenge, Shor's algorithm provides a clear blueprint for its potential impact, making quantum-resistant cryptography an urgent priority.

2.2 Identifying the Quantum Threat Scenarios for Digital Infrastructures that use PKI

2.2.1 Quantum Threats: Store Now, Decrypt Later and Real-Time Access

The threat posed by a future quantum computer is not monolithic (Amadori, et al., 2024). It manifests in different ways, with some risks being immediate and others crystallising only when the machine becomes operational (Joseph, et al., 2022). Two primary threat scenarios dominate the landscape: 'store-now-decrypt-later' and 'real-time access.' Table 2 provides an overview.

Table 2: Comparison of Quantum Threat Scenarios

Threat Type	Timeline	Primary Impact	Affected Security Pillar	Mitigation Urgency
Store-Now-Decrypt-Later (SNDL)	Already Active	Data Confidentiality Loss	Confidentiality	High (immediate)
Real-Time Access	Post Q-Day	Trust, System Integrity & Availability	Confidentiality, integrity and availability	Critical (pre Q-Day)

1. Store-Now-Decrypt-Later (SNDL):

The SNDL threat is an immediate and covert risk posed by quantum computing (Lindsay, 2020) (Amadori, et al., 2024). Adversaries—including state actors and cybercriminals—are believed to be collecting encrypted data today with the intention of decrypting it in the future using a cryptographically relevant quantum computer. Shor's algorithm would allow them to break current public-key encryption retrospectively (Amadori, et al., 2024). This threat is especially critical for data with long-term confidentiality needs, such as state secrets, intellectual property, personal data, and legal or financial agreements. Since the value of this data persists well beyond the time it may take to develop a powerful quantum computer, this threat is already active. The urgency lies not in when the quantum computer will be built, but in how long the data must remain secure. SNDL primarily undermines confidentiality, making it a silent but ongoing risk.

2. Real-Time Access:

Once adversaries gain operational access to a cryptographically relevant quantum computer, the threat escalates to real-time attacks with immediate consequences. This scenario affects all three pillars of information security: confidentiality, integrity, and availability. Communications could be intercepted and decrypted, digital signatures forged, and identities impersonated—compromising trust across financial systems, government operations, and software distribution. The ability to disrupt secure protocols could lead to denial-of-service attacks or force organisations to shut down PKI-dependent services, risking widespread digital disruption. Critical services may face the dilemma of operating with compromised trust or halting essential functions. Unlike SNDL's passive data theft, real-time access represents a scenario with direct operational impact on digital infrastructure.

2.3 A method for Assessing the Risks of Quantum Computing on PKIs

Recognising the complexity and far-reaching nature of the quantum threat, the HAPKIDO project developed a structured methodology for assessing its societal risks. This Societal Risk Assessment (SRA) method provides a framework for organisations to move beyond purely technical analysis and understand the broader societal impact that would occur if the PKI they rely on were to fail. Previous research on risk assessment methods (Ma, Colon, Dera, Rashidi, & Garg, 2021) (Aven, 2017) (Wadhwa, Barnard-Wills, & Wright, 2014) was consulted to structure the steps in the SRA Method.

The SRA method is designed to be usable by any party involved in the PKI ecosystem, from a policy authority to an end-user organisation. It guides the assessor through a systematic process to identify vulnerabilities, map them to critical assets, and evaluate the resulting impact on both the organisation and society at large. Figure 1 provides an overview of the method.

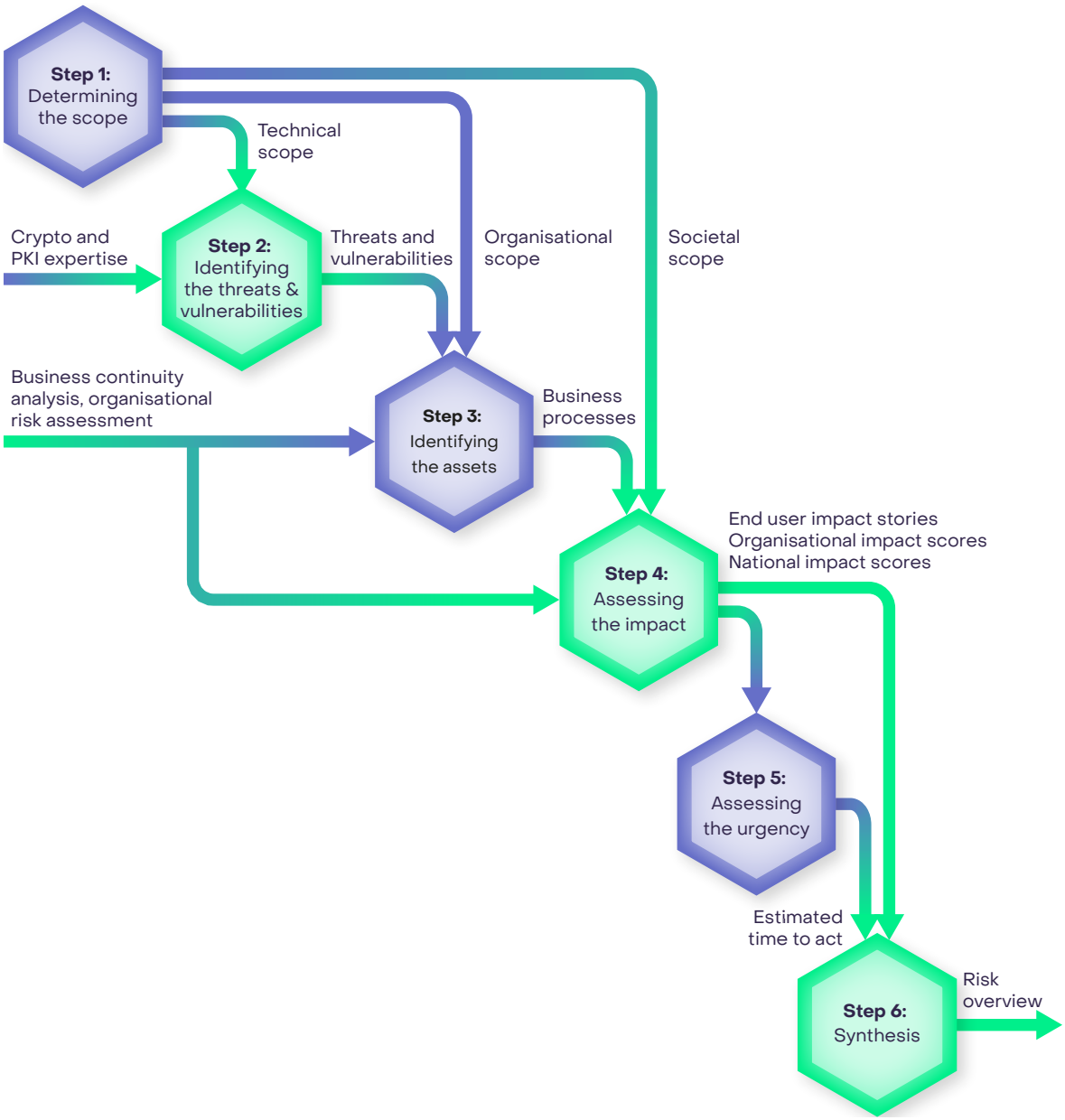

Figure 1: Overview of the SRA method

The method consists of six core steps:
Step 1: Determine Scope: The assessment begins by clearly defining three scopes:
- Technological Scope: Delineating the specific technologies under review (*e.g.*, asymmetric cryptography in PKI).
- Organisational Scope: Defining the boundaries of the assessing organisation itself.
- Societal Influence Scope: Identifying the broader societal sphere that the organisation's services and operations affect.

Step 2: Identify Threats: This step focuses on the "what to defend against." It involves identifying the relevant quantum threats (like SNDL and real-time access) and the specific vulnerabilities they exploit (*e.g.*, reliance on RSA and ECC).

Step 3: Identify Assets: Moving to "what to defend," this step identifies the critical assets that rely on the vulnerable cryptography. The SRA defines three types of assets:
- *Business Processes*: Core operational activities within the organisation.
- *Applications*: The specific software and systems that use PKI.
- *Services*: The end-user or societal functions enabled by the applications.

Step 4: Assess Impact: This is the core of the societal risk analysis. The impact of the threats materialising against the identified assets is assessed from two perspectives:
- *Organisational Impact*: Using categories like financial, reputational, and operational damage to the organisation itself.
- *Societal Impact*: This is assessed from an end-user perspective and, crucially, from a national security perspective, using a framework that includes categories like territorial security, economic security, and social/political stability.

Step 5: Assess Urgency: This step addresses the uncertainty of the timeline. It uses a model inspired by Mosca's Theorem (X+Y < Z), which considers the shelf-life of data (X), the time needed to migrate to a quantum-safe solution (Y), and the estimated time until the threat materialises (Z) (Mosca & Mulholland, A Methodology for Quantum Risk Assessment, 2017). This helps prioritise risks based on how quickly they need to be addressed.

Step 6: Synthesise: The final step combines the impact and urgency assessments to create a prioritised overview of the societal risks. This provides a clear picture of which business processes and services pose the greatest risk and require the most immediate attention.
By systematically walking through these steps, the SRA method transforms an abstract technological threat into a concrete set of identifiable and prioritised societal risks, providing a crucial foundation for informed decision-making. The next part of this chapter shows the results of the application of the SRA method.

The evaluation of the SRA method can be found in HAPKIDO deliverable 1.1 (Klunder, Bharosa, Meijaard, & Klaver, 2022).

2.3.1 Application of the Societal Risk Assessment Method in Government, Banking, and Telecom

To move from a theoretical framework to a practical understanding of the quantum threat, the HAPKIDO project applied the Societal Risk Assessment (SRA) method to three critical sectors in the Netherlands: Government, Banking, and Telecom. Through workshops with experts from each sector, the SRA was used to identify key PKI-dependent processes and trace the potential societal fallout from their compromise.

The application of the SRA method yields insights into the potential societal impact of a quantum attack. The findings reveal an interconnected digital ecosystem where a failure of trust in one area can trigger cascading failures across society. Please note that this chapter contains a summary of the impact assessment.

For a more detailed description, readers are advised to read the underlying HAPKIDO deliverable 1.2 (Meijaard, Spagnuelo, & Bharosa, 2023).

Government Sector

The Dutch government relies heavily on *PKIoverheid* for secure digital interactions (Kong, Janssen, & Bharosa, 2022). Key processes include access control via PKI-enabled passes (*e.g.*, *Defensiepas* for military and the UZI-pas for healthcare), citizen services through DigiD, and business-to-government communications using systems like *eHerkenning* for digital identities and Digipoort for legally binding digital signatures. A quantum attack compromising these systems could disrupt public service delivery, causing widespread social unrest. The failure of DigiD would block access to essential services like healthcare and taxation. Compromised professional certificates could enable fraud, undermining legal and financial trust. Additionally, forged military access or decrypted sensitive communications pose direct threats to national security.

Banking Sector

Digital trust is foundational to banking, with PKI securing online banking, card transactions, international transfers (*e.g.*, SWIFT), and PSD2 services (the open banking framework that allows third-party applications to interface with bank services). The SRA revealed that a quantum attack could trigger economic collapse by forcing banks to suspend digital operations or revert to offline protocols. This disruption could cascade into a broader financial crisis (Grimes, 2019). Even without total collapse, forged transactions would erode financial trust, leading to individual and institutional losses. The failure of digital payment systems could cause a run on cash, depleting ATMs and disrupting access to basic necessities, resulting in severe social instability.

Telecom Sector

Telecom operators secure network services, securing the identity and traffic on wired and mobile networks (*e.g.*, 4G/5G) for both public and emergency services, web hosting, and the remote management of devices (*e.g.*, modems, routers) using PKI. A quantum breach would undermine trusted communication, allowing rampant eavesdropping and impersonation. While connectivity might remain, its integrity would collapse, affecting emergency services and business operations. Compromising Customer Premise Equipment (CPE) could enable mass hijacking of internet traffic, forming botnets or intercepting data. The loss of secure web services and the shift to manual maintenance would degrade service quality and inflate operational costs, straining both providers and users.

This impact assessment is by no means complete when considering the amount and the variety of business processes in each of the three sectors. Nonetheless, the workshops with representatives of each sector, conducted during the HAPKIDO project, underline the importance of making a business impact analysis that focuses on the core business processes that rely on PKIs.

Table 3 provides a high-level overview across the three sectors in the scope of HAPKIDO.

Table 3: Sectoral Impact Summary from SRA Application

Sector	Critical PKI Dependencies	High Risk Scenario	Estimated Societal Impact Level
Government	*PKIoverheid*, DigiD, UZI-pas	Erosion of trust in the national public identity system (DigID)	Extreme - Social unrest
Banking	Online banking, SWIFT, PSD2	Transaction forgery	Extreme - Economic collapse
Telecom	TLS, CPE management, 5G	Certificate forgery	High - Communication breakdown

Across all three sectors, the compounded effect is what is most alarming, and it is alarming at every level. For individuals, the fundamental mechanisms of digital life would cease to function. For businesses, supply chains would halt and digital commerce would become impossible. At the national and international level, the very systems that support global finance, diplomacy, and defence would be rendered untrustworthy, creating a crisis of unprecedented scale.

2.3.2 Generalisability: Impact for Other Sectors that Depend on PKI

The HAPKIDO project's findings, though focused on Government, Banking, and Telecom, are moderately generalisable to other sectors due to the shared architecture and cryptographic standards of public key infrastructures. The core vulnerabilities—disruption of services, loss of confidentiality, and erosion of trust—apply broadly (Yunakovsky, et al., 2021). In healthcare, PKI secures electronic health records and provider communications; a quantum attack could expose sensitive data or alter medical records with life-threatening consequences. In energy and utilities, PKI protects industrial control systems; forged certificates could allow attackers to manipulate power grids or water supplies, threatening public safety (ENISA, 2022). Manufacturing and supply chains rely on PKI for secure communications and software updates; a breach could disrupt operations or compromise industrial machinery (World Economic Forum, 2022b).

Other vulnerable sectors include automotive and e-commerce. Connected vehicles use PKI for secure communications and software authentication; a quantum-enabled attacker could take control of critical vehicle functions, with long vehicle lifespans compounding the urgency for quantum-safe transitions (Lohmiller, Kaniewski, Menth, & Heer, 2025). E-commerce depends on TLS, which uses PKI to secure payments and protect customer data; a real-time quantum attack could halt online shopping entirely. Ultimately, any sector that relies on secure internet communication, user or device authentication, or long-term data protection faces systemic risk from quantum threats. The collapse of PKI would undermine the digital trust that underpins the global economy (World Economic Forum, 2022b).

Digital infrastructures reliant on public key cryptography face two quantum threats: the immediate risk of "store-now-decrypt-later" attacks and the future danger of real-time disruptions to system integrity and availability. Using the SRA method developed in the HAPKIDO project, these risks are framed not as abstract technical failures but as tangible threats to essential services. The findings reveal the potential for systemic collapse across government, banking, and telecom sectors, with cascading effects that could destabilise economies and erode public trust. Given the uncertainty surrounding the arrival of a cryptographically relevant quantum computer, this chapter emphasises that understanding the scale and societal implications of the quantum threat is the essential foundation for action.

3. Recent Policy Developments

The growing realisation that quantum computers could undermine current public key infrastructures (PKIs) has led to increased international attention, especially due to the potential disruption to critical sectors like government services, banking, and telecommunications. In response, governments and standardisation bodies have shifted from academic research to active policy-making, focusing on the adoption of Post-Quantum Cryptography (PQC). PQC standards are nearing finalisation, and a hybrid cryptographic approach—combining classical and quantum-resistant algorithms—is being promoted to enhance security and ensure interoperability during the transition.

This momentum has led to a surge in policy initiatives aimed at managing the quantum threat. These policies are not just technical guidelines, but strategic frameworks designed to coordinate efforts across public and private sectors, safeguard national security, and maintain economic stability. The chapter proceeds to examine key policy developments across various regions, including the U.S., EU, UK, Netherlands, and Asia, highlighting both shared strategies and regional differences in their approach to the quantum transition. Table 4 provides an overview of the recent PQC policy developments.

Table 4: Global PQC Policy Approaches Comparison

Region/Country	Policy Type	Implementation Timeline	Key Characteristics
United States	Mandatory (NSM-10)	2030-2033	Top-down, federal focus
European Union	Coordinated roadmap	2026-2035	Member state coordination
Netherlands	National program (QvC Rijk), supplemented with a migration handbook	Following EU timeline	Public-private partnership
United Kingdom	Risk-based guidance	No fixed timeline	Pragmatic, technically focused
South Korea	National competition	2035	Cryptographic sovereignty
China	National standards	Undisclosed	Technological independence

The goal of this chapter is not to provide a complete and in-depth overview of all developments. Instead, it illustrates the variety of policy directions across the globe.

3.1 United States

The U.S. government's response to the quantum threat is marked by a structured, top-down approach with clear mandates and timelines, and a strong emphasis on leveraging the expertise of the National Institute of Standards and Technology (NIST) (Alagic, et al., 2025). This began with Executive Order 14028[5] in May 2021 and was followed by National Security Memorandum 10 (NSM-10) in 2022[6], which formally recognised quantum computing as a national security risk. NSM-10 required federal agencies to inventory cryptographic systems and prepare for migration using NIST's forthcoming Post-Quantum Cryptography (PQC) standards. These directives—shifting from a broad cybersecurity focus to a specific quantum threat in the spam of one year—underscore the urgency and strategic importance of transitioning to quantum-safe systems.

Legislative backing came with the Quantum Computing Cybersecurity Preparedness Act, signed into law in December 2022, which codified NSM-10's requirements (117th Congress USA, 2022). It tasked the Office of Management and Budget (OMB) with overseeing the migration and required agencies to develop migration plans within a year of NIST's PQC standard release. In July 2024, the OMB, in collaboration with agencies like CISA, published a detailed strategy and cost estimates for the transition (Executive Office of the President of the United States, 2024). Additionally, the NSA updated its Commercial National Security Algorithm Suite (CNSA 2.0), which specifies the cryptographic algorithms required for protecting national security systems. CNSA 2.0 sets deadlines of 2030 and 2033 for the mandatory use of specific, NIST-approved PQC algorithms, creating a clear and non-negotiable timeline for the defence and intelligence communities.

Together, these actions reflect a comprehensive and mandatory U.S. policy framework focused on securing federal systems first, thereby setting a precedent for the private sector and international partners.

3.2 European Union

The European Union has pursued a more coordinative and recommendation-based policy approach, reflecting the political structure of its 27 member states. The goal is to create a harmonised transition across the Union, avoiding a fragmented digital single market. The European Union Agency for Cybersecurity (ENISA) play a central role by publishing reports and guidelines that raise awareness, assess current cryptographic practices, and offer strategic recommendations for both public and private sectors.

In 2025, the European Commission, together with member states, introduced a coordinated roadmap for transitioning Europe's digital infrastructure to PQC (European Commission, 2025). This roadmap was developed by the NIS Cooperation Group in response to the Commission's recommendation in April 2024, reflecting a growing urgency around quantum threats. The roadmap is politically backed and designed to ensure synchronised action across the EU, emphasising PQC as a critical defence against future quantum-enabled cyberattacks.

---

5 Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/)

6 National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/)

The roadmap outlines key milestones: by the end of 2026, member states should begin national strategies and migration 'first steps' through assessments, awareness campaigns, and cryptographic inventories; by 2030, high-risk systems—such as utilities, telecom, finance, and government—must be secured with PQC; and by 2035, the transition should be completed for most systems, including legacy and lower-risk ones. This phased timeline balances urgency with practical feasibility, ensuring that Europe's digital infrastructure becomes quantum-safe in a structured manner.

In the beginning of 2026, the European Commission also proposed amendments to the Network and Information Security Directive (NIS2)[7]. Among others, the proposal adds a new article requiring Member States to adopt policies within their national cybersecurity strategies *"for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies."* These amendments, if approved, are targeted to enter in force by 2027, and will affect medium and large-sized organisations active in critical sectors such as energy, transport, banking and financial services, healthcare, digital infrastructures in general, among others.

A notable feature of the EU's strategy is its emphasis on hybrid architectures, which combine classical and quantum-resistant algorithms. Chapter 6 provides more elaboration on hybrid architectures.

3.3 Netherlands

The Netherlands has taken a proactive national approach. The CWI (national research institute for mathematics and computer science), together with the General Intelligence and Security Service (AIVD) and TNO (the Netherlands Organisation for Applied Scientific Research), published The PQC Migration Handbook (Amadori, et al., 2024). This handbook provides numerous national and international organisations with concrete, actionable guidance on how to diagnose their quantum vulnerability, plan their migration, and execute the transition. The approach emphasises:

- *Public-private partnerships*: A strong focus on collaboration between government and industry, recognising that the threat affects all sectors.
- *A risk-based approach*: Guidance for organisations to identify themselves as "urgent adopters" based on the sensitivity and shelf-life of their data, allowing for a prioritised migration.
- *Conservative algorithm choices*: Like other European agencies, the PQC handbook (recommended by the NCSC-NL and reflected in their TLS recommendations) recommends conservative parameter sets for the new NIST standards, promotes hybrid algorithm use, and supports the standardisation of additional, more conservative algorithms.

Additionally, the Dutch government launched the "Quantumveilige Cryptografie (QvC) Rijk" program in 2023[8]. This national program is specifically designed to coordinate the PQC migration across all central government ministries and their associated agencies. The QvC Rijk program aims to

7 Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act | Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act)

8 Quantumveilige cryptografie Quantumveilige cryptografie - Digitale Overheid (https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/)

centralise expertise, develop a unified migration strategy for the national government, and ensure that all parts of the central administration move in lockstep to protect sensitive government data and communications (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025). This initiative demonstrates how a single member state can translate high-level policy recommendations into a practical, government-wide implementation strategy.

3.4 United Kingdom

The UK has adopted a risk-based policy approach, guided by its National Cyber Security Centre (NCSC-UK)[9]. The NCSC-UK has published a series of documents that provide guidance on preparing for the PQC transition (National Cyber Security Centre UK, 2024) (National Cyber Security Centre UK, 2025).

A central tenet of the UK's approach is its emphasis on standardisation. The NCSC-UK encourages organisations to only adopt algorithms that have undergone the internationally recognised standardisation processes, with reference to the NIST standards (National Cyber Security Centre UK, 2024).

The UK also maintains a cautious stance on hybrid cryptographic schemes (National Cyber Security Centre UK, 2024, p. 7). There may be multiple reasons for being cautious with hybrid schemes, including the introduction of additional complexity and overhead that come with maintaining multiple cryptographic algorithms. Therefore, the NCSC-UK recommends they should only be deployed when necessary and with a clear roadmap towards full migration to post-quantum solutions.

The UK's policy can be characterised as a measured, technically grounded approach that prioritises long-term stability and security over prescriptive, short-term mandates.

Regarding timelines, the NCSC-UK formulates milestones for 2028 (defining goals, initial plan and finishing discovery), 2031 (doing highest priority migration activities and plan revision) and 2035 (completion of migration) (National Cyber Security Centre UK, 2025). For PKI they expect a staged migration with a PQC PKI existing next to the old PKI for a period of time.

3.5 Asia

Policy developments in Asia are more varied, reflecting the diverse strategic priorities of different nations. However, a common thread is the ambition for technological leadership and cryptographic sovereignty. Several countries are not just adopting international standards but are actively developing their own.

South Korea: The Korean Post-Quantum Cryptography (KpqC) research centre launched a national PQC competition in 2021, with the winners announced in 2025, selecting two KEMs and two signature algorithms, which do not overlap with the NIST algorithms or European preferences (although some are similar) (KpqC, 2025). The plan is to transition the country's national cryptographic systems by 2035 (Burhan, Nawawi, & Kamel, 2024). This reflects a strong desire to build domestic expertise and reduce reliance on foreign technology.

China: The Chinese Association for Cryptologic Research (CACR) ran its own PQC competition, announcing winners in 2020. China's policy is driven by a national strategy to become a world leader in quantum technology. The government is heavily investing in both quantum computing

9 The National Cyber Security Centre - NCSC.GOV.UK (https://www.ncsc.gov.uk/)

and PQC research, and it is expected to mandate the use of nationally developed and approved algorithms for its domestic systems (Chinese Association for Cryptologic Research, 2020). These national efforts in Asia highlight a continuation of the trend where regions want their own cryptographic sovereignty. This is not new. China for example always used different algorithms, also for classical cryptography.

3.6 Call for Action from International Bodies

Beyond national governments, international organisations are playing a pivotal role in framing the migration to post-quantum cryptography (PQC) as a global economic and security priority, urging the private sector to take action. The World Economic Forum (WEF) has highlighted the quantum threat as a systemic risk to the global economy and called for collaboration between business and government leaders. Their policy recommendations emphasise that PQC migration should be treated as a strategic business priority requiring executive-level attention. The WEF also advocates for public-private partnerships to foster information sharing, develop common standards, and prevent new economic divides during the transition (World Economic Forum, 2022b).

Industry-led groups such as the Cloud Security Alliance (CSA) have complemented these efforts by offering practical guidance tailored to the private sector. Their resources help translate high-level policy into actionable steps for CISOs and IT leaders, focusing on cryptographic inventory, risk assessment, and supply chain engagement (Cloud Security Alliance, 2024). From a defence standpoint, NATO's Science & Technology Organisation has stressed the importance of coordinated PQC strategies among member nations to maintain secure communications and interoperability (NATO Science & Technology Organisation, 2024). Together, these international bodies reinforce the message that PQC migration is a shared global responsibility requiring coordinated, cross-sectoral action.

3.7 Key Challenges, Commonalities, and Differences

3.7.1 Challenges

One of the most significant policy challenges in the migration to post-quantum cryptography (PQC) is managing the global digital ecosystem's deep interconnectivity. No single organisation or nation can transition in isolation without risking interoperability issues, as digital infrastructure relies on a complex, international supply chain. Diverging national standards—such as the U.S. mandating one set of algorithms, the EU recommending a hybrid approach, and China adopting its own national standard—could lead to cryptographic fragmentation. This poses serious risks, especially for multinational entities like global banks, which may struggle to maintain secure and compliant operations across jurisdictions. This risk of cryptographic fragmentation is a major concern for international standards bodies like the Internet Engineering Task Force (IETF), which works to ensure the internet remains a single, interoperable network (IETF, 2024). Policymakers must therefore balance national urgency with international coordination, requiring diplomatic and technical collaboration to harmonise standards and protect the integrity of the global digital commons.

3.7.2 Commonalities

As nations around the world struggle with the quantum threat, a clear set of policy commonalities can be found, alongside distinct regional differences in approach.

- *Universal recognition of the threat*: Governments and cybersecurity agencies realise that the threat from quantum computers is real, urgent, and requires a proactive response.
- *Centrality of the NIST PQC process*: Despite some national competitions, the NIST PQC standardisation process is universally recognised as the primary source of trusted, well-vetted algorithms. Nearly all national policies reference the NIST standards as the foundation for their migration plans.

- *The 'inventory first' approach*: A common first step mandated or recommended by virtually every policy is for organisations to conduct a thorough inventory of their cryptographic assets[10]. This is seen as the essential prerequisite for any successful migration.
- *Emphasis on crypto-agility*: Policies worldwide are encouraging organisations to build systems that are "crypto-agile," meaning they can be updated with new cryptographic algorithms easily. This is a lesson learned from past, difficult cryptographic transitions.

3.7.3 Differences

Alongside the commonalities, we can identify some key differences.

- *Mandate vs. recommendation*: The most significant difference lies in the implementation mechanism. The U.S. has adopted a top-down, mandatory approach for its federal government, using executive orders and legislation to enforce strict timelines. In contrast, the EU relies on coordination and recommendations, guiding its member states towards a harmonised but less centrally controlled transition.
- *Stance on hybrid approaches*: While widely discussed, the enthusiasm for hybrid schemes varies. The EU and the Netherlands strongly recommend them as a practical transitional tool to mitigate risk. The UK, however, is more cautious, viewing them as a temporary measure that adds complexity and should be used sparingly.
- *Drive for cryptographic sovereignty*: While the U.S., EU, and UK are largely focused on adopting the global standards set by NIST, major powers in Asia, particularly China and South Korea, are pursuing policies aimed at developing their own national PQC standards. This reflects a strategic goal of technological independence and leadership.

10 Note that while there are tooling available that support cryptographic asset discovery and inventory, their completeness cannot be guaranteed, and providing an accuracy rate is also challenging due to the absence of ground truth. An overview of such tooling and their characteristics can be found in (Sijpesteijn, van Leuken, & Kerling, 2025).

The global policy landscape for post-quantum cryptography is evolving rapidly, with governments, international bodies, and industry leaders converging on the shared goal of building quantum-safe digital infrastructures. While approaches vary across regions, the urgency and complexity of the transition are universally acknowledged. The journey towards a quantum-secure world will span decades, and the following chapters in this handbook delve deeper into the technical and governance challenges, as well as the solution pathways developed in HAPKIDO.

4. Challenges in Transition

This chapter is based on the research done in deliverable 3.3, published in March of 2024. Its research was performed in 2023. A lot of progress happened between the report and the publishing of this handbook. We updated the conclusions where necessary.

A more detailed description is presented in HAPKIDO deliverable 3.3 (Rikken, Christiansen, Janssen, & Bharosa, 2024)

4.1 Problem Areas in the Impending Transition

The transition to quantum-safe PKI remains difficult as some critical milestones, such as the establishment of necessary technical standards, are still not fully completed. Until these standards are finalised, fully migrating certified services for key sectors is not yet possible. However, progress in the past 2 years have enabled the possibility of PQC PKI experiments: enough is standardised now to start gaining experience with the upcoming migration.

At the same time, organisational governance faces its own challenges. Many PKI users lack a clear understanding of the quantum threat and its potential impact on their systems, making it difficult to assess risks or identify necessary changes. This uncertainty limits both preparedness and urgency, leaving organisations hesitant to act (Kong, Janssen, & Bharosa, 2024). Within HAPKIDO we identify four main challenges in the impending transition.

4.1.1 Complex PKI interdependencies

For those anticipating the transition to quantum-safe cryptography, preparation may seem prudent, but practical steps remain limited. Quantum-safe solutions have not yet been formalised or validated, making independent action impossible. PKI is inherently a community-based system that relies on coordinated efforts among users, providers, and governance bodies. Changes must be aligned across the ecosystem to maintain functionality and trust, as isolated moves risk breaking interoperability.

PKI involves both governance and technical components to build a chain of trust, and any change to the trust anchor, a root Certificate Authority, for instance, must be reflected throughout the entire certificate hierarchy. This dependency can lead to interoperability challenges, particularly when organisations using older encryption levels attempt to interact with those that have adopted newer standards.

Even though not all necessary components are ready, especially for Hybrid PQC implementation, significant progress has been made: the first hybrid x.509 standard is available (Chimera) (ITU-T, 2019), NIST standards are finalised, the necessary OID for ML-DSA is added to x.509 (Massimo, Kampanakis, Turner, & Westerbaan, 2025) and the standard for composite algorithms in certificates is now in review to be published (Ounsworth, Gray, Pala, Klaußner, & Fluhrer, 2026a). This implies that several hybrid solutions will be soon available for testing and deployment.

4.1.2 Lack of urgency

Two years ago, regulatory agencies reported a growing awareness of the quantum threat, but sectors such as banking and government had a different perception of urgency still viewing the timeline as distant (Kong, Janssen, & Bharosa, 2024). This has shifted now: Dutch banks are amongst the most active in experimenting with PQC, and the Dutch government has started several awareness and migration projects, like the QvC Rijk program.

Despite these cases, the general lack of urgency still exists, but is less prevalent. It is compounded by a limited understanding of what the quantum threat entails and its specific implications for some at an organisational level. The concept of this threat often appears vague and abstract,

reducing its perceived importance. Disagreements among experts regarding timelines, risk areas, and potential solutions further muddy the waters for non-specialists trying to grasp the issue.

4.1.3 Lack of certified hardware and software

Implementing new PKI solutions often requires updated hardware and software, and in the hybrid model, these systems must support both legacy and modern PKI frameworks. While regulatory organisations may find these changes easier to implement, sectors such as banking and government face additional challenges because they rely on certified solutions (Kong, Janssen, & Bharosa, 2022) (Kong, Janssen, & Bharosa, 2024). In 2023, obtaining PQC certified hardware and software was not possible, as development stalled at early milestones, including the establishment of formal standards. Two years later we see the first certifications of hardware and software. This process has just started, a few standardised HSMs and cryptographic libraries are now becoming available[11]. The dependency on developers and third-party vendors still creates pressure for organisations to maintain services secure and protect sensitive data, even as they lack the tested and certified options needed to transition safely.

Compounding these challenges is a shortage of technical expertise among PKI users. The quantum transition remains an emerging topic, and many organisations lack the in-house knowledge to evaluate solutions or make informed decisions about initial steps. This uncertainty is intensified by the fact that developers themselves are constrained while waiting for key milestones, such as agreed-upon technical standards. As a result, organisations face a dual burden: limited guidance from experts and limited availability of reliable solutions, making the path towards a secure transition both complex and uncertain.

4.1.4 Unclear quantum-safe direction and governance

Until now, updating PKI has largely been viewed as a technical task to be handled by IT departments. Small and medium-sized enterprises (SMEs) particularly, may struggle to grasp the full implications of the quantum threat and often lack the resources and expertise to manage the transition effectively. Without clarity on what changes are required, preparation becomes nearly impossible.

Governance adds another layer of complexity. In centralised sectors, decision-making and transition planning can be relatively straightforward, as a single governing body can initiate action. In contrast, highly decentralised systems—such as government—face significant hurdles. Here, the transition becomes less about technical implementation and more about persuading non-technical stakeholders that their participation is essential (Kong, Janssen, & Bharosa, 2022). This dynamic turns governance into a collective action problem, where decisions rely on social connections and consensus rather than top-down authority. Questions of who should lead, who bears initial costs, and who holds accountability remain unresolved.

In the Netherlands, for example, Logius serves as the Policy Authority for PKIoverheid certificates, but its role is limited to technical oversight, leaving broader governance unclear (Christiansen, Bharosa, & Janssen, 2023). On the other hand, the banking sector is an example of a centralised governance approach, with a single centralised decision-making body leading the transition for the rest. In fact, the banking sector in the Netherlands has been one of the most proactive sectors in the transition and has already started experimenting with PQC. A difference in governance styles has resulted in different levels of progress for the two. The centralised approach utilised by the banking sector has allowed for a small central decision-making mechanism to make the key decisions for the group. This sets clear expectations and clearly displays who will take on the leadership.

Likewise, the government has created a small group to take charge of planning the government's transition, but unlike the baking sector, the government relies on a more fragmented, decentralised governance model. This means the individual actors within the system have more independence and a right to make decisions for themselves. Furthermore, the lines of communication in a

11 At the moment of writing, there were a few Common criteria certifications that included PQC, no FIPS 140-3 yet, and 11 CAVP certifications (a prerequisite for FIPS 140-3). Many are in the pipeline to be certified with PQC algorithms.

decentralised system can often be less clearly defined, leading to more difficulty communicating efficiently and dispersing knowledge equally across all actors. Therefore, the QvC Rijk has a more difficult task of accommodating an actor network with a diverse set of needs and limitations with unrefined lines of communication. This decentralised governance approach is expected to result in a longer timeframe for both planning and execution of the transition, as it presents many more complex and multifaceted decision-making challenges to be addressed. However, it is important to note that a longer timeframe does not equate to worse planning or instantiation.

Because PKI is a community-based system that depends on interoperability across self-governing entities, the quantum transition cannot succeed without coordinated action across the entire ecosystem. In recent years we have seen an increase in interest from the ecosystem. Evidence of this can be found in the PKI Consortium and the PQC Conference. The first conference in 2023 saw around one hundred on-site attendees, whereas the latest PQC Conference in 2025 saw approximately twenty-five hundred on-site attendees[12]. This exemplifies the growing interest and commitment from the ecosystem, as the PQC Conference attracts the leading actors in the field across research, public, and private sectors.

4.2 Different challenges for macro, meso, micro actors

This section discusses challenges in the transition as pertaining to different actor levels, with a specific focus on the transition in the Netherlands. One of the key aspects is who has decision-making rights and who has input rights. Decision-making rights refer to the right to make decisions on behalf of the group, whereas actors with input rights refer to actors who have the right to be heard and provide input on the decisions being made, but lack the authority to determine what the final choices will be (Weill & Ross, 2004) (Weill & Ross, 2005).

Following this distinction, actors can be divided into three levels. First, the ***macro level*** which looks to actors with decision rights for the transition. These are actors like the government and Logius. Second, the ***meso level***, concerns sectors who are considered to have input rights for the transition. Lastly, we consider organisations for the ***micro level***. The actors on this level are generally considered to have neither input nor decision rights. An overview of transition rights is depicted in Figure 2.

12 PKI Consortium (Public Key Infrastructure Consortium) (https://pkic.org/)

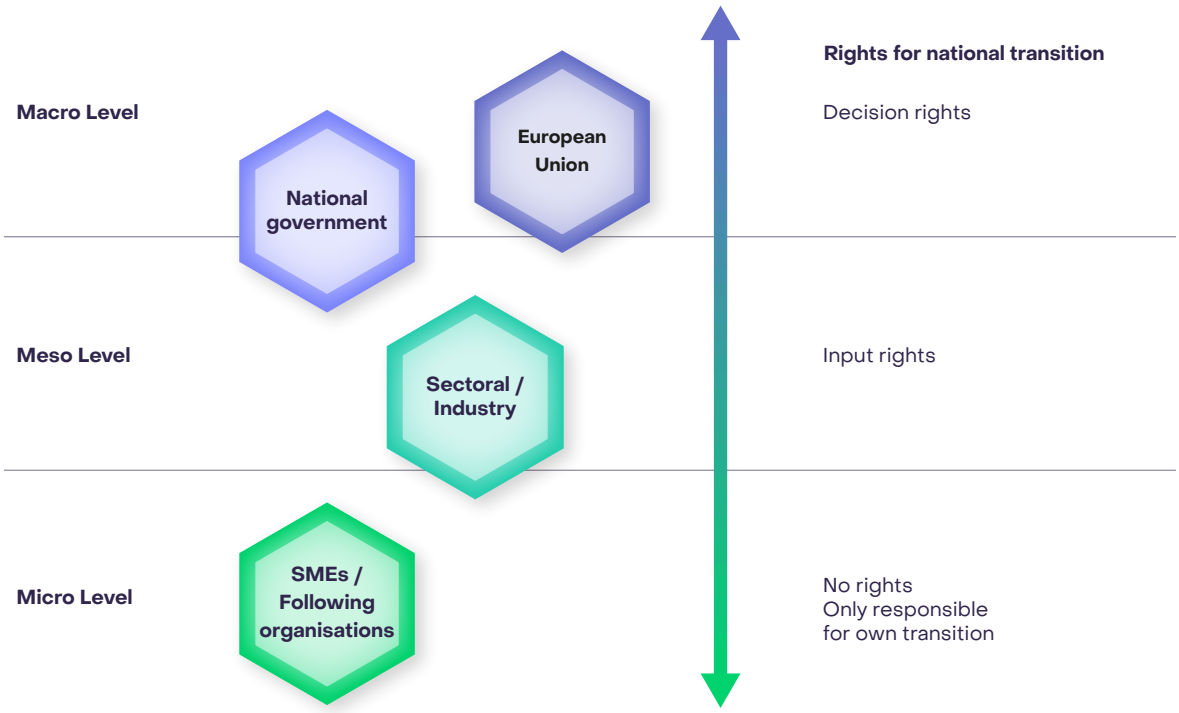

Figure 2: Overview of transition rights for the Netherlands

4.2.1 Micro

The micro level pertains to individual organisations and their internal structure for the transition. This level is not concerned with whether the organisation has any input or decision rights for the larger collective transition, but instead considers transition elements like incentive, costs, accountability, and decision making for the individual organisation. This scope falls more in line with traditional "pure" technology governance, which has a more top-down structure of decision making.

The success of this type of technology governance relies on clear communication and decision making, while relying on relevant personnel to offer perspectives and suggestions on what would be the best solutions for the company.

The challenges for this level centre on urgency, comprehension, and external dependencies. Compared to 2023, the challenges mentioned in Section 4.1 have improved but are not entirely solved. Deadlines have been indicated both by industry and the European Union (European Commission, 2025), although not yet obligatory. While larger organisations started working on the topic of comprehension with their staff to create experts on the topic, most organisations still lack resources to fully comprehend what the risks are for them and what the damage might be. Without this knowledge it is difficult to assess how much work is needed to mitigate risks and how time-consuming these changes would be. Lastly, there is the added challenge of organisations being dependent on third-party vendors to provide necessary hardware and software upgrades. This external dependency leads to a waiting position for taking action in the transition.

4.2.2 Meso

Sectors differ from the organisational perspective (micro level), since they are much less coloured by hierarchical relationships. This means governance for this level is more akin to commons governance and collective action, which see actors collaboratively maintaining resources, as well as making governance decisions in a collective way. While there are some sectors, like the banking sector, that have a centralised governance mechanism—which makes large-scale decisions for things such as the quantum transition to ensure the continued interoperability and functionality between banks—, it is much more common for sectors to be decentralised.

Sectors with decentralised governance have individual actors making decisions for themselves. In these instances, performing a sector-wide transition comes with a set of challenges. In contrast to the micro level, there are no clear decisions makers, and no one obligated to be accountable and to accept the initial cost of the transition. Managing these challenges is best done in collaboration, but not every sector has formalised lines of communication to facilitate this.

4.2.3 Macro

The macro level is characterised by having the least number of hierarchical tendencies present. For the purposes of this handbook, we consider the macro level to be the government and policy level in the Netherlands. The actors at this level are largely considered equal to one another, each with a right to make decisions for themselves. At this level, challenges are similar to the meso level with accountability, cost management, and decision-making. The key difference is that at the macro level, actors are considered to have decision rights for the larger ecosystem of PKI users, as it includes the government and Logius the Policy Authority for the PKIoverheid in the Netherlands. This means that their decisions not only impact their own organisation or an individual sector, but contributes to the potential success of most other sectors and organisations in the Netherlands.

4.3 Key Predicted Challenges in Implementing PQC Solutions

Implementing PQC solutions technically presents a complex set of challenges that go beyond simply swapping out cryptographic algorithms. In fact, many cryptographic dependencies must be updated, often introducing breaking changes that propagate through the software stack. *The breaking changes occur due to new properties of the cryptographic primitives, the ongoing development/standardisation and backwards compatibility.*

First, the new cryptographic algorithms are fundamentally different from the widely used RSA and ECC algorithms. The features that stand out are the differences in terms of cryptographic sizes and performance. As these new algorithms rely on different mathematical properties that make them quantum-safe, their design is also different. Unfortunately, this comes at the cost of large cryptographic keys and performance issues. As comparison, for 128 bits of security, RSA-4096 public keys are 512 bytes long and ECC-256 public keys are 32 bytes long. ML-KEM public keys are 800-1568 bytes (private keys are double that length). Other quantum-safe schemes can achieve cryptographic keys of several kilobytes, even megabytes (see the PQC Migration Handbook for a detailed overview of sizes and features).

Even though the computational demands of most of the new algorithms do not increase as much as the key-sizes (lattice-based cryptography and in particular ML-KEM is performance-wise competitive with RSA and ECC), implementing the new underlying mathematical structures can be challenging for low power devices.

Secondly, the quantum-safe schemes are still being implemented. Even though some quantum-safe schemes have been finalised by NIST and are now available, the deployment of PQC in different scenarios still heavily depends on other standards released by other standardisation institutions like IETF. The lack of finalised standards further complicates implementation efforts. Many specifications remain in draft form, and crucial elements such as Object Identifiers (OIDs) are not yet added to common protocols, for some PQC algorithms and some hybrid

combinations[13]. OIDs are fundamental in cryptographic protocols as they uniquely identify algorithms and parameter sets. Without them, systems cannot reliably recognise or negotiate the use of (hybrid) schemes, which hinders both deployment and interoperability. The absence of standards not only delays adoption but also increases the risk of inconsistent behaviour across systems.

It is recommended not to wait for standards to be finalised but actively engage in their development. This includes performing early testing with draft specifications, validating interoperability, testing latency and bottlenecks, and providing feedback to the standardisation bodies. Such involvement will help ensure that the final standards are fit-for-purpose and interoperable.

Finally, we note that it is difficult to upgrade from an implementation point of view. While some client applications such as browsers are among the first to support PQC, many legacy clients may not receive updates. One of the primary hurdles lies in the need to modify existing clients to support (hybrid) PQC schemes. These approaches can strain current protocol designs, especially when timeouts are configured too tightly to accommodate the increased computational demands and larger message sizes. For instance, cipher negotiations and long authentication chains in TLS or IKEv2 may cause message fragmentations and latency.

In addition, applications built on classical cryptographic schemes, such as RSA and ECC, tend to be inflexible and tightly coupled to their codebases. Even when the underlying cryptographic code is well-implemented, it is rarely designed to accommodate the cryptographic agility that is recommended for PQC. As a result, integration can demand a fundamental redesign of verification mechanisms and supporting infrastructure. For example, in case a hybrid migration approach is in place, the verification logic needs to be modified to be able to handle two cryptographic keys or signatures at the same time.

HAPKIDO deliverable 4.3 demonstrates such redesign on the Digital Signature Service software to support hybrid PDF-signatures (van den Berg, Amadori, & Spini, 2024).

For large enterprises, it is unlikely that the migration will occur at the same time for all the different components, as migrations of the assets are mostly risk-based: more sensitive and urgent assets will need to be migrated before others. The support for quantum-safe cryptography has to be manually added, requiring time and effort. This introduces the issue of backwards compatibility to make sure that the connected systems remain interoperable. For hybrid approach, however, there is no one-size-fits-all solution. As explained in Chapter 6, every hybrid approach comes with pros and cons and decisions must be made over the best fit for each use-case.

13 OIDs for the NIST algorithms are specified in the NIST standards. RFC 9935, 9881 and 9909 recently incorporated the OIDs for ML-KEM, ML-DSA and SLH-DSA in x.509 certificates. **a.** https://datatracker.ietf.org/doc/rfc9935/, **b.** https://datatracker.ietf.org/doc/rfc9881/ and **c.**https://datatracker.ietf.org/doc/rfc9909/ Composite OIDs for ML-KEM and ML-DSA are proposed but not yet standardised: **d.** https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/ and **e.** https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/

a b c d e

The transition to post-quantum cryptography (PQC) is not merely technical but a multifaceted transformation that touches every layer of cryptographic infrastructure and governance. The implementation of hybrid PQC schemes will introduce strain on existing protocols, software dependencies, and legacy systems, often requiring deep structural redesigns rather than simple plug-and-play replacements. These technical hurdles are compounded by the absence of finalised standards, which impedes interoperability and consistent deployment. Together, these issues underscore the need for coordinated governance, robust policy frameworks, and cross-sector collaboration to ensure a secure and sustainable transition to quantum-safe infrastructures.

5. Preparing for Transition

5.1 Clarifying the Terms Used in the Handbook

The handbook uses two complementary sets of terms to describe different aspects of the transition: one set focuses on governance and decision-making, while the other focuses on how organisations are connected and coordinate with each other. Using these two perspectives helps readers understand both who makes decisions and the interdependence between organisations across levels.

Macro, Meso, Micro

Chapter 4 introduces the terms macro, meso, and micro, which describe the scope of influence and decision-making authority at different levels, helping readers understand who makes decisions and how responsibilities are distributed.

- **Macro level**: Institutions and global actors with decision rights for the transition.
- **Meso level**: Sectors with broad input rights influencing the transition.
- **Micro level**: Individual organisations, focusing on internal structures, incentives, costs, accountability, and decision-making, without assuming input or decision rights over the larger transition.

These terms show that macro actors are responsible for making decisions, meso actors provide input to guide those decisions, and micro actors focus on managing processes within their own organisations.

Ecosystem, Inter-Organisational, Intra-Organisational

Chapter 5 introduces the terms ***ecosystem***, ***inter-organisational***, and ***intra-organisational*** levels to capture organisational interdependencies and how organisations can coordinate with each other. These levels clarify organisational boundaries and capture interdependencies, helping readers to understand the conditions and actions both within and across organisations.

- **Ecosystem level**: Organisations operating across multiple jurisdictions or sectors, often with regulatory or standard-setting responsibilities. Examples: Regulatory bodies across the EU: European Commission (EC), European Parliament (EP), International standards and cryptography organisations: NIST, ETSI, Network and information security authorities: ENISA, Multinational companies with cross-border responsibilities.
- **Inter-organisational level**: Organisations managing or applying regulations, standards, or critical infrastructure within a national context. Examples: Government agencies enforcing national regulations, organisations operating critical infrastructures across sectors.
- **Intra-organisational level**: Individual entities relying on or delivering services within organisations, without necessarily managing critical infrastructures themselves. Examples: Government agencies, banks, hospitals, small and medium enterprises (SMEs).

The terms show interdependencies across organisations, identify the conditions in the ecosystem and actions relevant at each level, and reduce confusion when interpreting governance and coordination.

Integrating Both Perspectives

By combining the governance perspective (*macro*, *meso*, *micro*) with the organisational perspective (ecosystem, inter-organisational, intra-organisational), the handbook provides a comprehensive framework. This dual lens allows readers to 1) understand who has decision-making authority at different levels; and 2) see how organisations interact and coordinate within and across sectors.

To make the handbook easy to follow, each set of terms is used consistently in the chapters, governance terms in Chapter 4, and organisational terms in Chapter 5. Using these complementary perspectives ensures that readers can analyse both decision-making power and organisational interdependencies, without confusing the two.

5.2 Growth Model for Transition

The growth model takes an ecosystem perspective, showing that quantum-safe transition is not merely a technical change, but a complex, multi-actor transition process that requires coordinated efforts among organisations. As organisations move through a series of stages, necessary conditions in the ecosystem need to be met, and collective action across organisations is required to achieve quantum-safety. The high-level overview of quantum-safe transition acts as a supporting and communication tool that can be complementary to the PQC Migration Handbook Part II (Amadori, et al., 2024). In the PQC Migration handbook, a three-step approach is mentioned, including: 1) ***Diagnosis***; 2) ***Planning***; and 3) ***Execution***. The stages of growth model can be used as a tool for addressing the second step, *Planning*.

The stages of growth model indicate necessary conditions in the ecosystem, and actions that organisations may need to execute to move with the ecosystem. The growth model communicates the complexity of transition and helps organisations position themselves in a broader transition process. In doing so, organisations can structure their discussions to navigate their transition and build the necessary capabilities.

There are five stages in the model, which are Quantum-safe awareness phase (***stage 1***), Quantum-safe assessment phase (***stage 2***), Quantum-safe preparation phase (***stage 3***), Quantum-safe implementation phase (***stage 4***), and Quantum-safe adaptation phase (***stage 5***). Figure 3 illustrates the five stages of growth model for quantum-safe transition. Each stage is described below, and *discontinuities* are presented at each stage as a set of conditions that need to be met in the ecosystem for organisations to move from one stage to the next.

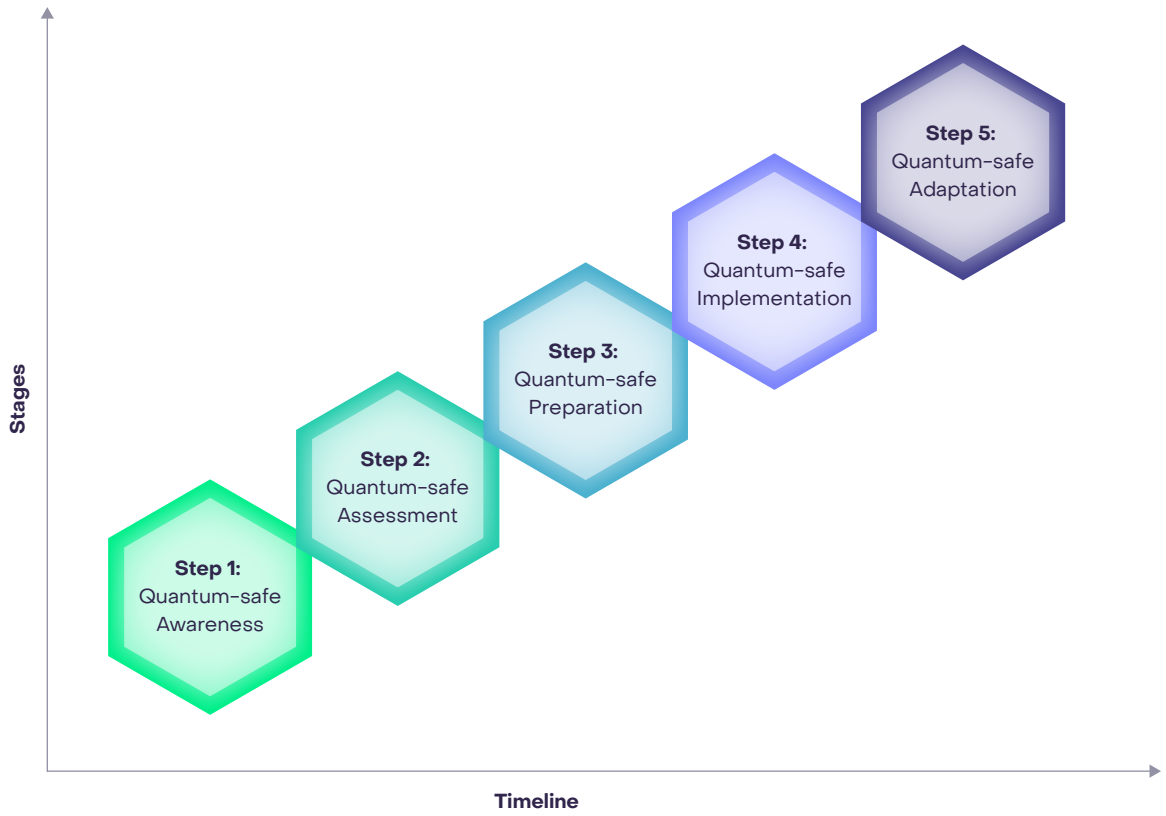

Figure 3: Stages of Growth Model for quantum-safe transition

Five Stages of Growth Model

The stages of growth model are explained with organisations across three different levels: the ecosystem level, inter-organisational level, and intra-organisational level. Organisations at the ***ecosystem level*** include regulatory organisations at the EU level (*e.g.*, European Commission, the European Parliament), the Standardisation bodies and multi-national companies. Organisations at the ***inter-organisational level*** include government agencies that apply national regulations and standards (*e.g.*, ministries, Logius, National Cyber Security Centre (NCSC-NL)) and organisations that manage and operate critical infrastructures across and within sectors in a national context. Organisations at the ***intra-organisational level*** include public and private entities that do not necessarily operate or manage critical infrastructures but rather rely on the services provided by these infrastructures (*e.g.*, government agencies, banks, tax office, and other small and medium enterprises (SMEs)).

The details of the results can be found in the PhD research (Kong I. , 2026).

5.2.1 Stage 1

At Stage 1, the quantum-safe awareness stage, discontinuities include: 1) acknowledgement of risks and vulnerabilities of quantum threats; and 2) a finalised list of PQC standardisation must occur in the ecosystem. During Stage 1, the security issues related to quantum computing technology may be discussed. However, there are many uncertainties and limited knowledge available in the ecosystem. The announcement from the standardisation bodies on standards and guidance for PQC algorithms may raise awareness and allow organisations to recognise the need for quantum-safe transition.

5.2.2 Stage 2

At Stage 2, the quantum-safe assessment stage, discontinuities include: 1) establishment of a steering committee and working groups; and 2) establishment of a testing environment for PQC solutions. During Stage 2, organisations may start assessing their existing infrastructures (*e.g.*, risk, readiness, and impact, etc.) to prepare for quantum-safe transition. In the ecosystem, organisations recognise the need for quantum-safe transition and seek expertise to coordinate transition efforts. Some organisations may be involved in setting up testing environments for PQC solutions.

5.2.3 Stage 3

At Stage 3, the quantum-safe preparation stage, discontinuities include: 1) availability of selected PQC solutions validated through testing; and 2) development of policies and regulations that support quantum-safe transition. During Stage 3, there are various transition efforts depending on the organisation's risk appetite. The majority of the organisations that are not participating in the testing environment may wait for the development of PQC solutions. While organisations finalise their assessments for existing infrastructures, mandatory policies and regulations may be available in the ecosystem to provide legal mandates and additional compliance related to PQC standards.

5.2.4 Stage 4

At Stage 4, the quantum-safe implementation stage, discontinuity includes: 1) availability of PQC solutions in HSM, Certificate Issuance software (CAs), smartcard management platforms and smartcard-processors. Without the availability of quantum-safe hardware and software, organisations cannot implement PQC solutions in their existing infrastructures. During Stage 4, organisations may further seek resources, training, and expertise to coordinate their transitions with various stakeholders, such as CAs. To avoid interoperability and backward compatibility issues, organisations may start their implementation on a small scale.

5.2.5 Stage 5

At Stage 5, the quantum-safe adaptation stage, discontinuities include: 1) availability of lessons learned and best practices from the implementation of PQC solutions; and 2) development of a cross-organisational coordination mechanism. During Stage 5, a full-scale transition may take place to implement PQC solutions across systems. With lessons learned and a cross-organisational coordination mechanism, efforts at the previous stage do not remain isolated. This allows organisations to work towards a seamless transition with coordinated efforts.

5.3 Actions Needed Across Organisations

While organisations have different levels of resources, risk appetite, and timeline for quantum-safe transition, an overview of actions needed across organisations shows that quantum-safe transition remains complex, and organisations cannot progress independently without affecting interoperability. From banks, government agencies, technology providers, to CAs, there are multiple stakeholders involved in quantum-safe transition. Without timely and coordinated actions, misalignment among these stakeholders can create security issues, interoperability challenges, and regulatory non-compliance. Therefore, proactive initiatives are essential to ensure that dependencies are managed, and organisations move together with the ecosystem to achieve quantum-safety.

In addition, standards and regulations for PQC are rapidly evolving. European frameworks such as NIS2 and DORA, along with emerging international PQC standards, are still maturing. Organisations cannot rely solely on static compliance checklists. By understanding the scope of quantum-safe transition and what different organisations can do, organisations may navigate changes in the ecosystem and anticipate actions needed in their strategies. The list of actions needed for quantum-safe transition shows that organisations need to align the transition process with the ecosystem. This allows organisations to further navigate uncertainties, prioritise initiatives, manage dependencies, and sequence the stages of PQC adoption in a controlled way.

For organisations at the inter-organisation level, the list of actions is shown in Table 5. For organisations at the intra-organisational level, the list of actions is shown in Table 6.

Table 5: List of Actions at the Inter-Organisational Level

Stage	List of Actions at the Inter-Organisational Level
Stage 1	• Participate in discussions on PQC solutions across industry, academia and government.
Stage 2	• Define clear roles, responsibilities and decision-making structure for quantum-safe governance via a steering committee and working groups. • Establish testing environment to test and select suitable quantum-safe standards.
Stage 3	• Develop hardware and software that are suitable with PQC solutions. • Develop relevant sector-wide guidelines that support quantum-safe transition.
Stage 4	• Migrate non-PQC systems of CAs to selected PQC solutions. • Facilitate an expertise centre for quantum-safe transition to share knowledge and skills needed for quantum-safe transition.
Stage 5	• Foster collaboration across sectors on future research, development, and standard setting to address evolving security threats and challenges.

Table 6: List of Actions at the Intra-Organisational Level

Stage	List of Actions at the Inter-Organisational Level
Stage 1	• Raise awareness on the importance of quantum-safe transition and the complexities in implementing PQC solutions.
Stage 2	• Conduct assessments to identify the level of risk, readiness, and impact for quantum-safe transition.
Stage 3	• Communicate tendering requirements for quantum-safe products and services (*e.g.*, hardware and software using PQC solutions).
Stage 4	• Modify non-PQC part of the existing systems on a smaller scale with PQC solutions. • Provide training and support to ensure that quantum-safe transition is managed with necessary skills and expertise.
Stage 5	• Finalise the adoption of PQC solutions in a scaled environment across all systems. • Monitor, adapt and adjust security practices to enable rapid adaptation to changes based on new insights, regulatory and technological changes.

The list of actions across organisations at different levels (*e.g.*, inter and intra levels) creates a common understanding of goals towards achieving quantum safety, recognises constraints and possible timelines that can be discussed in enabling coordinated execution. By understanding what needs to happen at each stage, organisations can think about bottlenecks and analyse decision points to make informed choices to be aware of risks and strategic implications. Organisations may further allocate their resources to proactively seek expertise, training, and budget where it matters most so that potential silos that can occur during transitions can be avoided.

Due to diverse organisations that are interdependent across different levels in the ecosystem, organisations may need to collectively take part and execute actions to carefully prepare for quantum-safe transition. The list of actions in different stages of growth model shows which actions should be tackled first. Organisations may further clarify roles and responsibilities to align internal teams and identify decision makers to ensure that transitions remain coordinated with their stakeholders. By further mapping dependencies and risk points, organisations may need to highlight critical decision points and trade-offs. It is crucial to tailor and make adjustments to the strategies as changes occur in regulations, standards, and technology.

5.4 Organisational Readiness Assessment Model

In addition to the five stages of growth model and the list of actions needed across different organisations, an organisational readiness assessment model provides an overview of important dimensions that organisations need to think about when undergoing quantum-safe transition. While the growth model provides an overview of quantum-safe transition with an ecosystem and what organisations may need to do to move with the ecosystem, the organisational readiness assessment model recognises that quantum-safe transition helps organisations assess their current state and identify dimensions that may need to be addressed for transition efforts.

By understanding the readiness of organisations, the model allows organisations to identify gaps that need to be addressed. This provides an opportunity for organisations to highlight dimensions where additional efforts are needed. The list of dimensions includes Collaboration, Governance, Policy and Regulation, Awareness, quantum-safe solution standards, Hybrid quantum-safe solution, Cryptographic Agility Strategies, and Knowledge of quantum-safe transition. The dimensions

have been clustered using the *Technology–Organisation–Environment* (TOE) framework. The term *environment* has been revised to *Ecosystem* to better align with the context of quantum-safe transition.

The details of readiness levels can be found in HAPKIDO deliverable 7.1 (Kong, Janssen, & Bharosa, 2024).

5.4.1 Technology

5.4.1.1 Quantum-Safe Solution Standards

Although quantum-safe technology with new encryption levels is not yet available, organisations need to conduct technical inventory assessments to identify their vulnerabilities and technical interdependencies. Also, interoperability and backward compatibility are crucial to communicate over networks in the existing infrastructures. Thus, organisations need to evaluate the functionality, performance, and resilience of quantum-safe solutions. While some actors may be involved in the testing phase of quantum-safe solutions to select the right algorithms, other actors may wait on those decisions and technical developments.

5.4.1.2 Hybrid Quantum-Safe Solution

The term hybrid provides several definitions, which may involve using either classical cryptographic primitives or quantum-safe cryptographic primitives or employing both of these primitives to secure core processes over networks. Due to the wide implementation of the core processes, there needs to be an assessment of which part of the existing infrastructures requires a hybrid quantum-safe solution. While the usability and effectiveness of the solutions are not yet known, organisations need to navigate the development of quantum-safe technology and select quantum-safe solutions that have been validated in their functionality, performance, and resilience.

5.4.1.3 Cryptographic Agility Strategies

While organisations with defined cryptographic policies and guidelines follow industry-wide accepted cryptographic algorithms and key management, the existing systems are rigid, and changes cannot occur in isolation due to path dependencies. Current cryptographic strategies that organisations have in place do not provide security against quantum threats, and these strategies are not agile enough to adapt to the changing environment of new technologies. Due to many uncertainties surrounding quantum-safe transition, it is crucial for organisations to develop cryptographic agility strategies and adopt new cryptographic algorithms, protocols, and technologies that become available.

5.4.2 Organisation

5.4.2.1 Awareness

Since many of the security threats posed by quantum computers are not yet visible (*e.g.*, store now and decrypt later), there is a lack of urgency regarding quantum computing-based threats and risks associated with the technology. Likewise, modifying the cryptographic algorithms in the existing infrastructures is an under-the-hood process where the need for quantum-safe transition can go unnoticed by organisations. While many of the decisions regarding quantum-safe technology have not yet been crystallised, it is crucial for organisations to raise awareness and stay up to date with the development of quantum-safe technology so that they become ready for quantum-safe transition.

5.4.2.2 Knowledge on Quantum-Safe Transition

There is a lack of knowledge on the scope of quantum-safe transition, the impact of quantum threats on existing business processes, and vulnerabilities identified from technical inventory assessments. The selection criteria for quantum-safe solutions are not yet known, and organisations do not know which part of the existing infrastructures needs hybrid quantum-safe solutions. The lack of knowledge on quantum-safe transition creates uncertainties and delays decisions in the ecosystem. More knowledge sharing and research are needed on the topic of quantum-safe transition. Organisations need to stay up to date with the development of

quantum-safe technology and translate insights into their strategic planning to better navigate quantum-safe transition.

5.4.2.3 Policy and Regulation

Many aspects of quantum-safe transition are subject to change due to the ongoing development of quantum-safe technology. This also means that if decisions are made in the ecosystem, it may also influence organisations' direction of quantum-safe transition. Although having policies and regulations can provide legal mandates and scrutinise uncertainties in standard and compliance requirements, there is currently no policy or regulation available for quantum-safe technology. Organisations may need to monitor the regulatory process and identify the requirements for quantum-safe transition.

5.4.3 Ecosystem

5.4.3.1 Collaboration

For organisations, the facilitation of critical infrastructures requires multiple actors in the ecosystem, such as regulatory bodies, service providers, software companies, hardware vendors, and end users. The underlying technical interdependencies maintain the secure functioning of the existing infrastructures. However, this also means that organisations cannot change the existing infrastructures without affecting other interdependent actors involved in the use and facilitation of the infrastructures. Since quantum-safe transition cannot be addressed by one organisation, achieving collective action with multiple actors in the ecosystem is crucial.

5.4.3.2 Governance

The topic of quantum-safe transition is relatively new, and there are no existing guidelines, rules, or mechanisms for decision-making and accountability. For organisations, there is a clear institutional void without well-defined roles and responsibilities. Due to many uncertainties regarding the maturity of quantum-safe technology, preparation for quantum-safe transition remains vague. While some actors may be involved in making external decisions in the ecosystem, other actors may wait for those decisions and follow the lead of frontrunners. Thus, there is a need for clear governance for organisations to coordinate actions to prepare for quantum-safe transition with multiple actors in the ecosystem.

The growth model outlined in this chapter offers a structured pathway for organisations to navigate the impending transition, highlighting the evolving roles and responsibilities across ecosystem. As organisations progress through the five stages—from uncertainty to full-scale implementation—they must recognise and seize opportunities, and acquire dynamic capabilities that allow them to sustain growth and support, while also assessing their readiness across technological, organisational, and ecosystem dimensions. Ultimately, the successful transition to Quantum-Safe PKI will depend not only on technological innovation but also on the ability of organisations to align their strategies, policies, and infrastructures with the emerging quantum landscape.

6. PQC in PKI

6.1 NIST PQC standards

The US National Institute of Standards and Technology (NIST) started in 2016 the Post-Quantum Cryptography (PQC) Standardisation process for standardising new key encapsulation mechanisms (KEMs) and digital signature schemes, which are believed to offer security against quantum attacks. Researchers and cryptographers were asked to develop such schemes and submit them, so that they can then be publicly scrutinised and evaluated. The inspection would go through several rounds aiming at evaluating different aspects, like security, performance and implementation. After close to ten years of competition and four rounds, NIST has standardised one KEM (ML-KEM, lattice-based), and another one (HQC) will follow. Additionally, NIST has standardised the digital signature scheme ML-DSA, which is lattice based, and SLH-DSA, which is hash-based (and so there is no need to be used with hybrid crypto), and another one (FN-DSA) will follow. There is also an additional on-ramp competition for digital signatures with different design and performance goals, which is in its second round at the time of writing.

As reviewed in Chapter 3, many countries have already published their requirements for the usage of PQC and whether they mandate, recommend or repel the use of PQC with conventional crypto in hybrid mode.

6.2 Hybrid Certificate Standards: Structure, Purposes, and Recent Developments

Hybrid cryptography's purpose can be twofold. It is mainly recommended for security reasons: if there are two layers of (non-optional) security, one can break without the data being exposed. This form of hybrid is sometimes called hybrid "AND". The other option, hybrid "OR", often used for backwards compatibility, uses two algorithms, but it is optional which to use.

HAPKIDO deliverable 5.2 reviews developments on hybrid security, focusing on combiners for public-key encryption schemes (or KEMs) and digital signature schemes (Fehr, Huang, & Amadori, 2023).

Hybrid certificates are meant to enable the use of digital signatures in hybrid mode. Naturally, in order to use hybrid cryptography, the infrastructure using public-key cryptography requires changes to accommodate the deployment of hybrid cryptography. This implies that the certificates should also change part of their structure and information which they contain. Several approaches to hybrid certificates have been proposed and are being considered, with various trade-offs in terms of structure, compatibility, and security guarantees.

There are different approaches to include hybrid cryptography, and they are enjoying different stages of development and standardisation. There is no one size fits all and all the types of hybrid certificates have pros and cons. This section outlines the main strategies under consideration and highlights ongoing standardisation efforts.

6.2.1 Parallel Certificates

This approach involves issuing two separate certificates—one using a classical algorithm and the other using a post-quantum algorithm. Applications then digest and verify both certificates. Binding the two certificates together to ensure consistent identities can be done out-of-band or with explicit linking extensions, by having a common or cross-trusted root cross-sign the two certificates. An advantage of this solution is that it maintains compatibility with systems expecting

only classical algorithms, and it separates concerns and allows independent validation and easy rollback: It is possible to remove one chain without disturbing the other. However, it comes with an increased management complexity, and it is harder to enforce synchronised revocation or lifecycle management (Okubo, Bonnell, Gray, Ounsworth, & Mandel, 2025).

6.2.2 Composite Hybrid Certificates

Composite hybrid certificates offer a simple approach for using hybrid cryptographic algorithms as it does not change the structure of the digital certificate. Instead, this method involves composing the classical and quantum-safe public keys and signatures, and handles them as a unique new algorithm, and places them into the corresponding fields of the certificate. For instance, a hybrid certificate may include both an ECDSA key and a post-quantum key (*e.g.*, ML-DSA or FN-DSA) in the *SubjectPublicKeyInfo* field, and the signature over the certificate consists of a composition of the classical and quantum-safe signatures in the *SignatureValue* field. In a "composite" certificate, a composite public-key is an ASN.1 sequence of the two public-keys. Verification succeeds only if the composite algorithm is satisfied, which enforces that both underlying algorithms are validated (hybrid "AND").

Composite certificates are simpler to implement, handle, and verify, and offer backward compatibility since it does not require adjustment to the certificate format. However, it does require updates to parsers, libraries, HSMs, and toolchains to understand the OIDs and encodings of the hybrid keys and signatures.

Composite OIDs to accomplish composite certificates are not yet standardised and are still an IETF-draft—but its efforts are stabilising (Ounsworth, Gray, Pala, Klaußner, & Fluhrer, Composite ML-KEM for use in X.509 Public Key Infrastructure, 2026b) (Ounsworth, Gray, Pala, Klaußner, & Fluhrer, Composite ML-DSA for use in X.509 Public Key Infrastructure, 2026a).

6.2.3 Chimera Hybrid Certificates

In Chimera certificates (also known as Catalyst certificates), the certificate structure is kept intact, and the main body contains classical public keys and signatures, but three "alternative" non-critical extensions are added, called: *SubjectAltPublicKeyInfo*, *AltSignatureAlgorithm* and *AltSignatureValue*. The extra fields are included in extension field. The extensions' non-critical nature means only the algorithm in the main body of the certificate is mandatory. This implies that clients that have not yet upgraded to quantum-safe cryptography are not impacted by digesting a chimera certificate: they can ignore these unknown extensions and still validate the classical signature (hybrid 'OR'), making it an easy solution for backwards-compatibility. It also offers easy migration for ecosystems that cannot upgrade all verifiers at once. On the downside, new extension processing rules and a signature-over-extension logic must be implemented for post-quantum verification. This form of hybrid "OR" does not provide extra security as compared to hybrid "AND", as it leaves the choice which algorithm(s) to use to the certificate consuming application/protocol. Originally released as a patent, it is now an open standard maintained by ITU-T since 2019 (ITU-T, 2019).

6.2.4 Delta-Extension (or Chameleon) Hybrid Certificates

In this approach, the Delta-Extension certificate consists of two certificates that are merged into one: one certificate is the "base" (or outer) certificate, and the second one is the "delta" (or inner) certificate. Except for a specific non-critical extension, the base certificate looks exactly like a traditional certificate, so an unmodified tool should be able to parse and verify it. In principle, this format is therefore retro-compatible. The difference from the delta to the base certificate is encoded in the above-mentioned non-critical extension, and so the delta certificate can be reconstructed by the base certificate into a fully verifiable certificate. It has similar drawbacks as the above option, however it simplifies the management of the signatures and public keys in the certificate during the creation and verification processes (Bonnell, Gray, Hook, Okubo, & Ounsworth, 2025).

6.3 Merkle Tree Certificates

The current PQC standards produce bigger keys and signatures, which can become problematic with the inclusion of larger chains in some protocols.

Merkle Trees types of certificates are being considered for this issue for webPKI (Benjamin, O'Brien, Westerbaan, Valenta, & Valsorda, 2025). They are being tested by Google Chrome and Cloudflare and experimentation is planned for 2026. The goal of this innovative design is to help reduce the redundancy in the Certificate Transparency logs and the certificates themselves, making their management more agile and sensibly reducing the size of log entries and certificates.

In Merkle Tree Certificates, during the process of certificate issuance, a CA creates a batch of certificates and builds a Merkle Tree. The head of the tree is signed, and the Merkle Tree Certificate contains now only the public key of the subject, an inclusion proof to create the path of the tree to reach the head and its signature. Since the certificate signature is not stored in the certificate, the size of the certificate is much smaller. The signature verification consists in checking if the certificate is part of the tree and if the signature of the head matches, preventing processing of the entire verification chain.

Due to their design and deployment requirements, Merkle Tree certificates have been designed for the webPKI and are not going to replace private PKIs or non-webPKI scenarios.

6.4 Crypto-Libraries and the Implementations of Hybrid Certificates

Crypto-Libraries are central for the migration of hybrid certificates. First of all, crypto libraries need to provide implementations for PQC algorithms and their hybrid modes, as well as the corresponding OIDs for usage. Without support for quantum-safe algorithms, even without hybrid certificates, migration is extremely challenging. Most of the development of libraries, HSM, and products depended on the introduction of PQC algorithms. This was made possible with the release of the NIST algorithm standards.

The IETF and other standards should play a central role in the adoption of hybrid cryptography in practice, but this is not always what happens. For example, the hybrid key exchange X25519MLKEM768 has been integrated in OpenSSL and is now the default algorithm for key exchange even though the standard has not been completed yet.

Even without standardisation, cryptographic libraries can already help by giving the building blocks necessary to prepare for the transition, by placeholding the standards, allowing a testing environment to be set up to already test performance and impact on the service. Nonetheless, with the standardisation of the PQC algorithms the adoption becomes easier since this provides a framework to produce production ready code that can be included in a “pre-migrated” software.

The lack of standards can definitely slow the availability of cryptographic functionalities. Most of hybrid functionality is still in test because there are no standards supporting them. At the time of writing, libraries like Openssl, Botan have support for PQC and hybrid KEMs, but offer no support to hybrid signatures or certificates. OpenSSL can be integrated with an external provider, namely *oqsprovider* which offers functionalities for composite certificates. WolfSSL supports hybrid Chimera-type certificates. Bouncy Castle (based on Java) offers support to all types of mentioned certificates. That does not imply that software relying on Bouncy Castle also supports this. For example, at the time of writing, EJBCA community edition[14] does not offer support to non-standardised hybrid certificates even though it uses Bouncy Castle as fundamental building block.

---

14 GitHub - Keyfactor/ejbca-ce: EJBCA® – Open-source public key infrastructure (PKI) and certificate authority (CA) software (https://github.com/Keyfactor/ejbca-ce).

HAPKIDO deliverable 4.5 publishes an extended version of EJBCA-CE, which adds support to Composite and Delta-Extension hybrid modes (Amadori & van den Berg, 2025).

As hybrid cryptography emerges as a practical bridge between classical and quantum-safe systems, the evolution of hybrid certificate formats—composite, parallel, chimera, and delta-extension—reflects the diverse technical and operational needs of modern infrastructures. These innovations offer varying degrees of compatibility, flexibility, and complexity, but require significant updates to cryptographic libraries, toolchains, and standards. While some libraries like OpenSSL and Bouncy Castle have begun integrating PQC and hybrid functionalities, the lack of finalised standards continues to hinder widespread adoption and interoperability.

7. Recommendations

7.1 Organisational Uncertainties: When and What to do next?

For leaders in business and government, the quantum threat presents a convoluted set of uncertainties. The World Economic Forum expects that 20 billion digital devices will need to be upgraded or replaced with post-quantum cryptography in the next 20 years (World Economic Forum, 2022b). The challenge is not just technical; it is strategic, organisational, and economic (Alagic, et al., 2025). The core questions that organisations grapple with include:

7.1.1 When will there be a Cryptographically Relevant Quantum Computer?

Expert timelines vary, but an optimistic estimate places the arrival of a cryptographically relevant quantum computer within a 10-to-20-year window. However, this is fraught with uncertainty. A scientific breakthrough could accelerate the timeline, while unforeseen engineering hurdles could delay it.

This uncertainty creates a difficult strategic dilemma (Christiansen, Bharosa, & Janssen, 2023). Acting too early could mean investing in quantum-safe solutions that become obsolete or are not yet standardised, wasting resources. Acting too late, however, could lead to critical operational impacts, leaving an organisation exposed to the SNDL threat or unable to migrate its systems before the real-time threat materialises. The key is to approach this not as a single date to prepare for, but as a period of escalating risk that requires a phased and agile response. For data with a 20-year confidentiality requirement, the risk period has already begun.

Additionally, the focus on potential timelines and risk appetite will become less relevant due to the emergence of migration pressure from law, policy and sector rules, which can either be specific with strict deadlines (like we see in the US Quantum Computing Cybersecurity Preparedness Act), or demand migration more indirectly (an example would be regulations like DORA and GDPR which demands technical measures which take into account the state of the art).

7.1.2 When are post-quantum cryptography (PQC) standards widely available?

Post-quantum cryptography (PQC) refers to cryptographic systems that are currently being developed to strengthen security against quantum technology-based intrusions. The American National Institute of Standards and Technology (NIST) coordinates the development and selection of PQC algorithms through a public, competition-like process to specify additional digital signature, public-key encryption, and key-establishment algorithms to supplement current standards (Alagic, et al., 2025). These algorithms are intended to protect sensitive information well into the foreseeable future, including after the emergence of a CRQC. The NIST standardisation process is being completed[15], with the winners announced and the three out of five algorithms (including the main winners) standardised. Figure 4 provides an overview of the standardisation process.

15 Post-Quantum Cryptography | CSRC(https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline)

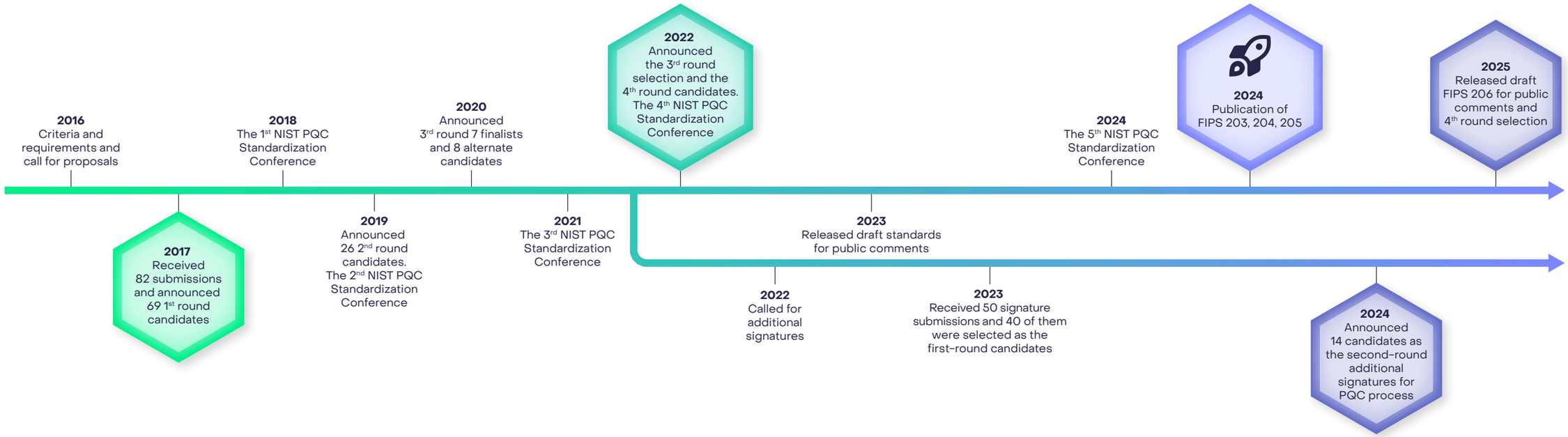

Figure 4: NIST standardisation process, image based on the original in (Moody, 2025), published before the announcement of HQC as an additional winner

In 2024, after three rounds of evaluation and analysis, NIST announced the selection of the first algorithms to be standardised. The public-key encapsulation mechanism (KEM) selected for standardisation was CRYSTALS-Kyber (ML-KEM). The digital signatures selected were CRYSTALS-Dilithium (ML-DSA), Falcon (FN-DSA), and SPHINCS+ (SLH-DSA). In May 2025, HQC was announced as the back-up winner for KEMs.

7.1.3 What can my organisation do (micro level)?

What awaits beyond awareness and societal risk assessment? Industry, governments, and other organisations currently face a choice between proactive and reactive migration to PQC solutions (Trzcinski, Vaidyanathan, Higuchi, & Jayanti, 2023).

For organisations asking what practical steps can be taken beyond awareness, the Revised PQC Migration Handbook (Amadori, et al., 2024) provides a clear roadmap. As previously mentioned, it outlines three key phases: (1) performing a Quantum-Vulnerability Diagnosis, (2) planning the migration, and (3) executing the migration. Specifically for a PKI migration scenario, a number of activities are suggested:

Phase 1: Perform a Quantum-Vulnerability Diagnosis. Identify the assets with higher risk and migration priorities, the assets that are local, and the assets that are "on-site" or deployed. These include PKI platforms, HSMs, certificates and private signing keys, smart cards, passports, authentication barriers, Point of Sales (POS), digitally signed documents, access tokens, etc. Identify cryptographic suppliers and query their quantum-readiness roadmap.

Phase 2: Plan for migration to PQC. Create a team dedicated to the migration trajectory. Involve PKI experts, software architects and engineers, policymakers, cross-departmental contact persons and managers. Plan budget and effort and create milestones depending on self-assessed PQC persona. Keep track of your progress using PKI maturity assessment tools such as the proposed by the PKI Maturity Model Working Group (PKIConsortium, 2026) and the HAPKIDO's five stages growth model as presented in Chapter 5.

Phase 3: Execution step of the PQC migration. Identify your roadmap to achieve cryptographic agility. It is recommended to not plan only for PQC migration, but design the architecture and the assets with enough flexibility to allow for future cryptographic migrations. Cooperate in working groups, projects and consortia with suppliers and organisations in the same sector. Consider a certification such as FIPS or Common Criteria for your cryptographic assets. Run tests and pilots for benchmarking and assess interoperability between the different components in the ecosystem. Participate in standardisation activities whenever possible.

7.1.4 What should other organisations do on a sectoral (meso) and global (macro) level?

The quantum threat to PKI-dependent digital infrastructures is a systemic problem that cannot be solved by any single organisation in isolation (National Academies of Sciences & Medicine, 2019). Because most PKIs are inter-organisational constructs—relying on standards, hardware, and software governed by a fragmented global ecosystem—the transition to PQC is not a routine IT upgrade. Rather, it is a complex, multi-dimensional shift that requires collective action across sectoral (meso) and national and international (macro) levels. Yet, what to do on the macro and meso level depends on the developments and the transition challenges on the micro level.

Findings from HAPKIDO reveal four challenges that currently impede the transition (described in Chapter 4):

1. Uncertainty arising from complex PKI interdependencies (see Section 4.1.1), where the need for coordinated, ecosystem-wide action makes costs, benefits, and risks difficult to assess, undermining the development of robust business cases.
2. Uncertainty and disagreement regarding the timeline and practical implications of a CRQC (see Section 4.1.2), resulting in an abstract perception of the quantum threat and a reduced sense of urgency among organisations.

3. Limited availability of tested, certified, and production-ready PQC-enabled hardware and software (see Section 4.1.3), constraining organisations' ability to safely deploy hybrid PKI solutions.
4. A lack of transition guidance (see Section 4.1.4), including certified decision-support tools, and advisory services, leaving organisations without clear direction, ownership, or governance structures to guide the quantum-safe transition.

Addressing these challenges requires intervention beyond individual organisations. Governance interventions at the meso and macro levels typically take the form of policy making, legislation, standardisation, financial support and market development, all of which aim to create incentives for coordinated action. A recent example is the proposed amendment to the NIS2 Directive, which require Member States to incorporate post-quantum cryptography considerations into their national cybersecurity strategies. If adopted, this amendment would function as a regulatory compliance incentive, signalling that EU policymakers recognise both the quantum threat and the growing urgency of preparing for it.

However, while macro-level instruments such as NIS2-related legislation provide an incentive, legislation alone is insufficient to remove the previously mentioned challenges. Complementary actions at both the macro and meso levels (*e.g.*, EU bodies and national governments) are needed to translate policy ambition into concrete progress. These may include integrating PQC-compliance requirements into public procurement processes, establishing targeted funding mechanisms to support SMEs and critical infrastructure providers in their migration efforts, and actively stimulating (hybrid) PQC transition pilots, consortia, and working groups to foster experimentation, and shared learning across the ecosystem.

7.2 Future Directions and Considerations

7.2.1 Algorithm choice and performance

From a compliance point of view, different policies in different sectors, organisations or other subdivisions of society might call for the use of specific algorithms. This can limit the choices available. To help differentiate between the remaining choices, we can consult performance results of real-world migrations, such as done during the PCSI post-quantum benchmarking project[16,17], where migration was executed for a load-balancing application used for TLS traffic.

For most general-purpose hardware currently in use, such as dedicated servers or regular laptops with a mainstream CPU with several cores and mainstream RAM, the performance overhead of post-quantum algorithms is predicted to be minimal as long as the increased bandwidth can be supported by the infrastructure, according to the PCSI results, where both servers and clients were tested. The outlier is SLH-DSA – a hash-based signature scheme known for its conservative security – it shows a significantly lower performance compared to other post-quantum signature schemes such as ML-DSA and FN-DSA, especially if multi-threading is leveraged. Another informative result is the small overhead of hybrid mode: of combining the fastest post-quantum schemes and classical schemes – both for key exchange as well as signing. For applications with unique performance requirements, we recommend doing similar tests to determine performance impact.

16 How to get un-stuck by Architecting for Resilience | News (https://pcsi.nl/en/news/how-to-get-un-stuck-by-architecting-for-resilience/)

17 How to get un-stuck by PQC Benchmarking test details | News (https://pcsi.nl/en/news/how-to-get-un-stuck-by-architecting-for-resilience-2/)

To support practitioners to make algorithm choices there is tooling available, such as the PQC choice assistant[18]. The PQC choice assistant is an Interactive web page that guides user through the landscape of post-quantum algorithms to find the most suitable choice.

7.2.2 Hybrid

Digital signatures are not meant to protect confidentiality, and therefore are not vulnerable to the store-now-decrypt-later attack. For signatures, the real-time access attack applies, where private (signing) keys are calculated using a quantum computer after Q-day to forge signatures, leading to a "trust-now-forge-later" scenario. Depending on how long the signatures are valid and what they are used for, this can already be a problematic attack vector. In order to clarify this, we focus on two distinct uses of signatures in a PKI.

First of all, there is the end certificate. This certificate contains the public key (verification key) of the end entity for a specific purpose, like authentication in a TLS connection. If the certificate is short-lived, *e.g.*, 47 days (CA/Browser Forum, 2024), then these keys do not necessarily need to be protected with hybrid security. In other words, we do not currently expect a need for hybrid signatures in TLS. As elaborated next, for applications outside TLS, signatures may have a much longer lifetime, such as document signing or software signing, here Hybrid would be warranted.

The connection between an end entity and their verification key, as specified in the end certificate, is determined through the certificate chain. This is the second case where signatures are relevant in a PKI. The CAs in this certificate chain might have long-lived certificates. Depending on how long exactly, it might already be necessary to migrate to post-quantum cryptography as soon as possible. In that case, it could be wise to migrate to hybrid signatures of the composite type, because they provide a security fallback in case the chosen post-quantum signature scheme turns out to be insecure against classical attacks.

In order to make this decision, it is important to consider the fact that hybrid signature schemes will have somewhat worse performance and are more complex to implement correctly, since several protocols related to PKI services are not yet equipped to deal with hybrid certificates. Additionally, conservative choices for post-quantum signature schemes exist. The most conservative choice in terms of security is SLH-DSA, because it is a hash-based algorithm and the security of hash functions has been studied for a long time and is considered well understood. For these cases, SLH-DSA can therefore be a suitable candidate without using a hybrid mode. However, as mentioned in the previous section, the performance of SLH-DSA can become a challenge. If key sizes and signature generation time are not critical to the functioning of the service, then SLH-DSA is still suitable, but if this is not the case, then a hybrid combination of a classical digital signature scheme and a post-quantum signature scheme like ML-DSA or FN-DSA might be more appropriate.

The same analysis holds for end certificates for which the verification key is used for long-lived certificates in the respective application, such as long-term contracts or other types of agreements. In these cases, the migration to post-quantum cryptography also needs to happen well in advance of Q-day and the same considerations apply.

7.2.3 Migration strategy

When concrete algorithm choices have been made, a migration strategy needs to be chosen. A common migration strategy for new generations of CAs is to set up a parallel PKI that only issues certificates of the new type. The old CA will not issue or renew certificates anymore and only support the PKI service for previously issued certificates. Certificate renewal and issuance request will therefore only be processed by the new CA. This way, there will be natural point in time when all certificates Issued by the old CA have expired, at which point the CA can be retired.

18 PQChoiceAssistant (https://tno.github.io/PQChoiceAssistant/)

This topic is further explored in HAPKIDO deliverable 6.2 (Marcus & Amadori, 2025).

The time it takes to migrate from one CA to another with this strategy depends on the validity period of the previously issued certificates. If these timelines are not appropriate, then early revocation will need to take place. Since this strategy has already been used previously for PKIs, it becomes a natural choice for the PQC transition as well, provided that the costs and overhead of a parallel PKI can be supported.

While the timeline for a cryptographically relevant quantum computer remains uncertain, the risk period for long-term data confidentiality has already begun, and regulatory pressures will accelerate migration regardless of quantum breakthroughs. With NIST's PQC standards nearing completion, the focus must shift from awareness to action. Performance benchmarks indicate that most PKI applications can adopt PQC with limited overhead, though specialised use cases may require careful algorithm selection and hybrid strategies. Ultimately, proactive planning, informed algorithm choices, and collaborative migration approaches will be essential to ensure resilience and interoperability in a post-quantum world.

8. Conclusion

Focusing on understanding the path towards hybrid quantum-safe PKIs, and devising plans to achieve it, HAPKIDO has uncovered that despite shared urgency (Chapter 2), at a *meso* level, harmonising efforts remains critical to maintaining interoperability and digital trust. This is particularly valid for **sector regulators** and policymakers. As new policies emerge at a *macro* level, concerns about cryptographic fragmentation due to differing national policies and standards become more evident (Chapter 3).

As transitions are still in the horizon, hindered by ongoing standardisation of critical PKI protocols, early migration efforts remain limited due to: hybrid functionalities which are still experimental, dependence on software and hardware vendors (Chapter 4), lack of sector-specific migration policies, and integration which often requires external providers. HAPKIDO project proposes a tool to support organisations in preparation for the impending transition (Chapter 5), and elaborates on the cryptographic primitives underlying hybrid quantum-safe PKIs (Chapter 6).

This handbook has two main goals: 1) to **educate** and create **awareness** on topics related to the transition to QS PKIs; and 2) to support discussion of next steps through **actionable insights** (see Chapter 1).

GOAL 1: EDUCATION AND AWARENESS. The first goal of education and awareness is addressed throughout this handbook: it is designed to help our audience—particularly executive leadership—understand the risks posed by the quantum threat, its potential impact on business operations, and how this knowledge can support informed decision making. This is particularly relevant in the light of recent report by Algemene Rekenkamer[19] which shows that 70% of the government organisations in the Netherlands have yet to start preparing for the quantum threat.

HAPKIDO supports both the audiences who are new to QS PKI and those seeking to deepen their expertise. To support a more advanced understanding of the topic, this handbook links to relevant HAPKIDO deliverables, helping our reader to navigate the extensive body of literature. In addition, as a more accessible educational tool, HAPKIDO also offers Massive Open Online Courses (MOOCs) in two different tracks that cover governance aspects, as well as technological challenges and solutions of Quantum-safe Digital Infrastructures.

HAPKIDO offers MOOCs in governance tracks (TU Delft, 2026a), and technological aspects of Quantum-safe Digital Infrastructures (TU Delft, 2026b).

To strengthen this first goal, we recommend that organisations and sector regulators complement this handbook with dedicated awareness raising activities, supported by the tools developed by HAPKIDO. These may include internal or cross sector campaigns, structured communication efforts, or systematic risk analyses of sensitive services to highlight the urgency of transitioning towards quantum safe PKIs.

GOAL 2: ACTIONABLE INSIGHTS. Building on knowledge acquired through the combination of multidisciplinary streams of work, HAPKIDO addresses the second goal of this handbook by making actionable recommendations in two fronts:

19 Focus op quantum bij de rijksoverheid | Algemene Rekenkamer (https://www.rekenkamer.nl/documenten/2026/02/04/focus-op-quantum-bij-de-rijksoverheid)

8.1 Meso level: Sector-specific transition plans

Migration for PKI systems should be guided by a unified governance framework that builds on existing regulations, such as eIDAS[20], and guidance by normative regulatory bodies ETSI, **while allowing sector-specific adaptations**. Although the core PKI roles and processes (CAs, RAs, VAs, certificate issuance) remain consistent across sectors, differences in hierarchy, proof of identity, and certificate attributes call for **tailored transition plans**. These plans should address hybrid approaches—combining classical and PQC algorithms—to ensure crypto and certificate agility during migration.

Sector-specific transition plans should focus on practical constraints such as certificate management, algorithm properties, hardware limitations (*e.g.*, algorithm performance on smart cards), and dependence on vendors—as vendors are often active in specific sectors—, which can impact compliance and system architecture. High-assurance environments, such as those governed by strict regulations, will require robust compliance and audit mechanisms, whereas sectors with lower trust requirements may adopt lighter solutions. To ensure interoperability, underlying sectorial policies should encourage flexibility in architecture. Ultimately, a coordinated approach—combining overarching governance with sector-specific technical guidance—will enable a secure, efficient, and interoperable PQC migration across diverse PKI ecosystems.

While there are some heavily regulated sectors, like banking, for which a centralised governance mechanism is possible, it is much more common for sectors to be decentralised. Devising a successful sector-specific transition plan is best done collaboration, but not every sector has formalised lines of communication to facilitate this. Since there is not much hierarchy between actors on the meso level, decision-making must be aligned, as well as incentives regarding individual organisations.

8.2 Micro level: Proactive testing and collaboration

In order to achieve such coordinated approach, we suggest organisations first adopt a **proactive testing strategy** (*e.g.*, by participating in testbed consortia) before formal hybrid standards are finalised, in order to educate and prepare for cross-organisation conversations.

Migrating the PKI infrastructure itself is expected to be relatively straightforward due to centralised control over hardware and software, and largely due to the fact that transition here falls more in line with traditional technology governance. However, the real complexity will lie in migrating PKI-dependent applications, which are decentralised and managed by diverse vendors. Early testing of hybrid approaches—such as implementing “hybrid OR” mode for backwards compatibility—will help identify interoperability issues and performance constraints. Also reducing risks when transitioning to “hybrid AND” mode in a following stage, where downgrade attacks are no longer possible. Such early testing should be conducted as much as possible, despite the non-finalised standards and incomplete integration in cryptographic libraries.

In addition to technical readiness, **collaboration within sectors and with software vendors** is critical. Vendors will make different design choices based on market priorities, so **joint testing environments**, shared toolkits, and migration guidelines should be developed to foster consistency and interoperability. Investing in these collaborative efforts now will accelerate adoption, minimise fragmentation, and ensure that both PKI systems and applications can transition smoothly once hybrid standards are formalised.

20 Regulation - EU - 2024/1183 - EN - EUR-Lex (https://eur-lex.europa.eu/eli/reg/2024/1183/oj)

As this handbook is published, at a macro level the European Commission works on a proposal for amendments to the Network and Information Security Directive (NIS2) that includes "*the requirement for Member States to adopt policies for the migration to post-quantum cryptography (PQC) as part of their national cybersecurity strategy*". Embedding such a requirement within regulatory frameworks underscores the strategic importance of timely migration, and helps clarify priorities and unlock resources to pilot quantum-safe transitions, such as funding, incentives, and sector specific support mechanisms. This is especially significant for providers of essential services, including government, financial services, telecommunications, and healthcare, where early adoption will be crucial for the resilience of national and European digital infrastructure.

9. Appendices

9.1 Glossary of acronyms

Acronym	Explanation
CA(s)	**Certificate Authority** — responsible for issuing certificates in a PKI. The CA can have additional services such as tracking revocation information, but these can also be delegated to other authorities.
CRQC	**Cryptographically Relevant Quantum Computer** — A fault-tolerant quantum computer with enough computing capacity to run algorithms that break classic cryptography. CRQC is expected to emerge within the next decades.
FN-DSA	**Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm** — A lattice-based digital signature scheme selected, and soon to be standardised by NIST. Formerly known as Falcon.
HAPKIDO	**Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations** — A research project granted by the Dutch Research Council (NWO).
HSM	**Hardware Security Module**.
KEM	**Key Encapsulation Mechanism** — A cryptographic mechanism used to securely distribute keys.
ML-DSA	**Module-Lattice-based Digital Signature Algorithm** — A lattice based digital signature scheme standardised by NIST. Formerly known as CRYSTALS-Dilithium.
ML-KEM	**Module-Lattice-based Key Encapsulation Mechanism** — A lattice based key encapsulation mechanism standardised by NIST. Formerly known as CRYSTALS Kyber.
NCSC-NL / UK	**National Cyber Security Centre** – Netherlands / United Kingdom.
NIST	**National Institute of Standards and Technology** — runs the PQC standardisation process and publishes PQC algorithm standards.
PQC	**Post Quantum Cryptography** — A class of cryptographic algorithms resistant against both classical and quantum technology based threats. Interchangeably called Quantum-safe cryptography in this book.
PKI	**Public Key Infrastructure** — the trust mechanism used to couple identities to cryptographic keys, relying heavily on asymmetric cryptography.
OID	**Object Identifier** — Unique identifiers for algorithms and parameter sets in cryptographic protocols.
Q-day	Theoretical day of arrival of the CRQC.
QS	**Quantum-safe**.
SLH-DSA	**Stateless Hash-Based Digital Signature Algorithm** — A hash-based digital signature scheme standardised by NIST. Formerly known as SPHINCS+.

Acronym	Explanation
SNDL	**Store Now Decrypt Later** — an immediate quantum threat which is hard to detect where encrypted data is collected today to decrypt once a CRQC becomes available. Also referred in the literature as Harvest-Now-Decrypt-Later (HNDL).
SRA	**Societal Risk Assessment** — method developed in HAPKIDO to assess societal risks of quantum threats on PKIs.
TLS	**Transport Layer Security** — commonly used protocol that uses certificates for secure communication.

9.2 Authors Biography

Dayana Spagnuelo, Ph.D. (TNO). *Editor of this book.*
Dayana is a researcher specialised in information security and its interplay with regulatory requirements. Her research focuses on how current and future digital solutions should be tailored to accomplish principles of privacy and confidentiality. In HAPKIDO, she has contributed to the Societal Impact Analysis (WP1), Requirements gathering (WP2), Migration Architectures (WP6), and Dissemination & Education (WP8).

Alesandro Amadori, Ph.D. (TNO)
Alessandro is a cryptographer at TNO. His current focus is on the migration to post-quantum cryptography. He is part of the HAPKIDO Project where he contributes to the realisation of proof-of-concepts. In HAPKIDO, he has contributed to the Hybrid QS-PKI system (WP4), Requirements gathering (WP2), Migration Architectures (WP6), and Dissemination & Education (WP8).

René Bakker, MA MSc (TNO). *Project lead of HAPKIDO.*
René is project manager at the department of Applied Cryptography and Quantum Algorithms. He has a background in cyber security (University of Leiden) and worked previously in privacy and security related fields. Currently he is in charge of several projects regarding applied cryptography, for instance for the AIVD, department of Economic Affairs, and several B2B clients. Next to project management he has contributed to the Dissemination & Education work (WP8).

Stefan van den Berg, MSc (TNO)
Stefan is a cryptographer at the department Applied Cryptography and Quantum Algorithms at TNO. He has a background in information security and embedded systems. His work focuses on development of various Privacy-Enhancing Technologies, Post-Quantum Cryptography solutions and Quantum Applications. In HAPKIDO, he has contributed to the Hybrid QS-PKI system (WP4), and Dissemination & Education (WP8).

Nitesh Bharosa, Prof.dr.ir. (TU Delft)
Nitesh Bharosa is Full professor of 'GovTech & Innovation' at the Faculty of Technology, Policy and Management of Delft University of Technology. His research focusses on designing and governing GovTech solutions in Digital Public Infrastructures. In HAPKIDO, he has contributed to the Societal Impact Analysis (WP1), and Dissemination & Education (WP8).

Lærke Christiansen, MSc (TU Delft)
Lærke Christiansen is a PhD Candidate in Technology Governance and Serious Gaming at the Delft University of Technology. With a background in Anthropology and Sociology of Law she uses a social science lens to research how a serious game can be used to facilitate collective action in migrating to quantum-safe PKI systems in the Netherlands.
In HAPKIDO, she has contributed to the Governance Transition (WP3), and Dissemination & Education (WP8).

Serge Fehr, Prof.dr. (CWI)
Serge Fehr is a researcher at CWI and a professor in the Mathematical Institute at Leiden University. His research focuses on cryptography and quantum information science: how does the cryptographic landscape change when considering information-processing devices that behave according to the laws of quantum mechanics? In HAPKIDO, he has contributed to the Cryptographic Tools (WP5), and Dissemination & Education (WP8).

Ini Kong, MSc (TU Delft)
Ini Kong is a PhD researcher at Delft University of Technology. Her research focuses on developing a growth model-based roadmap for organisations to achieve quantum safety. This involves analysing activities, organisational capabilities, and governance needed to progress from one stage to the next. In HAPKIDO, she has contributed to the QS-PKI transition roadmap (WP7), and Dissemination & Education (WP8).

Michiel Marcus, MSc (TNO). *Reviewer of HAPKIDO deliverables.*
Michiel is a cryptographer within the Applied Cryptography and Quantum Algorithms department of TNO. He specialises in post-quantum cryptography and the formal verification of cryptography, which are both essential in the upcoming migration to post-quantum cryptography. In HAPKIDO, he has contributed to the Migration Architectures (WP6), and Dissemination & Education (WP8).

Manon de Vries, MSc (TNO). *Scientific lead of HAPKIDO.*
Manon is a cryptographer within the Applied Cryptography and Quantum Algorithms department of TNO. She specialises in PKI, cryptography in practice and cryptographic architecture. In HAPKIDO, she has contributed to Dissemination & Education (WP8).

HAPKIDO

A consortium of

TU Delft

TNO innovation for life

ZYNYO.

kpn

Microsoft

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CWI
Centrum Wiskunde & Informatica

NWO

HAPKIDO is funded through the NWO-programme
'Cybersecurity - Naar een veilig en betrouwbaar digitaal domein'.