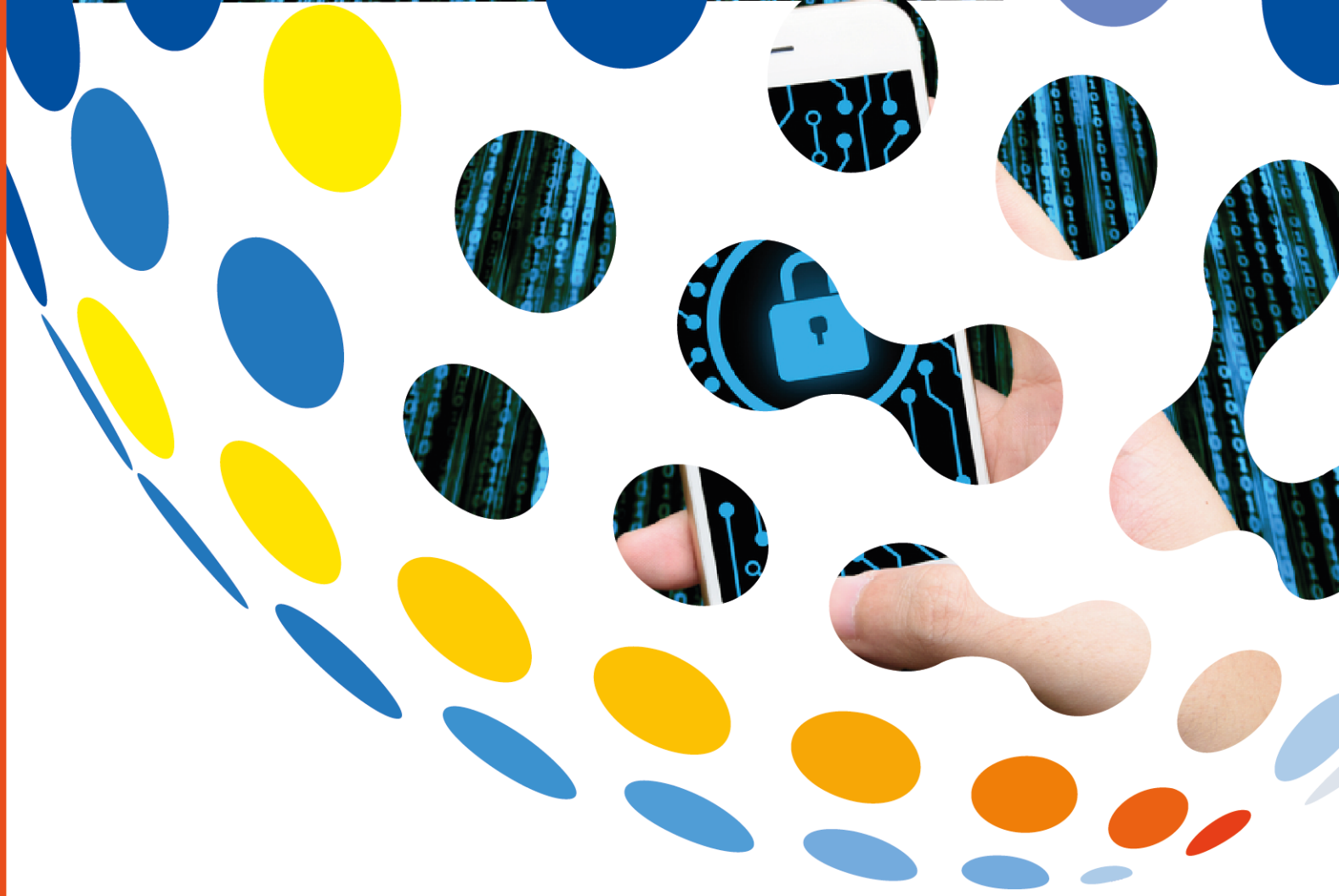

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025

NIS COOPERATION GROUP

Contents

---

1 Executive Summary

Digital infrastructures require robust cybersecurity. Cryptographic systems are vital to protect the confidentiality and authenticity of data. Quantum computing will be a threat to many of the cryptographic algorithms used to achieve these protection goals. Data that is currently not quantum-safe, whether it is stored or transmitted, and that must remain confidential for a long time, may be compromised in the future by quantum computers ("store now, decrypt later" attacks). In addition, authenticity will also be jeopardised by quantum computers. The threat that quantum computing poses to cybersecurity can be countered by a timely, comprehensive and coordinated transition to post-quantum cryptography (PQC).

Consequently, on 11.04.2024, the European Commission published a "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography" [1]. For the development of this "Implementation Roadmap" the Commission recommended to establish a work stream on PQC within the NIS Cooperation Group (NIS CG).

This document is the first deliverable of the NIS CG work stream on PQC and is meant to be a first high-level paper aimed at the Member States. The set of recommendations that Member States need to implement for a synchronised transition to PQC are divided into *First Steps* that are required to initiate the transition, and *Next Steps* that should follow. The recommendations in this document include measures to ensure that all stakeholders are well informed of the quantum threat to cryptography and can exchange their knowledge and experience, at national, European and international level. It is recommended to

ensure that the quantum threat becomes a part of risk management of all relevant entities and to establish mature cryptographic asset management to facilitate the transition to PQC and to improve cryptographic agility in general. Many of the steps highlighted in this document for the PQC transition constitute "no-regret" moves; they improve cybersecurity in general and support the compliance with cybersecurity regulations, in particular the NIS2 Directive [2].

In addition to these recommendations, this document presents a recommended timeline for the transition to PQC in the European Union, taking into account the current assessment of the status of quantum computer development by the German Federal Office for Information Security (BSI) and in line with the recent publication "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography" [3], a joint statement by partners from 21 European states.

In particular, it is recommended that all Member States initiate a national PQC transition strategy following *First Steps* by the end of 2026 and coordinate their efforts at the EU level. At the same time, high-risk use cases should be transitioned to PQC as soon as possible, no later than the end of 2030. Furthermore, quantum-safe upgrades should then be enabled by default and the PQC transition plans should be refined, in particular by implementing the recommended *Next Steps*. By 2035, the transition should be completed for as many systems as practically feasible. This ambitious timeline is justified by the severe consequences broken cryptography would have on safeguarding data and securing sensitive communications which are vital for the EU's and its Member States' society, economy, security and prosperity. When migrating to post-quantum cryptographic solutions, it is recommended to use standardised and tested hybrid solutions, whenever feasible and suitable.

Over the past years, the EU has put in place a strong strategic, policy and legislative framework to strengthen the EU's cybersecurity and collective resilience. In particular, the NIS 2 Directive [2] and the Digital Operational Resilience Act (DORA) [4] require entities in scope to adopt cybersecurity risk-management measures, including on the use of state-of-the-art cryptography, and provide that the entities' management bodies can be held liable for failing to comply with these requirements. Furthermore, the Cyber Resilience Act (CRA) [5] lays out horizontal cybersecurity requirements for all products with digital elements placed on the EU market starting from 11.12.2027, including a requirement to protect confidentiality through encryption where relevant. The necessity to ensure the authenticity and integrity of software and firmware upgrades and the very capability of the devices to be upgraded for compliance with the likely evolving landscape of PQC standards is of relevance for manufacturers, and in particular for Member States as they prepare for the implementation of the CRA and its future enforcement. Additionally, the development of harmonised standards, which includes the participation of various stakeholders including academia, industry and public bodies, should also consider the timeline mentioned in this document. The Commission also designs actions to support standardization activities which are issued within the Union Action Plan for Standardization.

2 Introduction and motivation

Cryptography is crucial to securing a broad range of services having a direct impact on our daily lives. Those encompass, for instance, digital government services, the banking system, and communication services such as messaging apps. Cryptography is vital to ensure the secure operation of all of our critical infrastructures.

If the currently deployed cryptography was to be broken, the consequences on digital infrastructures would be devastating. The development of quantum computers poses such a threat to cryptography. This is known since 1994, when Peter Shor published quantum algorithms, which can be used to break many of the cryptographic algorithms in use. The foundation of our secure digital infrastructures would thus be undermined if these algorithms could be implemented on a sufficiently powerful quantum computer.

There is currently no evidence that this is already possible. Nevertheless, in 2015 the US National Security Agency (NSA) issued an urgent warning about the imminent threat to current quantum-vulnerable cryptography posed by the development of quantum computers. European agencies have also publicly informed about this threat from early on, e.g. in [6]. In order to properly assess the current state of development or the potential future availability of quantum computers, the study "Status of quantum computer development" was initially conducted on behalf of the BSI from 2017 to 2020 and has most recently been updated in 2024 [7]. This updated assessment shows that it is likely that such a quantum computer will be feasible in a maximum of 16 years (i.e. by 2040 or earlier). However, this period could be significantly reduced to 10 years if current heuristics in error correction and mitigation as well as quantum computer hardware are fully verified. The most recent "Quantum Threat Timeline Report" [8] by the Global Risk Institute provides opinion-based estimates of leading experts for the likelihood of a quantum computer being able to break RSA-2048 in 24 hours. They estimate that there is a 19%-34% chance that it will happen within the next decade.

Even though it remains impossible to precisely predict when quantum computers will be able to compromise the quantum-vulnerable cryptography currently in use, the impact of such an event necessitates that certain organisations should already start working on mitigating measures now. The most promising solution is so-called post-quantum cryptography (PQC). PQC can be implemented on currently used systems and computers, but it is designed with the goal to be secure against quantum computers. However, the transition from quantum-vulnerable cryptography towards PQC will require significant time and resources. Judging from previous transitions this process might take well over five years.

Two main threat scenarios are currently of concern:

- The "store now, decrypt later" scenario, where adversaries store encrypted data for decryption once a cryptographically relevant quantum computer emerges. This is a threat when the confidentiality of data needs to be protected for a long time period (for instance governmental data, sensitive personal data, trade or business secrets).
- Long transition periods, which occur for complex systems such as public-key infrastructures (PKIs) or devices with a long lifetime. Even if a system is not affected by ongoing attacks, as in the first scenario, there is a risk that the transition to quantum-safe cryptography might not be completed in time, potentially compromising the confidentiality and authenticity of all communications.

Therefore, the PQC transition requires a well-prepared, systematic and persistent treatment. National governments will have to act now in order to complete the transition to PQC in time and shall be supported by the European Union in this process.

3 Scope and definitions

3.1 Scope

The document at hand is the first deliverable of the NIS CG work stream on PQC. It is meant to be a first high-level concept paper on the transition to PQC aimed at the Member States. With some adaptions this document will also be useful for government organisations and other entities including the ones that have to comply to the NIS2 Directive.

There exist already several publications with information about and guidance on mitigating the quantum threat on cryptography such as [3], [9], [10] [11], [7], [12], [13], [14], [15], [16], [17]. (The list is certainly not exhaustive.)

This document represents the first release of the Coordinated Implementation Roadmap as per the Commission's Recommendation. Public administration entities and other critical infrastructures, notably those in scope of the NIS2 Directive should refer to this document and its further releases to ensure a synchronised transition through the whole EU.

This first release of the Coordinated Implementation Roadmap contains a recommended timeline for the PQC migration of the Member States and a list of measures which are to be included in national PQC roadmaps of each Member State, taking into account and pointing to the existing literature where appropriate to avoid duplication of efforts. The timeline is outlined in the next section and the measures are divided into *First Steps* and *Next Steps* to guide the Member States setting up their national programs. Later versions and additional parts of the Coordinated Implementation Roadmap will provide more (technical) details and define further recommended measures, after consultations with governments, industry, and academia.

3.2 Definitions of frequently used technical terms

cryptographic agility (or crypto-agility)
: The design of cryptographic protocols and systems in a modular way that enables replacing the cryptographic components. This concept must not be confused with a requirement to negotiate the cipher suite during protocol execution; the latter often leads to downgrade attacks if not done very carefully.

cryptographic inventory
: A structured overview of cryptographic assets.

cryptographically relevant quantum computer
: A quantum computer that is powerful enough to solve factorization and discrete logarithm problems of sizes that are used in quantum-vulnerable cryptography today.

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

post-quantum cryptography (PQC)
: Asymmetric cryptographic algorithms that are developed and designed to be secure against traditional and quantum attacks.

public-key infrastructure (PKI)
: A framework for issuing, maintaining, and revoking public-key certificates.

quantum attack
: Using a cryptographically relevant quantum computer running a quantum algorithm to attack a cryptographic algorithm.

quantum-safe
: Something that is expected to be secure against traditional and quantum attacks. This term also covers symmetric cryptography algorithms.

quantum-vulnerable
: Not quantum-safe. Cryptographic algorithms that are expected to be vulnerable to quantum attacks.

traditional
: Quantum-vulnerable (for a cryptographic mechanisms) or non-quantum (e.g. for attacks) depending on the context.

4 Timeline

4.1 Overview

The European Commission's "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography" [1] suggested that such a roadmap should be published within two years after publication of the recommendation (i.e. by April 2026). A development and further adaptation of national PQC transition plans should follow in accordance with the principles set out in the Coordinated Implementation Roadmap. However, as the transition process is expected to take many years, it seems prudent to act as early as possible and in particular not to wait for the final deliverable of the work stream. Consequently, this document provides initial guidance and is aimed at facilitating a swift transition to PQC across the EU and ensure a minimum level of readiness in all Member States by the end of 2026.

In general, a risk-based approach for the PQC transition is recommended. However, as a first guideline, the NIS CG work stream on PQC has developed an initial recommended timeline, which is summarised below. On the one hand, this timeline takes into account that the transition requires some time, and on the other hand, it is based on the latest update of the study "Status of quantum computer development" [7]. It is important to note that immediate action is required and since it will not be possible to transition all public-key cryptography in use at once, clear priorities need to be established, which are reflected in the timeline.

At this point, this document does not contain detailed technical recommendations. However, when migrating to post-quantum cryptographic solutions, it is recommended to use standardised and tested hybrid solutions, whenever feasible and suitable. In particular, whenever a quantum-vulnerable public-key cryptographic mechanism, such as RSA or any discrete logarithm based mechanism, is currently used, replacing it by a standardized hybrid combination which includes PQC should be considered. For high-risk use cases, quantum-vulnerable public-key mechanisms shall not be used stand-alone after the end of 2030, analogously after the end of 2035 for medium-risk use cases. It should be noted that alternatives, such as using symmetric methods instead of public-key cryptography are also worthwhile to consider, depending on the application.

For most applications, adhering to the recommended timeline should provide adequate protection from the quantum threat while avoiding a chaotic transition that could introduce new vulnerabilities from insufficiently tested solutions. However, if the recommended deadlines cannot be met, the individual risk has to be evaluated. This might encompass closely monitoring quantum computing developments and considering other (ad-hoc, possibly temporary) measures. It might even require a more sophisticated threat

analysis to minimise the impact of the quantum threat in the future.

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

4.2 The timeline in detail: Milestones, first and next steps

1. The work stream on PQC has identified a set of initial measures (see *First Steps*), which:
   - are required for a successful transition;
   - can be initiated now;
   - will also facilitate cryptographic agility.

   In particular, all Member States should start initiating or updating their national transition plans in 2025 to implement the steps described in this document. Member States should ensure the measures listed in *First Steps* are accomplished before the end of 2026 and are encouraged to provide regular status updates to the work stream on PQC to ensure a harmonised implementation.

   On the deployment side, it is important that Member States initiate the transition by running pilots and starting the transition of high-risk use cases. The recommended steps and milestones which should be reached by the end of 2026 are summarised in the box "Milestone 1", but we refer to *First Steps* for details on these measures. It is important to note that the list of steps to complete should not be seen as exhaustive and additional measures might be identified at the national level or within the work stream on PQC. They might also be reflected upon in additional parts of the roadmap. Furthermore, it is also crucial that Member States do not wait until the end of 2026 to start implementing the *Next Steps*. These should also be initiated as soon as possible but might take more time to complete.

Milestone 1: 31.12.2026

- First Steps:
  - Identify and involve stakeholders.
  - Support mature cryptographic asset management.
  - Create dependency maps.
  - Perform quantum risk analysis.
  - Include the supply chain.
  - Create a national awareness and communication program.
  - Share knowledge and get involved with the NIS CG work stream on PQC.
  - Develop a timeline and an implementation plan.
- **Main achievements**:
  - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
  - Initial national PQC transition roadmaps have been established by all Member States.

2. This document provides some guidance on identifying relevant use cases by defining three quantum risk categories: "low", "medium" and "high". For some background on estimating the quantum risk and these risk categories, see *Estimating the quantum risk*. When confidentiality of data is protected using public-key cryptography, this document considers a use case as *high-risk* if compromising confidentiality after 10 years or more would still cause *significant damage*. This implies in particular that attackers have a strong motivation to capture and store such encrypted information even today in order to break the encryption in the future. Taking the estimates from [7] into account, data that needs to remain confidential for at least 10 years should be protected from quantum computer attacks starting no later than by the end of 2030. This recommendation is in agreement with the joint position paper 'Securing tomorrow, today' [3], which strongly advises to take action immediately to ensure confidentiality of the most sensitive use cases and to protect them by 2030 the latest. Note that the recommended deadline may in fact not always be sufficient and a national implementation plan should prioritise protecting the most critical assets. Also note that unexpected advances in quantum computing could warrant an acceleration of the transition process.

   While safeguarding encrypted traffic and data at rest from quantum attacks in the future has the highest priority, the transition plan has to take into account that the transition of systems with a long life-cycle or of complex systems (such as PKIs) to PQC will take a lot of time. Therefore, it is necessary to plan the migration of these systems well in advance. Consequently, it is recommended to start developing detailed transition plans for these systems as soon as possible. This should include running pilots and testing to ensure business continuity.

Milestone 2: 31.12.2030

- Next Steps:
  - Support cryptographic agility and a quantum-safe upgrade path.
  - Allocate resources for the transition.
  - Adapt certification schemes.
  - Evolve the rules.
  - Look for opportunities within the ecosystem.
  - Considering transversal activities throughout the creation and implementation of the roadmap.
  - Implement pilot use cases and contribute to testing centres.
- **Main achievements**:
  - The PQC transition for high-risk use cases has been completed.
  - PQC transition planning and pilots for medium-risk use cases has been completed.
  - Quantum-safe software and firmware upgrades are enabled by default.

An integral part of a transition plan beyond 2030 is a quantum-safe upgrade path. It is therefore highly recommended to ensure that products entering the market with an expected lifetime beyond 2030 should be upgradable to PQC and that the upgrade mechanism for software and firmware upgrades should incorporate post-quantum signature schemes for integrity and authenticity.

Again, the recommended deadline is also based on the quantum computer study [7] and the estimate that it might easily take about 5 to 10 years to fully migrate all relevant systems to PQC. Note that all of these steps need to be initiated as soon as possible, and waiting for the completion of Milestone 1 cannot be afforded.

3. Member States should aim at transitioning as many systems as feasible by the end of 2035 and prioritise completing the transition for medium-risk use cases. This date is based on the following considerations. In the recently published initial public draft of NIST IR 8547 [18], it is stated that traditional public-key cryptographic mechanisms will be disallowed after 2035. This date is based on the goal set out in the US National Security Memorandum 10, namely for the USA "of mitigating as much of the quantum risk as is feasible by 2035." Similarly, the recently published timeline of the UK NCSC [19] sets 2035 as the target date for the PQC transition. Therefore, the milestone to complete the PQC transition for high- and medium-risk use cases aligns the EU well with the international ecosystem.

5 Estimating the quantum risk

This document advises to perform a quantum risk analysis to help prioritisation of the transition process. In the future, the quantum risk should be integrated into the regular risk management. For the quantum risk analysis, we use the model described in Section 2.4 of "The PQC Migration Handbook" [17], which is compatible with the general IT risk

management methodology as defined in ISO standard 27001 and national standards such as BSI-Standard 200-3 "Risk Analysis based on IT-Grundschutz" [20].

The recommended *Timeline* distinguishes between the three basic quantum risk levels "high", "medium" and "low". These risk levels are defined based on the quantum risk score defined in Figure 2.7 of [17]. Following this approach, the quantum risk level of a use case (an application or system) is influenced by three factors:

- the quantum weakness of the cryptography used;
- the expected impact of the used cryptography being broken;
- the estimated time and effort required to migrate to PQC. This methodology incorporates the quantities present in "Mosca's theorem" [8] but focuses on the parts that are under the control of the organisation responsible for the transition. The estimated time until a cryptographically relevant quantum computer will be available is, however, factored into the dates given for the transition outlined in the previous section.

The PQC Migration handbook assigns scores for these three factors and gives a mapping to an overall quantum risk score. The mapping to the three risk levels "high", "medium", and "low" used in this document is as follows.

Quantum risk score following in Figure 2.7 of [17]	Quantum risk level in this document
1	low
2	medium
3 – 4	high

Note that while the PQC migration handbook also uses the term "acute risk" when the quantum risk score is 4, for the purpose of this document, three risk levels are sufficient.

In the following, a very rough classification for a use case in which confidentiality and authenticity is currently protected by traditional (quantum-vulnerable) *public-key* cryptography is given.

- If confidentiality needs to be protected, then the quantum risk level is medium or high.
- If confidentiality needs to be protected for a long time period (at least 10 years), and an attack after 10 years or more would still have significant impact, then the quantum risk level is high.
- If the transition effort is high (taking more than 8 years), the quantum risk level is medium or high.
- If the transition effort is high (taking more than 8 years) and the impact of an attack is high, for example for securing software updates, the quantum risk level is high.

The second example implies in conjunction with the recommended *Timeline* that when long term confidentiality needs to be protected, the PQC transition needs to be completed as soon as possible and latest by the end of 2030. The last example highlights the need to secure software and firmware updates with quantum-safe signatures as soon as possible, which is reflected in the recommended *Timeline*.

6 Steps towards the PQC migration

6.1 Introduction

This section describes recommended steps, including "no-regret" moves, to initiate the creation of a national PQC roadmap, as described in *Scope and definitions*, and highlights again that Member States should start to act now. The "no-regret" moves support the improvement of overall cybersecurity maturity and the compliance with cybersecurity regulations like the NIS2 Directive [2]. Because of the complexity and large scale as well as the many uncertainties and rapid developments, no entity or Member State can or should perform this transition in isolation.

6.2 First Steps

- *Identify and involve stakeholders.* Due to the large scope and the complexity of the transition, it is essential to involve important (national) stakeholders right from the start and their strategic advice has to be managed in an organised manner. Stakeholders to be considered include CTO, CISO, and CIO functions from ministries, large government organisations and other critical entities, as well as representatives from science and research who are concerned with PQC developments. Further relevant stakeholders are for instance the National Cybersecurity Authority, the National Cybersecurity Certification Authority (NCCA) in the context of the Cybersecurity Act (CSA) [21] and the National Coordination Centre (NCC). It is important to also involve supervisory bodies for e.g. NIS2 and eIDAS and enable close cooperation between regional and local authorities, as well as all providers of critical infrastructures. The advice on strategic matters is key for the development of a national roadmap for the transition to PQC and the implementation of this roadmap. The stakeholders should be in close cooperation with the national body or bodies in charge of the national PQC roadmap. As a practical example, France has conducted surveys to determine market readiness, identify obstacles for the PQC transition and to learn about the needs of three types of stakeholders: providers, users, and consulting companies [22].
- *Support mature cryptographic asset management.* A first essential step and "no-regret" move for every entity is to create and maintain current inventories of assets that perform cryptographic operations and of assets that have cryptographic operations performed on them as part of asset management. Such inventories support incident and vulnerability management as part of the general IT controls, not only related to the quantum threat. They support the reliability and continuity of the processes and services for which they are being used; both on premise and in the cloud. Member States should promote and support that useful cryptographic inventories are being created and maintained. Some regulatory requirements on keeping cryptographic inventories already exist but might have to be amended with information relevant to the PQC transition. Generating and maintaining cryptographic inventories can be aided by tools (discovery and asset management tools). Using a standardised format for a cryptographic inventory, like CBOM (Cryptographic Bill of Materials, an extension of the SBOM standard), is recommended.
- *Create dependency maps.* Entities should do a mapping of dependencies for applications, products, platforms, operations, looking at both internal dependencies and third party dependencies. This dependency mapping will eventually be driven by supply chain dependencies. It will help identifying the migration constraints and the design of an efficient planning. It supports the alignment with the supply chain and

a full asset lifecycle. Essential information for prioritisation and planning can only be provided after this step. Guidance on and an example of such dependency analysis can be found in [12]. The mapping activity will also allow to identify the interdependencies of applications and platforms that permit the provision of cross-border services in view of starting an alignment for interoperability at EU level.

- *Perform quantum risk analysis.* Member States should encourage public administrations and other critical infrastructures, notably entities in scope of the NIS 2 Directive, to include the quantum threat to cryptography in their top-level risk management. This ensures that the threat and risk is being discussed and evaluated at the board level. If a Member State publishes a relevant national (e.g. annual) cybersecurity threat or risk report which organisations can refer to, it is highly recommended to include information about the quantum threat to cryptography in this report.
- *Include the supply chain.* Every organisation also needs to start the dialogue with product and service suppliers because the transition depends on them. They need to integrate PQC and cryptographic agility (see also the *corresponding item* in *Next Steps*) in the development of their product/service roadmap, seeking alignment with the PQC roadmap, nationally and across the EU.
- *Create a national awareness and communication program.* All relevant organisations and entities have to be aware of the threat of quantum computers to public-key cryptography and the urgency to start preparing now. To support this, it is necessary to develop an awareness and communication program. This awareness program is likely to include all personnel and stakeholders who play a role in this transition: the board and management, C-level, and IT and OT related personnel (like developers, system administrators, IT and enterprise architects). Such program should consider:
  - *Customised awareness*. Because the different stakeholders have different roles in the transition, the impact of the threat on their responsibilities and tasks will differ. Therefore, a one-size-fits-all approach for awareness is not sufficient. A general introduction can be provided, but it is essential to communicate with all stakeholders using their specific terminology to ensure that the message aligns with their daily work. It is also recommended to not only inform all stakeholders, but also to discuss their concerns and needs. Since developments are progressing fast, it is necessary to regularly update the awareness program and key messages for the stakeholders.
  - *Means of communication*. In order to reach and maintain the required level of awareness, it is not enough to only have awareness activities. Different means of communications should be used to support awareness and create an adequate sense of urgency. It is recommended to publish relevant information on a well recognisable platform, including on issuance and update of guidelines from different entities, on advises from the main stakeholders, and on PQC national and international events. The awareness program should also take into account communication via social media, professional magazines and key messages from politicians and top-level management at influential conferences and events.
- *Share knowledge and get involved with the NIS CG work stream on PQC.* Because of the complexity and large scale as well as the many uncertainties and rapid developments, no entity or Member State can or should perform this transition in isolation. In cyberspace all nations are connected across borders, and depend on each other also in this transition. Therefore, Member States should create an environment or com-

munity where organisations, entities and stakeholders can share knowledge and experiences. Member States should also create opportunities for dialogues with other Member States in case of existing cross-border services. These services require a synchronised transition (plan) that needs to be agreed upon by the Member States concerned. Furthermore, we highly recommend every Member State to follow standardisation activities in the field of PQC and participate in an active way in the NIS CG work stream on PQC. This will not only help to synchronise the PQC transition in the EU as a whole, but will also help all individual Member States to be able to reach a state of readiness in order to be quantum-safe in time.

- *Develop a timeline and an implementation plan.* Member States should define priorities for the national roadmap and develop an implementation plan consistent with the prioritisation. This allows to develop a timeline, which should reflect the major milestones of the recommended *Timeline* but should also take each Member States individual situation into account. For such a plan, it can be helpful to include three high-level steps: "prepare", "plan", and "act". However, it should be noted that these are not three consecutive phases of the PQC transition, but rather follow different timelines for each individual use case.

6.3 Next Steps

After work on the *First Steps* has been started and an initial implementation plan has been established, it is important to pursue activities that could help to carry out a smooth migration and to fine-tune and update the implementation plan continuously. Further actions which should be considered in this process are listed below.

It is advised to consider the steps outlined below as soon as possible and not wait for completion of the *First Steps* or the end of the year 2026. For instance, certified qualified electronic signature creation devices including PQC must be available to allow for integration in the systems of trust service providers, migration of their customers and carrying out conformity assessment and supervision.

- *Support cryptographic agility and a quantum-safe upgrade path.* When new products are being developed, support for cryptographic agility should be considered at first. Then, from December 2027, it would need to be systematically implemented according to the CRA. One important example in this context is to provide a quantum-safe upgrade path, i.e. even if a product is not fully transitioned to PQC, the software and firmware upgrade routines should use quantum-safe signatures. This allows safely upgrading the product to PQC when the quantum threat becomes imminent. This assumes that cryptographic mechanisms used by a product can be updated, which is a basic requirement for cryptographic agility. Moreover, the deployment of standardised post-quantum signature schemes is highly recommended. The PQC migration handbook [17] contains more detailed information on cryptographic agility. Dialogue with all stakeholders and with vendors should be continued. This would lead to an iterative refinement of migration plans. Cryptographic agility should be discussed with all stakeholders and should be considered in the national procurement process when the firsts steps are completed or earlier on for mature entities. One may also consider to include cryptographic agility in evaluation of NIS2 conformity.
- *Allocate resources for the transition.* The PQC migration certainly requires resources – budget and personnel –, thus Member States should estimate and ensure that adequate resources are allocated at all levels. Furthermore, organisations should be encouraged to make budget reservations in their life-cycle management.

- *Adapt certification schemes.* Certification schemes, including national and European cybersecurity certification schemes (adopted pursuant to the CSA) should take arising threats posed by quantum computers into account. Existing work in this domain includes the European Cybersecurity Certification Group Agreed Cryptographic Mechanisms document [23] which applies to security certifications of IT products within the EU Cybersecurity Certification Scheme on Common Criteria (EUCC). In particular, version 2 of this document includes algorithm recommendations for PQC. In general, actors in the field of certification, in particular the European Cybersecurity Certification Group, need to be consulted and involved in the PQC transition. In parallel, the CRA should make it possible to initiate a dialogue to integrate PQC in products. By imposing PQC measures on products, the EU will ensure that there is an industrial supply to respond to the quantum threat. Member States should also consider connecting to NIS2 and eIDAS supervisory bodies, as well as CRA market surveillance authorities to understand the implications of the quantum threat for regulated entities.
- *Evolve the rules.* Member States might have national and sectoral laws/regulations (or cryptographic recommendations from national authorities) with technical requirements. A complex initial task will be to identify these regulations and cryptographic policies, and then systematically update them with state-of-the-art recommendations for PQC. If no such regulations or cryptographic policies exist, Member States should consider creating them, for example by consulting other countries and the NIS CG. Mass adoption will require both the availability of the products and example set by institutions. Member States should consider starting integrating PQC requirements in their future national procurement processes and are encouraged to contact their current IT suppliers to assess their maturity on PQC. If their national procurement usually requires a certain level of assurance (e.g. via certification), it will be necessary to assess the potential needs for new certifications to be issued, and therefore work with evaluation centres to build them and established, with the industry, a timeline for PQC product availability.
- *Look for opportunities within the ecosystem.* As outlined in *First Steps*, connecting stakeholders will be the key to a smooth, global transition. In particular:
  - With the private sector: Member States should discuss transition plans with product suppliers, and with service providers that will create consultancy services for the transition, in order for them to plan the migration of their offered services (e.g. advice on integrating hybrid mechanisms or cryptographic agility). Member States should open the dialogue with them about the development of their product/service roadmap regarding PQC to seek alignment with the national roadmap.
  - With training programs: Member States should identify existing training programs on PQC and cybersecurity/cryptography in general in their country, in order to enhance them with PQC information. Member States could also consider creating an informative basis to help the trainings in this process. The training should be tailored towards specific audiences, and Member States should share experiences and educational opportunities with each other.
  - With funding programs: Member States should consider integrating PQC migration-related actions (for asset inventories, enhancing PQC products, creating migration services, promoting user adoption, etc.) in national funding programs. Member States should also open the dialogue with their National Coordination Centre (NCC) and national European Cybersecurity Competence centre

(ECCC) Governing Board members to learn more about existing European funding opportunities and sharing with them useful input for defining future funding opportunities. Member States should seek feedback on existing funded projects (national and European) and their status to see how it could help with their own national roadmap.

- *Include transversal activities throughout the creation and implementation of the roadmap.* International standards are essential for an orderly transition and PQC standardisation efforts are underway worldwide and in Europe. If Member States' authorities are already involved in standardisation committees, they should evaluate the possibility to get involved in and support PQC standardisation working groups. If not, they can also connect to other entities (national or in other Member States, via the NIS CG) to learn more about ongoing work and decide on their investments. Moreover, PQC and quantum computing remain very active research areas. Member States should continue to support this research, as well as identify and track relevant sources of information on these topics and share them with the NIS CG so they can all have relevant and quality information. Member States are also encouraged to cooperate on research and educational training, namely via joint research programs or joint PhD programs.
- *Implement pilot use cases and contribute to testing centres.* To support a smoother PQC transition across the EU, Member States should promote international cooperation for testing interoperability of PQC solutions. To go even further in the means implemented for the transition, Member States can consider creating national expertise centres and entities are encouraged to make use of the coming EU testing infrastructure(s) funded under the Digital Europe Programme. Work on concrete use cases representing real-world scenarios, for example as in ETSI Plugtests or IETF PQC hackathons, is encouraged. National expertise centres plus the EU testing infrastructure(s) will allow to refine threat models and the implementations of countermeasures in real-life PQC implementations. This expertise centre could also offer a testing infrastructure to evaluate the interoperability of many solutions in real conditions and facilitate proofs of concept before implementation.

7 What the EU can do

The EU is implementing a comprehensive approach to catalyse the transition to PQC. In addition to actively engaging in discussions with Member States, industry and academics, the Commission designs supportive measures on PQC, with actions under the Digital Europe Programme and Horizon Europe Programme. The Commission engages in discussions at the international political level, and designed and adopted the 'Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography" on 11.04.2024. The EU, via the Commission and ENISA, provides a bridge between the PQC roadmap and the activities undertaken under the ECCG to develop recommendations on PQC mechanisms and their evaluation. The Commission and ENISA can also support peer sharing between Member States on best practices, methods and tools that facilitate migration to PQC.

References

[1] European Commission. Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. 2024. URL:

https://eur-lex.europa.eu/eli/reco/2024/1101/oj.

[2] European Parliament and Council. Directive (EU) 2022/2555 (NIS 2 Directive) on measures for a high common level of cybersecurity across the Union, amending Regulation (eu) No 910/2014 and Directive (eu) 2018/1972, and repealing Directive (EU) 2016/1148. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[3] Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography. 2024. [Accessed 23.01.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html.

[4] European Parliament and Council. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) no 909/2014 and (EU) 2016/1011. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[5] European Parliament and Council. Directive (EU) 2024/2847 (Cyber Resilience Act) on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[6] AIVD. Informatieblad over quantumcomputers. 2014. [Accessed 31.01.2025]. URL: hhttps://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers.

[7] BSI. Study: Status of quantum computer development, Version 2.1. 2024. [Accessed 30.01.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html.

[8] Global Risk Institute. Quantum Threat Timeline Report 2024. 2024. [Accessed 31.01.2025]. URL: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

[9] ANSSI. ANSSI views on the Post-Quantum Cryptography transition. 2022. [Accessed 31.01.2025]. URL: https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf.

[10] ANSSI. ANSSI views on the Post-Quantum Cryptography transition (2023 follow up). 2023. [Accessed 31.01.2025]. URL: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.

[11] BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations. 2021. [Accessed 31.01.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html.

[12] ETSI. ETSI TR 104 016 V1.1.1 (2024-10), CYBER; a Repeatable Framework for Quantum-Safe Migrations. 2024. [Accessed 31.01.2025]. URL: https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf.

[13] DGX WG on Cyber Security. The Post-Quantum Cryptography Migration Starts Today. 2024. [Accessed 30.01.2025]. URL: https://www.tech.gov.sg/files/media/Reports/DGX_2024_Cyber_Working_Group_Report.pdf.

[14] NIST. Nist SP 1800-38A (Initial Preliminary Draft) – Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography. 2023. [Accessed 31.01.2025]. URL: https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf.

[15] NIST. Nist SP 1800-38B (Initial Preliminary Draft) – Migration to Post-Quantum Cryptography: Cryptographic Discovery. 2023. [Accessed 31.01.2025]. URL: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf.

[16] NIST. Nist SP 1800-38C (Initial Preliminary Draft) – Migration to Post-Quantum Cryptography: Testing Draft Standards. 2023. [Accessed 31.01.2025]. URL: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf.

[17] TNO AIVD, CWI. The PQC Migration Handbook, revised and extended 2nd edition. 2024. [Accessed 30.04.2025]. URL: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf.

[18] NIST. NIST IR 8547 (initial public draft), Transition to Post-Quantum Cryptography Standards — csrc.nist.gov. 2024. URL: https://doi.org/10.6028/NIST.IR.8547.ipd.

[19] UK NCSC. Timelines for migration to post-quantum cryptography. [Accessed 21.03.2025]. URL: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[20] BSI. BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz. 2017. [Accessed 04.02.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html.

[21] European Parliament and Council. Regulation (EU) 2019/881 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (eu) No 526/2013. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[22] ANSSI. L'ANSSI partage deux études de marché sur la cryptographie post-quantique menées auprès de l'écosystème. 2024. [Accessed 30.04.2025]. URL: https://cyber.gouv.fr/actualites/lanssi-partage-deux-etudes-de-marche-sur-la-cryptographie-post-quantique-menees-aupres.

[23] ECCG Sub-group on Cryptography. Agreed Cryptographic Mechanisms - version 2. 2025. URL: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.