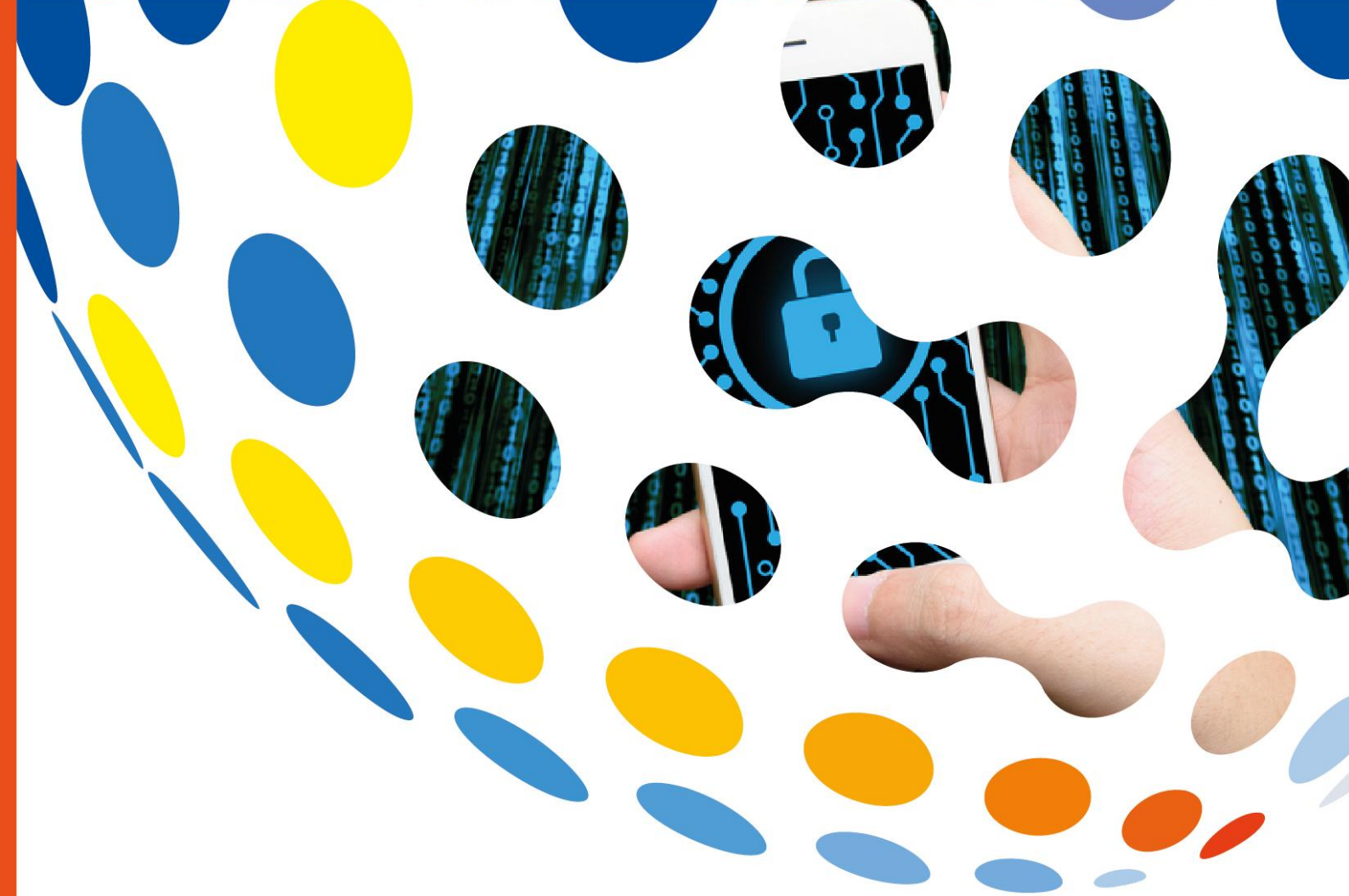




EU Roadmap on PQC – Frequently Asked Questions

NIS Cooperation Group

15.04.2026

Table of Contents

Contents

1. Introduction.....	4
2. Quantum risk estimation, milestones, and prioritisation.....	4
2.1 How is the threat posed by ‘store now, decrypt later’ attacks covered by the risk model presented in section 5 ‘Estimating the quantum risk’ of the EU Roadmap on PQC?	4
2.2 Is it correct that using AES-128 to protect long-term confidentiality is seen as medium risk and therefore prioritised at the same level as migrating the ‘easy’ cases (which do not require a lot of effort like complex PKIs) for authentication?.....	4
2.3 Is symmetric cryptography impacted by CRQCs? And if so, does that change prioritisation?	5
2.4 One example in section 5 of the EU Roadmap on PQC says that if migration takes more than eight years and the impact of an attack is high, then the quantum risk level is high. According to the timeline, high-risk cases must be migrated by the end of 2030, as this less than eight years away, isn’t it contradictory?	5
2.5 How is the prioritisation balance between the threat to confidentiality vs integrity and authenticity?	5
2.6 How do your suggested timelines align within Europe and globally?	6
3. Hybrid schemes.....	6
3.1 What are hybrid schemes in the context of the transition to post-quantum cryptography?.....	6
3.2 Is the use of hybrid cryptographic schemes combining several public-key cryptographic schemes seen as a long-term or a short-term strategy?	6
3.3 Is there different guidance on hybrid key encapsulation mechanisms and hybrid signature schemes?	7
3.4 Which specific hybrid mechanisms does the NIS CG workstream on PQC recommend and how do these recommendations align within Europe and globally?	7
4. Milestones, ‘First Steps’, and ‘Next Steps’	8
4.1 Do the milestones and the associated deadlines apply to deployments, to product availability or solely to the availability in standards?	8
4.2 Does an organisation need to finish creating its cryptographic inventory before planning and prioritising the transition to PQC?	8
4.3 Do the ‘First Steps’ need to be completed before moving on to the ‘Next Steps’?	8
5. National roadmaps.....	9
5.1 Which aspects of the EU Roadmap on PQC should be included in a national roadmap?	9
5.2 Will the NIS CG workstream on PQC publish additional sector specific guidance?..	10

5.3 Will the NIS CG workstream on PQC recommend specific algorithms?	10
5.4 What does ‘mature cryptographic asset management mean’?.....	10
5.5 To ensure resilience against future attacks by sufficiently powerful quantum computers, which cryptographic algorithms and protocols need to be replaced?.....	10
5.6 What about quantum key distribution (QKD), is it considered a quantum-safe alternative or additional solution?.....	11
6. European Union.....	11
6.1 What is the role of EU institutions and what actions can they take to support the transition?	11
6.2 How does the EU Roadmap on PQC align with EU legislation such as NIS2, CRA, GDPR, CSA, and DORA?	12
6.3 What can be done to address gaps in knowledge and the shortage of professionals in the EU to support the transition to PQC?	13
6.4 What resources are available from EU institutions to support the implementation of PQC solutions?	13
7. Miscellaneous	14
7.1 How do I migrate my organisation to PQC?	14
7.2 What if the development of quantum computers accelerates rapidly?	14
7.3 Do all critical infrastructure systems need to be resilient against potential attacks by a sufficiently powerful quantum computer by 2030?	15
7.4 Which entities should create inventories of cryptographic assets and dependency maps, involve the supply chain, and perform a quantum risk analysis as outline in the ‘First Steps’?	15

1. Introduction

This document provides answers to frequently asked questions (FAQs) regarding the publication “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography” (EU Roadmap on PQC), issued by the NIS Cooperation Group.

2. Quantum risk estimation, milestones, and prioritisation

2.1 How is the threat posed by ‘store now, decrypt later’ attacks covered by the risk model presented in section 5 ‘Estimating the quantum risk’ of the EU Roadmap on PQC?

A: In a ‘store now, decrypt later’ attack, adversaries can harvest encrypted data now to store for future decryption i.e. when a sufficiently powerful quantum computer becomes available. This is a risk for any information that must be kept confidential for longer periods of time (beyond 2035). Calculating the quantum risk score can help organisations assess their vulnerability to quantum computing threats and guide them in prioritising mitigation strategies for their cryptographic systems.

Using Figure 2.7 of the [PQC Migration Handbook](#), the quantum risk score can be calculated by combining the individual weakness, impact, and migration effort scores. For example:

- If one or more of the algorithms used are not secure against quantum attacks, then the *quantum weakness score* is 2.
- If an attacker could perform a ‘store now, decrypt later’ attack on data whose confidentiality must stay protected after 2035 the *impact score* is three.
- Based on Figure 2.7 in the PQC Migration Handbook, it follows that the *quantum risk score* is either 3 or 4 depending on the migration effort score.
- A quantum risk score of 3 or 4 is associated with a quantum risk level of ‘high’ as set out in section 5 ‘Estimating the quantum risk’ of the EU Roadmap on PQC.

2.2 Is it correct that using AES-128 to protect long-term confidentiality is seen as medium risk and therefore prioritised at the same level as migrating the ‘easy’ cases (which do not require a lot of effort like complex PKIs) for authentication?

A: The EU Roadmap on PQC focuses on the migration of public-key cryptography, as the risk is substantially higher than for symmetric-key cryptography. The recommendation of the roadmap is to clearly prioritise migrating public-key cryptography. Note that there are some practical limits to (simple) risk score models. It is indeed correct that applying the quantum risk score model of the [PQC Migration Handbook](#) will give the same quantum risk score for both cases, and will thus lead to the same quantum risk level. See also the answer to the next question.

2.3 Is symmetric cryptography impacted by CRQCs? And if so, does that change prioritisation?

A: Since it is clear that a CRQC will impact public-key cryptography severely and attacking state-of-the-art symmetric-key cryptographic algorithms like AES currently does not seem practical in the foreseeable future (even with 128 bit keys), the EU Roadmap on PQC focuses on the migration of public-key cryptographic systems.

This does not change prioritisation according to the quantum risk level, but in practice it may affect the choice of solution. In general, implementing cryptographic agility is recommended to enable swift changes to algorithms and/or key lengths if necessary.

2.4 One example in section 5 of the EU Roadmap on PQC says that if migration takes more than eight years and the impact of an attack is high, then the quantum risk level is high. According to the timeline, high-risk cases must be migrated by the end of 2030, as this is less than eight years away, isn't it contradictory?

A: As the case described here is tricky with no straightforward answer, there are some key points to consider:

- It may be too late in some cases to only focus on the long-term solution. Transitioning from traditional asymmetric cryptography to PQC could take too long for a specific use-case, so short-term alternatives, like adding pre-shared symmetric keys, should be considered.
- While the full transition of a public key infrastructure (PKI) may not be feasible by the end of 2030, it may be possible to introduce a new PKI with PQC alongside the old quantum-vulnerable PKI before the 2030 deadline.
- It is essential to continuously assess risks and monitor developments in quantum computing along with establishing a backup plan in case a cryptographically relevant quantum computer emerges in less than eight years.
- Finally, it is important to understand why the transition period for a specific use case is so long. One reason could be the regular device lifetime or certificate validity periods. While adjusting these timelines can be challenging for a business, doing so may speed-up the transition process.

2.5 How is the prioritisation balance between the threat to confidentiality vs integrity and authenticity?

A: Section 5 of the EU Roadmap on PQC, 'Estimating the quantum risk' indicates performing a quantum risk assessment can assist in prioritising the migration process. The methodology for conducting the quantum risk analysis is set out in the [PQC Migration Handbook](#).

Organisations should calculate a quantum risk score for each of their different use cases using this methodology. They can then refer to section 5 of the EU Roadmap on PQC, to determine the quantum risk level, 'low', 'medium', or 'high', associated with the score for each of their use cases.

The 'Timeline for the transition to PQC' on page 7 of the EU Roadmap on PQC provides a timeline for each of the quantum risk levels.

It is important to note that the EU Roadmap on PQC specifically recommends that quantum-safe software and firmware upgrades be enabled by default by the end of 2030.

2.6 How do your suggested timelines align within Europe and globally?

A: The EU Roadmap on PQC recommends completing the migration of all use cases by the end of 2035, except for certain low risk use cases. This timeline aligns well with other guidelines in Europe and globally, except for Australia, where the deadline is more ambitious. The Australian Signals Directorate (ASD) recommends in their [Planning for post-quantum cryptography](#) that organisations complete their migration by the end of 2030.

In the US, the National Institute of Standards and Technology (NIST) [IR 8547 initial public draft](#) requires full migration by 2035, a date that was first set in the US National Security Memorandum 10 in 2022.

Likewise, the United Kingdom's National Cyber Security Centre (NCSC) recommends in their [Timelines for migration to post-quantum cryptography](#) that organisations complete the migration of all their systems to PQC by the end of 2035. The timeline given in the [Roadmap for the migration to post-quantum cryptography for the Government of Canada](#) set out by the Canadian Centre for Cyber Security (the Cyber Centre) is also the same, with federal departments and agencies expected to migrate all their systems by the end of 2035.

3. Hybrid schemes

3.1 What are hybrid schemes in the context of the transition to post-quantum cryptography?

A: In the EU Roadmap on PQC, a hybrid is defined as a combination of a post-quantum algorithm and a quantum-vulnerable algorithm for the mechanism, such that the security is as high as the higher of the ingredients. The EU Roadmap on PQC does not consider hybrids mechanisms using quantum key distribution (QKD) or using more than one PQC mechanism.

3.2 Is the use of hybrid cryptographic schemes combining several public-key cryptographic schemes seen as a long-term or a short-term strategy?

A: Currently, there is no clear guidance on whether hybrid cryptographic schemes are considered a long-term or short-term strategy. While there is no recommendation on when to start or stop using hybrid schemes, they may be beneficial for enabling crypto-agility.

3.3 Is there different guidance on hybrid key encapsulation mechanisms and hybrid signature schemes?

A: Yes, there are different guidelines for hybrid key encapsulation mechanisms (KEMs) and for hybrid signature schemes. Hybrid KEMs are easier to work with than hybrid signature schemes. For KEMs, using a Key Derivation Function (KDF) to combine the secrets from both the traditional (quantum-vulnerable) asymmetric algorithm and post-quantum asymmetric algorithm to derive a (shared) symmetric secret is standard practice and if done correctly can provide strong security. In contrast, hybrid signature schemes involve more complex interactions and a number of factors which can affect their security, making it more difficult to establish specific guidelines. However, this topic falls outside the scope of the EU Roadmap on PQC. For more specific guidance on hybrid KEMs, refer to, e.g., NIST [SP 800-227](#).

3.4 Which specific hybrid mechanisms does the NIS CG workstream on PQC recommend and how do these recommendations align within Europe and globally?

A: The NIS CG workstream on PQC does not maintain a list of recommended (hybrid) PQC algorithms. It does, however, recommend that standardised hybrid solutions are used wherever feasible and suitable. This is in line with the recommendations of other European cybersecurity agencies, such as French Cybersecurity Agency (ANSSI) in France and Federal Office for Information Security (BSI) in Germany. For example, the BSI [Technical Guideline – Cryptographic Algorithms and Key Lengths](#) recommends using a combination of traditional (quantum-vulnerable) cryptographic algorithms and post-quantum cryptography in hybrid solutions. Moreover, the [Recommendation from the European Commission from April 2024 on PQC](#) recommends hybrid schemes. The Swedish NCSC is agnostic to the use of pure PQC or hybrids, the main objective is to provide the best security in the particular use case.

From a global perspective, in the United States, the National Security Agency (NSA) [Commercial National Security Algorithm Suite 2.0](#) (CNSA 2.0) recognises that hybrid solutions may be necessary for protocol standards and interoperability. However, hybrid solutions are not included in the mandatory CNSA 2.0 algorithms for U.S. National Security Systems.

Additionally, NIST [IR 8547 initial public draft](#) indicates that hybrid techniques will be integrated into its cryptographic standards to facilitate the transition to PQC. However, it also suggests that these hybrid methods are likely to be temporary measures leading to a future transition to exclusive use of PQC algorithms.

In the UK, NCSC accepts PQC hybrids as an ‘interim measure’ which should be used within a ‘flexible framework’ (see [Next steps in preparing for post-quantum cryptography](#)) but recommends pure PQC schemes in general.

As each Member State is expected to establish a national roadmap aligned with the EU Roadmap on PQC, they should consider the existing recommendations implemented by other Member States.

4. Milestones, ‘First Steps’, and ‘Next Steps’

4.1 Do the milestones and the associated deadlines apply to deployments, to product availability or solely to the availability in standards?

A: The milestones and deadlines set out in the EU Roadmap on PQC apply to the deployment of PQC. This means that Standards Developing Organisations (SDOs) and vendors need to be ahead of the timelines set out in the EU Roadmap on PQC.

In 2024, the National Institute of Standards and Technology (NIST) published the first set of PQC standards. With the ongoing evaluation of additional algorithms, cryptographic agility will be important, not only for the migration to PQC but for a strong security posture.

When evaluating the milestones and associated deployments, first step recommendations in section 6.2 of the EU Roadmap on PQC emphasizes starting dialogue with product and service suppliers to understand their plans to integrate PQC and cryptographic agility in the development of their products or services. This will be vital for organisations as achieving the deadlines set out in section 4.2 of the EU Roadmap on PQC, which will be dependent on the availability of compliant products and services.

4.2 Does an organisation need to finish creating its cryptographic inventory before planning and prioritising the transition to PQC?

A: No, organisations do not need to complete their inventory prior to commencing planning and prioritisation. As outlined in section 6.2 of the EU Roadmap on PQC, creating and maintaining a cryptographic inventory is an essential first step and ‘no regret’ move to identify, evaluate and document cryptographic assets. Nevertheless, completing a full inventory and being able to interpret all its contents is challenging (thousands of cryptographic functions, keys, certificates, etc.). Therefore, it is important that entities, simultaneously with the creation of an inventory, produce a high-level mapping of their applications, what they support, which are essential, and which servers they rely on.

An initial inventory will enable the commencement of high-level planning and prioritisation for the transition of high-risk cases. Adopting a phased approach as outlined in the EU Roadmap on PQC means organisations can continue the inventory process while transitioning the most high-risk use cases. As inventory creation is an iterative process, simultaneous review and refinement of prioritisation and planning will be essential with each iteration. Maintaining a cryptographic inventory requires constant review and update to maintain a good security posture beyond the transition to PQC.

4.3 Do the ‘First Steps’ need to be completed before moving on to the ‘Next Steps’?

A: No, the ‘First Steps’ do not need to be completed prior to commencing the ‘Next Steps’. Section 6.3 of the EU Roadmap on PQC outlines the importance of pursuing other activities which can help facilitate a smooth transition once the ‘First Steps’ have been initiated. Engaging in activities outlined in the ‘Next Steps’ in parallel with the

ongoing 'First Steps' will ensure that the migration progresses without any undue delays.

5. National roadmaps

5.1 Which aspects of the EU Roadmap on PQC should be included in a national roadmap?

A: The EU Roadmap on PQC outlines concrete actions in the 'First Steps' and 'Next Steps' for Member States. When establishing their national roadmap, each Member State should consider these steps and expand on them to clearly outline their planned activities and corresponding timelines.

In terms of 'First Steps', Member States should consider including:

- An overview of relevant national and international stakeholders, detailing their planned involvement in the national migration.
- A plan to promote and support:
 - Creation and maintenance of cryptographic inventories and dependency maps.
 - Performance of quantum risk analysis.
 - Inclusion of the supply chain.
- Reference to a national awareness and communication programme, including tailored awareness and communication strategies.
- A proposal for knowledge sharing and participation in the NIS CG workstream on PQC.

In terms of 'Next Steps', Member States should consider including:

- A proposal to encourage and, where appropriate, enforce support for cryptographic agility and a quantum-safe upgrade path for products.
- Plans to:
 - Estimate and ensure the allocation of adequate budget and personnel resources at all levels, including budget reservations in life-cycle management.
 - Adapt cybersecurity certification schemes, both national and European, to address emerging threats posed by advancements quantum computing.
 - Identify and, if required, create cryptography-related regulations and cryptographic policies while updating them with modern recommendations for PQC.
 - Implement pilot use cases and contribute to testing centres.
- A comprehensive overview of opportunities within the ecosystem for a smooth global transition, including the private sector, training programmes, and funding programmes.

- A description of planned transversal activities to support PQC standardisation, including involvement in standardisation committees, collaborating with other entities and promoting further research.

Member States should consider including the steps outlined above as a minimum, however they have flexibility to go beyond these based on national requirements.

5.2 Will the NIS CG workstream on PQC publish additional sector specific guidance?

A: No, the NIS CG workstream on PQC will not publish additional sector specific guidance. However, it strongly encourages engagement and collaboration at national and international levels to foster industry partnerships and publish sector-specific roadmaps. The publication of sector-specific roadmaps will be beneficial for organisations to share learnings and expertise, not only within their sectors but across all sectors.

5.3 Will the NIS CG workstream on PQC recommend specific algorithms?

A: No, the NIS CG workstream on PQC will not suggest or recommend specific algorithms or mechanisms other than referring to existing standards and recommendations. The NIS CG workstream on PQC encourages national agencies to align their regulations and recommendations with those of other Member States whenever possible. This approach will optimise compatibility and acceptance of cryptographic products throughout the European Union.

5.4 What does ‘mature cryptographic asset management mean’?

A: The term ‘mature cryptographic asset management’ is not explicitly defined in the EU Roadmap on PQC or related documents. For the purposes of the EU Roadmap on PQC, it refers to a well-developed, structured, and secure approach to managing all cryptographic assets, such as keys and certificates, throughout their entire lifecycle. This includes maintaining a complete, up-to-date inventory of cryptographic assets, understanding their associated risks, and managing them with clear policies and processes that enable crypto-agility and timely migration to new standards.

In practice, implementing an IT Asset Management (ITAM) system should integrate the inventory and lifecycle management of cryptographic assets. For further details refer to section 2.4 of the [PQC Migration Handbook](#).

5.5 To ensure resilience against future attacks by sufficiently powerful quantum computers, which cryptographic algorithms and protocols need to be replaced?

A: To achieve resilience against future attacks by a sufficiently powerful quantum computer, it is essential to replace traditional asymmetric cryptographic mechanisms with quantum-safe alternatives. Many cryptographic protocols rely on asymmetric mechanisms and are therefore vulnerable to future quantum attacks. Specifically,

asymmetric algorithms such as RSA, DSA and ECC are at significant risk. More information on common protocols is available in section 4.3 of the [PQC Migration Handbook](#).

In respect of symmetric mechanisms and hash function the debate regarding the impact of quantum attacks continues. Ongoing research is investigating whether such attacks would be feasible in practice. Depending on the cryptographic standards implemented, it may be advisable to use longer key or output lengths to enhance security. Detailed information is available in the PQC Migration Handbook, in particular section 4.2 which discusses recommended cryptographic primitives, and Chapter 6 which provides background on these primitives. The BSI [Technical Guideline – Cryptographic Algorithms and Key Lengths](#) provide further details and clarifications.

Lastly, assessing quantum risk involves determining the quantum vulnerabilities of the algorithms in use. Section 2.4 of the PQC Migration Handbook addresses the quantum risk assessment, including a list of cryptographic algorithms along with their quantum weakness scores.

5.6 What about quantum key distribution (QKD), is it considered a quantum-safe alternative or additional solution?

A: The NIS CG workstream on PQC strongly recommends that organisations focus on replacing quantum-vulnerable cryptography with post-quantum cryptography (PQC). This recommendation is based on the current applicability and maturity of PQC and aligns with the [Position Paper on Quantum Key Distribution](#) (QKD) by the French Cybersecurity Agency (ANSSI), the Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA) and Swedish National Communications Security Authority, Swedish Armed Forces.

PQC algorithms are designed to run on existing IT systems and infrastructure. They are becoming increasingly ready as direct replacements for quantum-vulnerable public-key cryptography systems like RSA and ECC.

In contrast, QKD is an experimental, hardware-based technology. It uses quantum physical principles to provide an additional layer of security, but it is limited to highly specialised use cases that require dedicated infrastructure. Due to its limited practical applications and insufficient maturity, QKD is currently not considered a viable quantum-safe alternative.

6. European Union

6.1 What is the role of EU institutions and what actions can they take to support the transition?

A: EU institutions can take various initiatives to support the transition to PQC. Key actions include:

- The European Commission's Annual Union Work Programme for European standardisation can be leveraged to support the transition to PQC. In the 2025

programme, standards driving the development of quantum technology and the implementation of PQC protocols were identified as priorities. The European Commission has an opportunity to emphasize standardisation actions on PQC as a separate policy priority in future work programmes.

- The European Commission should integrate actions regarding PQC into the Rolling Plan for ICT Standardisation which connects EU policies and standardisation activities. The plan complements the Annual Union Work Programme for European standardisation and incorporates input from the European Multi-Stakeholder Platform on ICT standardisation (MSP).
- The European Commission or the EU Agency for Cybersecurity (ENISA) could develop an 'EU PQC Readiness Index' which allows organisations to report on their PQC readiness and compare it with that of other organisations. This index would enable a comprehensive assessment of the EU's overall readiness against future threats posed by sufficiently powerful quantum computers.
- The provision of additional EU funding for PQC migration related research and innovation projects would strengthen the competitiveness of the European internal market and bolster cyber resilience across the European Union.
- EU institutions can raise awareness about the quantum threat to cryptography and about PQC through conferences, panel discussions, workshops, webinars, publications, and press releases. This list is not exhaustive; there are many potential EU-led initiatives that could support the transition to PQC.

6.2 How does the EU Roadmap on PQC align with EU legislation such as NIS2, CRA, GDPR, CSA, and DORA?

A: The EU Roadmap on PQC underpins these legislative frameworks by providing guidance on advanced cryptographic measures to prepare for potential threats of quantum computing. Its implementation ensures the security and resilience of digital infrastructure and protects protection of data, including privacy, within the EU. Here is how it is aligned with key legislation:

- **NIS2 (NIS 2 Directive):** Lays down measures to enhance the EU's cybersecurity. Implementing PQC is crucial for protecting essential and important entities from quantum computing threats.
- **CRA (Cyber Resilience Act):** Lays down mandatory cybersecurity requirements for products with digital elements, including confidentiality of data, following a risk-based approach. PQC is necessary to protect these products from quantum threats.
- **GDPR (General Data Protection Regulation):** Regulates data protection, including security of data processing. Transitioning to PQC helps ensure compliance with GDPR by safeguarding data against quantum risks.
- **CSA (Cybersecurity Act):** Establishes the European Cybersecurity Certification Framework that enables the development and adoption of European cybersecurity certification schemes. Integrating PQC requirements in the certification process ensures that products are secure against quantum vulnerabilities.
- **DORA (Digital Operational Resilience Act):** Enhances the digital operational resilience of financial entities. Implementing PQC is crucial for protecting financial systems from quantum computing threats.

6.3 What can be done to address gaps in knowledge and the shortage of professionals in the EU to support the transition to PQC?

A: There are several actions that can be taken at national and EU level to build a robust talent capable of addressing the challenges and opportunities presented when transitioning systems to PQC, ensuring both technological advancement and cybersecurity resilience. Some of these actions include:

- **Education and training programmes:** Develop specialised courses and degree programmes in cryptography, including post-quantum cryptography, at universities and technical institutions using Member States' feedback of PQC industry and government needs. This could include offering postgraduate courses specifically focused on PQC.
- **Online learning platforms and MOOCs:** Develop, promote, and offer Massive Open Online Courses (MOOCs) and other online resources focused on post-quantum cryptography to broaden access to education across the EU.
- **Professional development and certification:** Develop certification for cybersecurity professionals utilising the European Cybersecurity Skills Framework (ECSF) as a basis and encourage the development of specialised additional certifications in PQC, leveraging partnerships with professional bodies and industry associations.
- **Public-private partnerships:** Encourage collaboration between industry, academia, and government to facilitate the exchange of knowledge and development of practical skills, including opportunities for internships and placement programmes for students and professionals.
- **Research funding and support:** Increase funding for PQC research to enable deeper engagement by students and researchers developing expertise and educational resources.
- **Collaborative research projects:** Support collaborative research projects across the EU to advance PQC technologies while providing training opportunities for researchers and professionals.
- **Workshops and conferences:** Organise events on PQC to share knowledge, best practices, and foster networking among professionals and students, providing a platform for learning and collaboration in this space.
- **Awareness campaigns:** Launch campaigns to raise awareness about the importance of PQC for cybersecurity, encouraging students and professionals to pursue careers in this field.

6.4 What resources are available from EU institutions to support the implementation of PQC solutions?

A: The implementation of PQC solutions in the EU is supported by initiatives from EU institutions that aim to facilitate research, development, and adoption of PQC technologies to ensure cryptographic systems remain secure in the future. Some key resources available:

- **Horizon Europe:** Horizon Europe, the EU's flagship research and innovation programme, provides funding for projects focused on advancing both fundamental research in PQC and real-world PQC solutions. It supports collaborative research across EU member

states on PQC in many calls for proposals in its cluster “Civil Security for Society” and several in the cluster “Digital, Industry and Space”. The European Research Council (ERC), with individual and collaborative grants, and the European Innovation Council (EIC) schemes are also part of Horizon Europe, and provide funds for fundamental science, innovation and acceleration.

- **Digital Europe Programme (DIGITAL):** This programme focuses on building the strategic digital capacities of the EU, including cybersecurity. It supports the deployment and uptake of PQC by funding associated research and development projects as well as infrastructure enhancements.
- **EU Agency for Cybersecurity (ENISA):** ENISA has published several studies on PQC, presenting key concepts of PQC, the status of standardization activities, risk assessments and the necessity to both design new cryptographic protocols and integrate post-quantum systems into existing protocols.
- **Collaboration and networking initiatives:** The EU supports various networks and collaborative platforms that facilitate knowledge sharing and joint efforts in the development and implementation of PQC, bringing together academic, industry, and governmental stakeholders.

7. Miscellaneous

7.1 How do I migrate my organisation to PQC?

A: The EU Roadmap on PQC provides high-level recommendations, milestones, and timelines for the transition to PQC. The ‘First Steps’ outlined in section 6.2 of the EU Roadmap on PQC will assist organisations initiating the planning and preparation for their transition to PQC. The ‘Next Steps’ outlined in section 6.3 can help facilitate a smooth transition for organisations. Furthermore, specific guidance in respect of the steps set out in the EU Roadmap on PQC are available in the [PQC Migration Handbook](#).

According to section 4.1 of the EU Roadmap on PQC, Member States should establish their own initial national roadmaps by the end of 2026. Organisations should refer to the national roadmaps in conjunction with guidance and advice issued by their National Cyber Security agencies.

The NIS CG workstream on PQC is considering additional publications which may further assist organisations with their migration to PQC.

7.2 What if the development of quantum computers accelerates rapidly?

A: Any acceleration in quantum computing developments will increase the urgency for the transition to PQC. To address the threat to prioritised systems, it is essential for organisations to establish contingency plans outlining swift mitigation actions.

7.3 Do all critical infrastructure systems need to be resilient against potential attacks by a sufficiently powerful quantum computer by 2030?

A: A risk-based approach as outlined in the EU Roadmap on PQC is recommended. The EU Roadmap on PQC indicates that all high-risk use cases should be transitioned to PQC by the end of 2030. While assessing the risk for individual critical infrastructure systems is beyond the scope of this document, each Member State should encourage providers of critical national infrastructure to incorporate the quantum threat into their risk management strategies.

7.4 Which entities should create inventories of cryptographic assets and dependency maps, involve the supply chain, and perform a quantum risk analysis as outline in the 'First Steps'?

A: In the EU Roadmap on PQC the term 'entity' refers to any organisation. At a minimum, entities in scope of the NIS 2 Directive, including public administration entities and critical infrastructure providers, should create an inventory of cryptographic assets and dependency maps, involve the supply chain, and perform a quantum risk analysis. However, as a proactive measure to ensure a robust security posture, all organisations are encouraged to undertake these steps.