CEPS TASK FORCE

Strengthening the EU transition to a quantum safe world

Technology, market, governance and policy challenges

Task Force comments to the NIS Cooperation Group
'Coordinated Implementation Roadmap
for the Transition to Post-Quantum Cryptography'
Published on 11 June 2025

29 September 2025

Introduction

The Centre for European Policy Studies (CEPS) launched a Task Force on 'Strengthening the EU transition to a quantum safe world' in April 2025. The Task Force's goal is to bring attention to the market, technical, ethical and governance challenges posed by the transition to a quantum-safe world in the EU and to suggest policy measures to facilitate the transition to a quantum-safe world. 28 organisations are participating in the Task Force, from the private sector, the EU institutions and agencies, academia and civil society.

The Task Force is currently discussing issues such as the status of the transition to post-quantum cryptography (PQC) in the EU, the status of quantum technologies, Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG), Quantum safe transition models, PQ inventories and the transition to quantum safe in the financial, defence and public sectors. As a part of these activities, the following comments aim to assess the '**Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography'** published by the NIS Cooperation Group on the 11 June 2025 (from now on 'the **Roadmap**').

Overall comments on the Roadmap

- We find the Roadmap very well-written and useful. In particular, we appreciate that the milestones align well with the international ecosystem, that the importance of early migration to quantum-safe software and firmware upgrades is emphasised and that the challenges of long transition periods, such as those faced by public-key infrastructures (PKIs) and long-lived devices, are clearly described, along with the need to begin migration planning for these systems as soon as possible.
- We support the EU's comprehensive approach to catalysing the transition to PQC and we especially welcome the European Commission's commitment to engaging not only with Member States but also with industry and academia. All these stakeholders will play a critical role in helping the Commission design effective support measures for PQC.
- The Roadmap stresses the need for cryptographic inventories and dependency maps, which are essential for identifying vulnerabilities and planning migration steps.
- It recommends tailored awareness campaigns to educate stakeholders about the quantum threat and the importance of PQC migration.
- Furthermore, while it defines itself as a 'high-level concept paper', it is also very action-oriented, emphasises swift implementation and is quite specific. For instance, it prompts the Member States to start working on or updating their transition plans immediately, without waiting for the final deliverable of this Work Stream and to start implementing next

steps in parallel with the first steps, so it tangibly strives to 'ensure a minimum level of readiness in all Member States by the end of 2026'.

- It provides concrete examples of good practice, for example on page 11 it refers to surveys conducted in France to 'determine market readiness, identify obstacles for the PQC transition and to learn about the needs of three types of stakeholders: providers, users, and consulting companies'.
- It states that relevant regulations and technical requirements or guidance stipulated at the national level should be systematically updated 'with state-of-the-art recommendations for PQC. If no such regulations or cryptographic policies exist, Member States should consider creating them, for example by consulting other countries and the NIS CG. Mass adoption will require both the availability of the products and example set by institutions. Member States should consider started integrating PQC requirements in their future national procurement processes and are encouraged to contact their current IT suppliers to assess their maturity on PQC' (page 14).
- The Roadmap **does a good job of emphasising the importance of protecting the confidentiality and integrity of data** (page 4). However, it should also explicitly address the need to protect data during processing, as it is increasingly common to process sensitive information in the cloud. Furthermore, rather than using terms such as 'stored,' 'transmitted' and 'communication', we suggest consistently using the widely accepted formulation of 'protect the confidentiality and integrity of data in transit, at rest, and during processing.'
- **The Roadmap should also explicitly highlight the need to protect availability.** While availability is partially a consequence of integrity protection, it is important for readers to understand that PQC migration also contributes to safeguarding the availability of critical infrastructure. For most critical systems, availability is at least as crucial as confidentiality and integrity, and making this explicit will help convey the full scope of why timely PQC adoption is necessary

Timeline

- The Roadmap provides a clear timeline with milestones for PQC migration, emphasising the urgency for high-risk use cases by 2030 and medium risk use cases by 2035.
- Specifically, both the timeline completion date of 2035 and the prioritising approach used are very well chosen. Given the complexities across sectors, the varying maturity across Member States and the need to be clear without being too strict, this document and the roadmap it describes gets the balance right.
- We support the approach to 'start now' while creating 'first steps' and 'next steps' and the timelines that are proposed by the Cooperation Group.

- We appreciate that the timelines and actions (2026, 2030, 2035) are also broadly consistent with US policy.
- However, as the Roadmap leaves the initiative entirely to individual Member States, it fails to address how their approaches can be harmonised. Moreover, it remains unclear whether the EU will play a coordinating role and the Roadmap does not specify the consequences of non-compliance.
- **We believe the Roadmap should be updated** to more clearly state that the timelines apply to deployments. For full PQC adoption in deployed systems, it is essential that standards are updated and stable implementation is made available well in advance of those deployment milestones. The timelines for different stakeholders in the ecosystem, such as standards development organisations (SDOs), equipment vendors and operators deploying the systems, are inherently different. Standards bodies need to finalise specifications early, vendors need sufficient lead time to implement, test and certify solutions and only then can large-scale deployments take place. A clearer distinction between these stages would help align expectations and ensure that all parties can plan their contributions effectively.
- We welcome the focus on piloting and learning in the field. An important aspect of these pilots should be to pilot the complete stack – since security must be rooted in a PQC-enabled infrastructure.
- We like and support the approach of pushing for PQC-enabled updates to allow continuous improvement. We suggest piloting this with hardware vendors to understand the state of the art and identify gaps to fully achieve this objective. We need to clarify how to handle systems that are not updateable (e.g. due to hardware limitations).
- Pilot use cases should: i) be 'ground-up', ii) include hardware and iii) ensure that application-level pilots are supported by PQC-enabled infrastructures and hardware.

Threats to cryptographic algorithms

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

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

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

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

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

- In this context, it is important that the Roadmap on page 6 acknowledges that 'symmetric key methods instead of public key cryptography are worthwhile to consider, depending on the application.'
- This calls for an opportunity to elaborate more on what this can mean in practice: which use cases? Which approaches? Hybrid? The PQC focused push is largely focused on some of the main large-scale use cases. But those who are responsible for other systems, where it is more complicated that 'just' updating to PQC algorithms, need guidance as well.

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

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

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

Hybrid solutions

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

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

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

- We believe this should be expanded and clarified. We agree that only standardised algorithms with broad international adoption by industry and government authorities should be used. However, it is important to note that no major body is currently recommending the use of hybrid solutions with hash-based signatures such as SLH-DSA. It should also be clarified that only a freely-availably specification should be used. Many organisations have taken a firm stance against paywalled specifications for cryptographic algorithms, viewing them as cybersecurity risks. Both the IETF and NIST are working to remove as many references to such algorithms as possible. The NIS Cooperation Group needs to likewise avoid referencing any paywalled cryptography.
- While hybrid KEMs have been standardised by the IETF and adopted in real-world deployments, hybrid signatures have not achieved the same level of standardisation or implementation maturity. Consequently, hybrid signatures are unlikely to be ready in time to meet the EU roadmap timelines. Currently, the only signature algorithm supported in OpenSSL 3.5 LTS for use in TLS is the standalone ML-DSA. Governments in the US and UK have also been far more active in driving progress within open standardisation bodies, such as the IETF and ETSI, as well as in supporting the implementation of standalone ML-KEM and ML-DSA in major cryptographic libraries. It is somewhat ironic that the only standardised hybrid KEM specifications (ETSI CatKDF and CasKDF) was driven by the UK government, which now only recommends standalone ML-KEM and ML-DSA.
- The practical reality is that the only realistic migration paths today for industry are hybridiSed ML-KEM, standalone ML-KEM, standalone ML-DSA and, to some degree, standalone SLH-DSA. Alternative PQC algorithms (FN-DSA, HQC, etc.) will not be standardiSed and widely implemented to meet the required timelines.

  In TLS, X25519MLKEM in has already seen massive implementation support and is the default in OpenSSL, Firefox, Chrome, Edge, Go, etc. Cloudflare reports that over 40% of all HTTPS client requests use PQC. OpenSSL 3.5 LTS supports ML-KEM, ML-DSA, and SLH-DSA. OpenSSH is now using mlkem768x25519 as the default key exchange. Many IKEv2 implementations support ML-KEM. IKEv2 always uses ML-KEM in hybrid with (EC)DHE. The availability of well-tested and interoperable implementations is an essential factor for industry adoption, as it enables cost-effective, reliable and interoperable deployments

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

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

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

Inventories

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

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

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

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

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

Standards

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

- We support a standards-based approach to build upon the NIST standards for PQC that were defined through an open competition, involving the world's leading PQC scientists.
- We believe that the number of standards that need to be updated with the new cryptography is not widely understood. Only a handful of the many hundreds of protocol and industry standards have been adapted to being quantum safe. Many industries depend on these standards and will not be able to transition without these standards being updated. We suggest to formally request, from as many standards bodies as possible, a list of all impacted standards that need to be updated, together with an estimated timeline for updating them. This would allow for an understanding of the current situation and help trigger action by the relevant standards bodies.
- We believe that excessive emphasis on certification may prevent the best solutions from being successful on the market. While we see a role for 'process' certification (e.g. ISO 27000) to consciously manage risk and improve systems, we believe that third-party certifications should not be the only way to prove PQC conformity and more industry-driven initiatives and tools should be supported.
- We suggest stronger alignment with the EU CRA process. This could be in the form of certification requirements that make product suppliers list the cryptography that their products contain. This would immediately raise awareness of large parts of the supply chain that organisations will depend on to provide quantum safe solutions.

Awareness, cooperation and governance

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

- We agree that all nations are interconnected, not only in cyberspace but also through trade and global markets. For European industries operating internationally, close alignment with already published global timelines and algorithm recommendations is essential. Many European companies are already deeply engaged in the development and implementation of ML-KEM, ML-DSA and SLH-DSA in their products and services, working to meet the ambitious 2030-35 PQC deployment timelines.
- It is not realistic to expect that each Member State can individually create communities that attract global organisations, entities and stakeholders such as the IETF, 3GPP, the US government or major US companies. Even coordinating this at the EU level is extremely challenging. Instead, Member States should actively participate in open, global standardisation organisations such as the IETF and 3GPP, as well as in the open-source

cryptographic community, to ensure alignment, influence and knowledge-sharing at the international level.

- Members States should lead by example with transparent transition plans: publish and regularly update government transition roadmaps – including timelines, milestones and budgets – to foster knowledge sharing and best practices.
- The roadmap should broaden its definition of 'stakeholder' beyond ministries, regulatory agencies and technical experts. Civil society, minority networks and grassroots DEI organisations should be recognised as co-leaders, not simply 'consulted'.
- The integration of social clauses and community dividends into procurement, partnership and policy evaluation is vital, not just as a 'best practice' but as a requirement for measurable inclusion.
- Awareness campaigns and training modules should not be generic or one-size fits all. This CEPS Task Force is asking for a radical expansion of civic and digital education, embedding PQC awareness, quantum risk and digital rights topics not just in technical teams but across society, schools, care institutions and community centres.
- The Roadmap should establish mechanisms (citizen assemblies, consultation panels, regular transparent updates) to ensure citizens not only receive information but can actively shape strategies.
- The Roadmap should encourage joint pilot projects at the EU level to test interoperability of PQC in cross-border services before 2030.
- We suggest establishing a public-private PQC migration observatory under ENISA to monitor advances and recommend acceleration of timelines if necessary.
- As policymakers move forward with implementation, they should avoid prescriptive regulations or requirements that could create engineering or interoperability challenges, either within or across jurisdictions. We advocate for continued international dialogue on transition strategies and standards. As one potential path forward, we would welcome the G7 expanding the scope of its current quantum safety initiative in the financial sector to include a broader conversation across all sectors.

Interoperability challenges

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

Greater Parallelisation

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

For example:

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

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

- **Policy & Regulatory Track**: Focused on mandates, legal harmonisation and public sector funding instruments.
- **Standards & Interoperability Track:** Focused on profiling, conformance criteria and integrating emerging international standards.
- **Vendor Enablement Track:** Focused on incentivising the development, certification and benchmarking of PQC-capable products.
- **Operational Deployment Track:** Focused on asset inventories, CBOMs, the migration of public services and incident response updates.
- **Oversight & Metrics Track:** Focused on measurement frameworks, audits and maturity models.

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

Guidance on cost estimations

The Roadmap lacks mentioning or pointing towards methodologies for estimating the costs of PQC migration, including hardware replacements, software updates and potential downtime. Comprehensive cost frameworks are essential for organisations to allocate resources effectively and plan their budgets.

Legislative Framework

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

On the same note, where the document states the importance of involvement of NIS2, eIDAS and CRA supervisory authorities, data protection authorities should certainly also be part of this process. The same goes for DORA supervisory bodies.

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

Editorial comments

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

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

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

References

[1] FIPS 205, Stateless Hash-Based Digital Signature Standard

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[2] IETF Statement on Quantum Safe Cryptographic Protocol Inventory
https://datatracker.ietf.org/liaison/1942/

[3] 3GPP Statement on PQC Migration
https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip

[4] Sam Jaques, 'Quantum Attacks on AES'
https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s

[5] NIST, Transition to Post-Quantum Cryptography Standards

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[6] NCSC, Next steps in preparing for post-quantum cryptography

https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography