ERICSSON

Date: August 29, 2025

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on EU Roadmap on Post-Quantum Cryptography

Dear NIS Cooperation Group,

Thank you for your efforts to produce well-written and open-access security documents to support the Post-Quantum Cryptography (PQC) migration. With the publication of FIPS 203 (ML-KEM) [1], FIPS 204 (ML-DSA) [2], and FIPS 205 (SLH-DSA) [3], PQC has rapidly progressed from research into implementation and deployment. Many industrial stakeholders and providers of critical infrastructure, such as Ericsson, have been preparing this migration for many years and are now actively implementing ML-KEM, ML-DSA, and SLH-DSA across all products and services. For European industries operating in global markets, close alignment between EU and already published timelines and algorithm recommendations [1–15] is essential. Many European companies are already in full development to meet the challenging 2030–2035 timelines.

Please find below Ericsson's detailed comments on the EU Roadmap for Post-Quantum Cryptography. Our feedback covers both the recently published roadmap and suggestions to help guide the next steps, including the technical recommendations that the NIS Cooperation Group is expected to publish in May 2026 [16–17]. We welcome the fact that the NIS Cooperation is adopting the same level of transparency as NIST by making submitted comments publicly available, since such openness is essential for building trust in cybersecurity and cryptography.

Feedback on the recently published roadmap:

- We find the roadmap 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 emphasized, 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 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 implementations are made available well in advance of those deployment milestones. The timelines for different stakeholders in the ecosystem, such as standards development organizations (SDOs), equipment vendors, and operators deploying the systems, are inherently different. Standards bodies need to finalize 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.

- *"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 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 [4, 18–21]. 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 [20]. 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 those efforts 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"*

- *"For most applications, adhering to the recommended timeline should provide adequate protection from the quantum threat"*

  We fully agree with this statement. The recommended timelines in the EU roadmap do provide adequate protection against the quantum threat, particularly since the deployment of PQC itself significantly reduces the incentive to invest in building a CRQC. Importantly, this position also implies that the NIS Cooperation Group fundamentally disagrees with the Quantum Threat Timeline Report, which "estimates" a 19%–34% chance of a CRQC no later than 2034. To avoid confusion and mixed messaging, we recommend removing the reference to the misleading Quantum Threat Timeline Report.

- *"There is currently no evidence that this is already possible."*

  This phrasing is unnecessarily alarming. There is a broad consensus among experts in government, industry, and academia that no CRQC exists today. Building such a machine would require efforts and resources on a scale that could not go unnoticed.

- *"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"*

  We agree with this definition of hybrids. The purpose of hybrid schemes should be to preserve or strengthen security, not to weaken it. In particular, we are not supportive of hybrid constructions that degrade the security of ML-KEM to anything less than IND-CCA2 security, or that reduce the security of ML-DSA to below SUF-CMA.

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

  We believe this should be expanded and clarified. Our view is that only standardized algorithms with broad international adoption by industry and government authorities should be used. Also, it is important to note that there are no government or SDO recommending hybridization of hash-based signatures such as SLH-DSA [3]. It should also be clarified that only freely-available specifications should be used. Many organizations have taken a firm stance against paywalled specifications of cryptographic algorithms, viewing them as cybersecurity risks. We strongly agree with that view. Many companies, as well as the IETF and NIST, are working to eliminate references to these algorithms wherever possible. NIS cooperation group should likewise avoid referencing any paywalled cryptography.

  While hybridized ML-KEM has been specified by the IETF [22—24] and adopted in real-world deployments [25—28], hybrid signatures have not achieved the same level of standardization or implementation maturity. As a result, hybrid signatures will, for the majority of use cases, not be ready in time to meet the EU roadmap timelines. The only TLS PQC signature algorithm supported in OpenSSL 3.5 LTS is standalone ML-DSA. Governments in the US and UK have been far more active in driving progress within open standardization bodies such as the IETF and ETSI, as well as in supporting implementations of standalone ML-KEM and ML-DSA in major cryptographic libraries. It is somewhat ironic that the only standardized hybrid KEM specifications (ETSI CatKDF and CasKDF) were mostly driven by the UK government, which now only recommends standalone ML-KEM and ML-DSA.

  European government agencies now express the highest level of confidence in ML-KEM and ML-DSA. We understand that the main reason for maintaining hybridization is the risk of implementation flaws, such as side-channel vulnerabilities in early implementations. Going forward, hybridization is expected to transition from a recommended practice to an optional one [29], reflecting growing confidence in the maturity of post-quantum signature implementations and the expectation that early risks will be mitigated through improved techniques, tooling, and evaluation frameworks. Making these points explicit in the report would help industry stakeholders plan long-term security strategies and align roadmaps with the evolving post-quantum standardization landscape.

- The practical reality is that, for European industry, the only viable migration paths today are hybridized ML-KEM, standalone ML-KEM, standalone ML-DSA, and, to some extent, standalone SLH-DSA. Alternative PQC algorithms (such as FN-DSA and HQC) and hybrid signatures are unlikely to be standardized or broadly implemented in time to meet the required deployment timelines.

In TLS, X25519MLKEM768 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 requests use PQC [25]. OpenSSL 3.5 LTS supports ML-KEM, ML-DSA, and SLH-DSA [26]. OpenSSH is now using mlkem768x25519 as the default key exchange [27], and many IKEv2 implementations support ML-KEM [28], which in IKEv2 is always hybridized with (EC)DHE. The availability of well-tested and interoperable implementations is an essential factor for industry adoption, as it enables cost-effective and reliable 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, the vast majority of the authors of Kyber, Dilithium, and SPHINCS$^+$ are European researchers, many of them supported by European universities, institutes, and companies. Research funding from EU Member States and the European Commission has been instrumental in making this possible. These investments have helped Europe play a central role in securing the world's digital infrastructure against future threats. This is an achievement that the NIS Cooperation Group should explicitly acknowledge and celebrate in its report.

- *"The most promising solution is so-called post-quantum cryptography (PQC)"*

  PQC is not merely "promising", it is already widely deployed and the only solution that does not require costly or complex changes to existing architectures. For most use cases, it is the only viable solution. It should be clearly emphasized that quantum key distribution (QKD) is not a solution. As government experts correctly state, QKD is not mature for any real-world application and, at best, could serve as defense-in-depth only in 20 years [17]. Any discussion of QKD risks diverting attention and resources from the urgent priority: migrating to PQC. Such a distraction would be both costly and dangerous. Europe is already behind the US in adopting PQC, which is essential for European cybersecurity, and a misguided focus on QKD projects has been one contributing factor. Quantum communication should be treated as basic research, with no practical use for cybersecurity.

- *"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. However, to meet the EU roadmap timelines of 100% PQC in deployment by 2030–2035, this step should have been initiated years ago. Organizations 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. Cryptographic inventories do not need to be complete to be valuable; even partial inventories that track only public-key algorithms, protocol versions, and library versions can help organizations identify and prioritize upgrades during the PQC migration.

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

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

It is not realistic to expect that each Member State can individually create communities that attract global organizations, entities, and stakeholders such as the IETF, 3GPP, US government, or US companies. Even coordinating this at the EU level is extremely challenging. Instead, Member States should actively participate in open, global standardization organizations such as the IETF ETSI, and 3GPP, as well as in the open-source cryptographic community, to ensure alignment, influence, and knowledge-sharing at the international level.

- We think the report does a good job of emphasizing the importance of protecting the confidentiality and integrity of data. However, it should also explicitly address the need to protect data during processing. Furthermore, rather than using terms such as "stored," "transmitted," and "communication," we suggest consistently using the widely accepted formulation: "protect the confidentiality and integrity of data in transit, at rest, and during processing."

  In addition, the report should 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.

Feedback to guide the next steps, including the technical recommendations:

- As stated above, we think the technical recommendations should fully embrace ML-KEM, ML-DSA, and SLH-DSA [1–3]. These global standards, largely developed by European cryptographers generously funded by Member States and the European Commission, are now endorsed with the highest level of confidence by European government agencies. Many European companies are already deeply engaged in developing and integrating these algorithms to meet the ambitious 2030–2035 PQC deployment timelines. Hybridized ML-KEM, standalone ML-KEM, standalone ML-DSA, and, to some extent, standalone SLH-DSA have already achieved broad implementation support and deployments. At present, they are the only realistic migration paths for European industry. The availability of well-tested, interoperable implementations is a key factor for industry adoption, enabling cost-effective and reliable deployments.

- We believe that technical recommendations should minimize exemptions from NIST specifications such as FIPS 180, 197, and 202–205. Diverging from these international standards introduces unnecessary cost and complexity for European industry, reducing competitiveness. This becomes especially problematic when requirements are imposed on constrained radio systems or applied retroactively to existing products and deployments [30–31]. NIST standards already strike a good balance: all approved options in FIPS 180, 197, and 202–205 provide adequate long-term protection for industrial use cases. Any profiling should be left to industry-led standardization bodies, which have the expertise to assess how cryptographic algorithms are used in their systems, the required protection lifetimes, the value of protected assets, system

upgrade cycles, and the availability of backup algorithms. For example, 3GPP profiles for X.509, IPsec, and TLS [32–33] are far stricter than their IETF counterparts, an appropriate approach for critical infrastructure such as 5G. This kind of industry-driven, standards-based process is vastly preferable to top-down regulation and better supports both technical innovation and economic growth.

- We do not believe the technical recommendations should be based on the ECCG Agreed Cryptographic Mechanisms [34], which appears primarily intended for national security systems and does not meet industrial requirements. Applying [34] as general guidance for European industry would impose significant costs, reduce the competitiveness of European companies and their products, and provide no practical security benefits.

  In particular, we strongly oppose the claim that 128–191-bit symmetric keys are under threat from quantum computers. The idea that CRQCs pose a practical risk to 128-bit symmetric algorithms is now seen as a misconception [4, 18-21]. For example, breaking a single 191-bit key would require a quantum computer with qubits covering the surface area of a very large star, which is very clearly not an attack of practical concern. We also oppose the suggestion that SLH-DSA level 1 should not be recommended. SLH-DSA is a substantially more conservative design than RSA or ECDSA, and we would place much greater trust in SLH-DSA level 1 than, for example, RSA-4096. For constrained systems, it is vital that level 1 of all PQC algorithms remain approved for industrial use. The increased sizes of public keys, signatures, and encapsulations are already difficult to accommodate at level 1. NIST has correctly designated level 1 as quantum-resistant, and there is no justification for revising this assessment. Finally, as noted above, hybrid signatures are neither standardized nor mature from an implementation standpoint and will not be ready in time to meet the EU roadmap timelines.

- It is noteworthy that the US government engages with European industry both more extensively and at a much earlier stage during the standardization process than European government organizations do. NIST has long recognized that input from cryptographers across global industries is essential to producing strong and widely adopted cryptographic and cybersecurity standards. Ericsson, for example, has submitted numerous public comments to NIST's cryptography standardization efforts in recent years [35], many of which have had a significant impact on the evolution of those standards. By comparison, the European Cybersecurity Certification Group has not, to our knowledge, yet sought public feedback on the Agreed Cryptographic Mechanisms. In this context, it is very positive that the NIS Cooperation Group is inviting feedback on the next steps well in advance of publishing its technical recommendations on PQC. We would encourage the Group to build on this openness by following NIST's example of releasing an Initial Public Draft (IPD) and actively engaging industry, academia, and international government agencies in the review process.

- The European telecom sector is well prepared for the transition to post-quantum cryptography (PQC). Both 3GPP and GSMA have been addressing the quantum threat and the PQC migration for many years. The GSMA Post-Quantum Telco Network Taskforce (PQTN) [36], launched in 2022, was established to promote awareness and readiness across the telecom ecosystem. Notably, the PQTN has published guidelines on PQC for telecom-specific use cases [37]. Following the publication of FIPS 203–205, the 3GPP security group SA3 initiated a Study on Transitioning to Post-Quantum Cryptography [38], with the aim of preparing normative work later in

Release 20. This will make 6G, which is expected from Release 21, fully quantum-resistant from the start. Since the vast majority of public-key cryptography in 5G relies on IETF protocols, vendors can begin migrating to PQC without having to wait for 3GPP to update its cryptographic profiles. For telecom-specific protocols, such as SUCI protection [39] and eSIM provisioning [40], concrete upgrade paths have already been specified and are expected to be standardized shortly. ETSI SAGE [41], the cryptography expert group will support 3GPP as needed. For an overview of the progress in migrating telecom networks to quantum-resistant cryptography on a global scale, see [42–43].

John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols, Ericsson

References

[1] FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[2] FIPS 204, Module-Lattice-Based Digital Signature Standard
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[3] FIPS 205, Stateless Hash-Based Digital Signature Standard
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[4] NIST IR 8547 ipd, Transition to Post-Quantum Cryptography Standards
https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[5] CNSA 2.0, Announcing the Commercial National Security Algorithm Suite 2.0
https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[6] ANSSI-PG-083, GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES
https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf

[7] ANSSI views on the Post-Quantum Cryptography transition
https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

[8] BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html

[9] Timelines for migration to post-quantum cryptography
https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[10] Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information
https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111

[11] National Quantum Strategy roadmap: Quantum communication and post-quantum cryptography
https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography

[12] Guidelines for cryptography
https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography

[13] Kvantsäker kryptografi
https://www.ncsc.se/sv/aktuellt/kvantsaker-kryptografi/

[14] NSM Cryptographic Recommendations
https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf

[15] The PQC Migration Handbook
https://english.aivd.nl/binaries/aivd-en/documenten/publications/2024/12/3/the-pqc-migration-handbook/The+PQC+Migration+Handbook+.pdf

[16] PQC Dialogue with Government Stakeholders – Slides
https://emanjon.github.io/Slides/2025%20PQC%20side-meeting.pdf

[17] PQC Dialogue with Government Stakeholders – Recording, summary, and transcript
https://ietf.webex.com/recordingservice/sites/ietf/recording/1e87f518ecb1413b9357e607cf825642/playback

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

[19] 3GPP Statement on PQC Migration
https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip

[20] Sam Jaques, "Quantum Attacks on AES "
https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s

[21] NCSC, Next steps in preparing for post-quantum cryptography
https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

[22] Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3
https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/

[23] PQ/T Hybrid Key Exchange in SSH
https://datatracker.ietf.org/doc/draft-ietf-sshm-mlkem-hybrid-kex/

[24] Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)
https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-mlkem/

[25] Post-quantum encryption adoption
https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryption-adoption

[26] OpenSSL 3.5 Final Release
https://openssl-library.org/post/2025-04-08-openssl-35-final-release/

[27] OpenSSH 10.0 Release Notes
https://www.openssh.com/txt/release-10.0

[28] What's New in strongSwan 6.0
https://github.com/strongswan/strongswan/releases/tag/6.0.0

[29] ANSSI views on technical aspects of the migration to PQC
https://na.eventscloud.com/file_uploads/b635298de1c10be6d3732863e8b1beca_Day2-1600-ANSSI.pdf

[30] Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange
https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/constrained-radio-networks-pqc2022.pdf

[31] Ericsson Comments on SP 800-38B (CMAC)
https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/initial-comments/sp800-38b-initial-public-comments-2024.pdf

[32] 3GPP TS 33.210 Network Domain Security (NDS); IP network layer security
https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/constrained-radio-networks-pqc2022.pdf

[33] 3GPP TS 33.310 Network Domain Security (NDS); Authentication Framework (AF)
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293

[34] Agreed Cryptographic Mechanisms
https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf

[35] Ericsson comments on cryptography submitted to NIST
https://github.com/emanjon/NIST-comments

[36] GSMA Post Quantum Telco Network Task Force
https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum-telco-network-task-force/

[37] GSMA PQ.03 Post Quantum Cryptography – Guidelines for Telecom Use Cases
https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

[38] Study on Transitioning to Post Quantum Cryptography in 3GPP
https://www.3gpp.org/FTP/Meetings_3GPP_SYNC/SA/Docs/SP-250858.zip

[39] LS on Augmenting SUCI Protection with ML-KEM
https://www.3gpp.org/ftp/Email_Discussions/SA3/SA3%23122/PQC/S3-25xxxx_LS%20SAGE%20ML-KEM%20SUCI.docx

[40] Post-Quantum Secure Channel Protocols for eSIMs
https://eprint.iacr.org/2024/2005.pdf

[41] ETSI SAGE
https://portal.etsi.org/TB-SiteMap/Sage/Activity-Report

[42] Ericsson, Migrating Telecom to Quantum-Resistant Cryptography on a Global – Slides
https://datatracker.ietf.org/meeting/123/materials/slides-123-ietf-sessd-ietf-123-host-speaker-slides-00

[43] Ericsson, Migrating Telecom to Quantum-Resistant Cryptography on a Global – Recording
https://www.youtube.com/watch?v=4xed46xUfa0