Council of the
European Union

Brussels, 22 April 2024
(OR. en)

9212/24

CYBER 129
TELECOM 162
COSI 62
COPEN 210
CSDP/PSDC 281
DATAPROTECT 192
IND 224
RECH 189
PROCIV 25
HYBRID 55
JAI 692
COMPET 465
MI 436
ESPACE 38

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	11 April 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2024) 2393 final
Subject:	COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

Delegations will find attached document C(2024) 2393 final.

Encl.: C(2024) 2393 final

EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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[1] (NIS 2 Directive).

Whereas:

(1) Safeguarding data and securing sensitive communications are vital for Union's society, economy, security and prosperity. Cybersecurity is of strategic importance in building 'Europe Fit for the Digital Age'[2], and a key objective of the Digital Decade policy programme[3] .

(2) The EU Security Union Strategy[4] and the EU Cybersecurity Strategy[5] both highlight encryption as a key technology for achieving resilience, technological sovereignty and for building operational capacity to prevent cyberattacks. In fact, encryption is essential to the digital world for securing digital systems and transactions, for protecting a series of fundamental rights as well as for securing defence capabilities. The race pursued by various countries and private entities for developing quantum computing capabilities, and unlocking new potentially rewarding opportunities, poses threats to current cryptographic standards. These standards play a pivotal role in ensuring data confidentiality, and integrity, the protection of sensitive communications, and supporting essential elements of network security.

(3) The future potential development of quantum computers capable of breaking today's encryption makes it necessary for Europe to look for stronger safeguards, ensuring the protection of sensitive communications and the long-term integrity of confidential information, i.e., by switching to Post-Quantum Cryptography as swiftly as possible. This new type of cryptography will remove the known vulnerabilities of current asymmetric cryptography and enhance the robustness against the threats posed by the malicious use of quantum computers.

---

1 OJ L 333, 27.12.2022, p. 80.
2 COM(2020) 67 final
3 Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L 323, 19.12.2022, p. 4).
4 COM(2020) 605 final
5 JOIN(2020) 18 final

(4) The Commission has been funding research and development Post-Quantum Cryptography for over a decade, recognizing the potential threat quantum computing poses to present public key cryptography.

(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper “How to master Europe’s digital infrastructure needs”, this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

(6) This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap. This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.

(7) For an effective transition to Post-Quantum Cryptography, the Post-Quantum Cryptography Coordinated Implementation Roadmap should provide the list of actions to be addressed by the Member States, including the consideration of Post-Quantum Cryptography algorithms, with a clear timeline for different phases and milestones to be reached, taking into account their interdependencies, as well as the stakeholders to be involved.

(8) For a harmonized implementation of Post-Quantum Cryptography across the Union it is essential to develop common European standards and develop a framework for identifying and selecting Post-Quantum Cryptography algorithms to be deployed in the digital networks and services across the Union. Through the active participation of EU-funded researchers, the Union is already supporting the development and testing of Post-Quantum Cryptography algorithm candidates for standards in international Post-Quantum Cryptography selection processes. This Commission Recommendation encourages Member States to work at EU-level closely with the Union’s cybersecurity experts, with the NIS Cooperation Group and with the European Union Agency for Cybersecurity (ENISA), on the evaluation and selection of the appropriate Post-Quantum Cryptography algorithms and their adoption as EU standards for a harmonized implementation across the Union.

(9) Member States and the Union should continue to cooperate actively with their international strategic partners in the development of international standards in Post-Quantum Cryptography with a view to ensuring interoperability of communications going forward.

(10) Once agreed by the Member States, the Post-Quantum Cryptography Coordinated Implementation Roadmap should serve as blueprint for the definition of the national transition plans towards Post Quantum Cryptography, or, where national plans exist, their alignment with the common Post-Quantum Cryptography Coordinated Implementation Roadmap.

(11) To ensure progress is made against the objectives of this Recommendation, the Commission intends to monitor closely the actions taken in response to the Recommendation. Member States are therefore encouraged to submit to the Commission, upon its request, all relevant information, which they can reasonably be expected to provide, to ensure such monitoring. On the basis of the information thus obtained and all other available information, the Commission will assess the effects of this Recommendation and determine whether additional steps, including proposing binding acts of Union law, are required.

(12) This Recommendation on Post-Quantum Cryptography builds on the policy objectives set out in the EU Cybersecurity Strategy for improving the end-to-end security and resilience of the Union's digital infrastructures and services for public administrations and other critical infrastructures; it serves the objectives of the Digital Single Market, and of the Joint Communication on European Economic Security Strategy 10919/23[6]; and it considers the risks to the physical and cyber security of critical infrastructures, as well as those identified under the recently conducted risk assessment for quantum technologies[7]. It respects the fundamental rights and observes the principles recognized in particular by the EU Charter of Fundamental Rights (Articles 7, 8, and 11) and European Convention on Human Rights (Articles 8 and 10), which imply positive obligations on governments to minimize the risk of unlawful access and control of information, necessitating the safeguarding and promotion of cryptographic technologies.

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

(4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national

6 https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/en/pdf

7 JOIN(2023) 20 final

security agencies and cybersecurity experts, notably from national cybersecurity authorities and ENISA. The sub-group may invite representatives of relevant stakeholders to participate in its work such as those of advisory bodies of public organisations, industry, service providers, and operators, with a view to gather input and exchange information on the transition of digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography in different sectors, coordinate their efforts at national level, and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap, in accordance with the Union competition rules and Union data protection law.

(5) This sub-group on Post-Quantum Cryptography should consider appropriate, effective and proportionate measures for defining and coordinating the development of the Post-Quantum Cryptography Coordinated Implementation Roadmap. The sub-group on Post-Quantum Cryptography is encouraged to engage in discussions with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges.

(6) To this effect, soon after the publication of this Recommendation, Member States are invited to establish such a sub-group on Post-Quantum Cryptography pursuant to Commission implementing decision (EU)2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and who should be tasked to define and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(7) The Post-Quantum Cryptography Coordinated Implementation Roadmap should be available after a period of two years following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.

3. ACTIONS AT UNION LEVEL

(8) The overall work will be monitored and assessed periodically by the Commission in cooperation with the expert representatives of the Member States.

(9) To this effect, the Commission may request Member States' representatives to submit all relevant information, which they can reasonably be expected to provide, to ensure the monitoring of the progress achieved in drafting such Post-Quantum Cryptography Coordinated Implementation Roadmap and the effectiveness of such measures.

(10) On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States' representatives and determine whether additional actions, including proposing binding acts of Union law, are required.

4. REVIEW

(11) Member States should cooperate with the Commission to assess the effects of this Recommendation maximum three years after its publication, with a view to determine appropriate ways forward. This assessment should take into account the outcome of the work by the sub-group on Post-Quantum Cryptography of national experts.

Done at Brussels, 11.4.2024

For the Commission
Thierry BRETON
Member of the Commission

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION