bipt

Belgian Institute for Postal Services and Telecommunications

Communication of the BIPT Council of 13/01/2026 on minimum requirements and a roadmap for the post-quantum transition in the telecommunications sector

Belgian Institute for Postal Services and Telecommunications
Boulevard du Roi Albert II 32 box 10 | 1000 Brussels
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The development of quantum computers threatens to make certain cryptographic algorithms used to secure telecommunications networks obsolete.

Given the risks of retroactive compromise via Store-Now-Decrypt-Later attacks and potentially severe consequences on customer confidentiality and service continuity, in order to ensure compliance with the Recommendation of 11 April 2024, EU Member States are working to ensure a coordinated transition towards post-quantum cryptography (PQC).

This document translates the European expectations at national level by defining the minimum requirements for quantum risk management and transition to post-quantum cryptography, as well as by setting the sector timeline for the objectives of the Belgian telecommunications operators.

The chosen referral approach is structured into three phases.

It includes:

- Inventorying cryptographic assets and analysing quantum risks;
- Planning the migration with the designation of a supervisor of the ecosystem coordination;
- Carrying out the progressive deployment of the solutions.

The sector timeline sets objectives ranging from the finalisation of inventories as from the publication of the document to the completion of the migration by 2030 for the most critical systems, with a supervision mechanism as foreseen within the framework of the Act of 13 June 2005 on electronic communications, as well as the NIS2 and CER (Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities) directives, to meet the European quantum resilience objectives by 2035.

1. Introduction

1. The development of quantum computers threatens to make numerous current cryptographic algorithms obsolete, in particular asymmetric algorithms (either RSA[1] or elliptic curves) used to secure telecommunications networks. [1]

2. Malicious perpetrators could now use this threat via Store-Now-Decrypt-Later attacks, by intercepting and storing encrypted communications to decrypt them once a sufficiently powerful quantum computer is available. [2] [3] The integrity and authenticity of data are also at stake, as breaking digital signatures could enable them to falsify software updates or critical records. [2]

3. In the face of these risks with potentially severe consequences (compromising customer confidentiality, service interruption, financial losses) [2], a coordinated transition towards post-quantum cryptography (PQC) becomes necessary. [3]

4. For several years now, major efforts have been ongoing to standardise PQC. The National Institute of Standards and Technology ("NIST") in the United States selected new algorithms resistant to quantum computers (e.g. CRYSTALS-Kyber for key generation, CRYSTALS-Dilithium for signatures) and published in 2024 the first official standards for post-quantum cryptography. [4]

5. Advances in standardisation and solution development are laying the technical foundations necessary for the transition. It is also the responsibility of the sector to take the necessary steps to accompany this dynamic and prepare for the quantum threat and be open to innovative technological solutions to guard against this threat. The temporary immaturity of solutions cannot justify inaction.

1.1 Objective and scope of the document

6. This document proposes a normative framework to accompany, supervise and assess the post-quantum transition of Belgian telecommunications operators designated as critical infrastructures. It provides a baseline for future inspections and aims to ensure a consistent minimum level of quantum security in the sector.

7. This document is in line with European expectations by laying down minimal requirements for the assessment, planification and execution of the transition, governance criteria of the quantum risks, and harmonisation with the European quantum resilience agenda (2026, 2030, 2035).

8. This document defines minimum requirements and proposes practices aligned with the state of the art. However, if alternatives better suited to an operator's specific context also meet these requirements, their use remains possible, provided they are justified.

[1] RSA stands for "Rivest–Shamir–Adleman". This is the name of the cryptographic algorithm.

9. **Exclusion of the scope of application:**
Quantum Key Distribution (QKD) technologies and other quantum cryptography solutions fall outside of the scope of this document, which only focuses on migration towards standardised post-quantum cryptographic algorithms.

2. Telecommunications background

10. Belgian electronic communications network operators correspond to the Urgent Adopters persona[2] according to the taxonomy established by the PQC Migration Handbook. [4] This results from the criticality of their infrastructure, operational longevity of their equipment and systemic exposition to quantum threat.

11. This means that operators must:

- immediately initiate post-quantum migration processes;
- implement a governance dedicated to quantum risks;
- establish a binding transition timeline;
- periodically report the progress of the migration process.

2.1 Quantum vulnerability of current telecommunications networks

12. The cryptographic architecture of telecommunications networks presents a layered vulnerability to quantum threats. As shown in Figure 1, the bottom layers of the network stack mainly use symmetric encryption on static connections (e.g. AES), whereas upper layers more often use asymmetric encryption on dynamic connections for key negotiations and/or authentication (e.g. TLS). The symmetric cryptography used in the bottom layers for the encryption of static connections requires an evaluation of the key sizes and distribution mechanisms. The asymmetric encryption, predominant in the upper layers (transport, application) for key generation and authentication, is a critical vulnerability requiring priority migration towards post-quantum standards. [5]

13. Operators must assess the quantum vulnerability of each security area of their infrastructure:

13.1. **Data plan:**
Transport of user communications with end-to-end cryptographic protection. Risk of retroactive compromise of sensitive data.

13.2. **Control plan:**
Network signalling and traffic routing. Critical vulnerability which may compromise the overall operational integrity of the network.

[2] A "persona" is a category of organisations defined according to their specific needs in terms of post-quantum migration. [4]

13.3. **Management plan:**
Configuration and monitoring of the network resources. Exposure of management systems via unsecured administration protocols to risks posed by quantum technologies.

13.4. **Network exposure interfaces:**
Network programmability APIs introducing new attack surfaces. These APIs enable external applications to control certain network functions of the operator (bandwidth allocation, quality of service, routing). These interfaces use cryptographic authentication mechanisms that are vulnerable to quantum attacks, risks amplified by the increasing opening-up of network architectures.

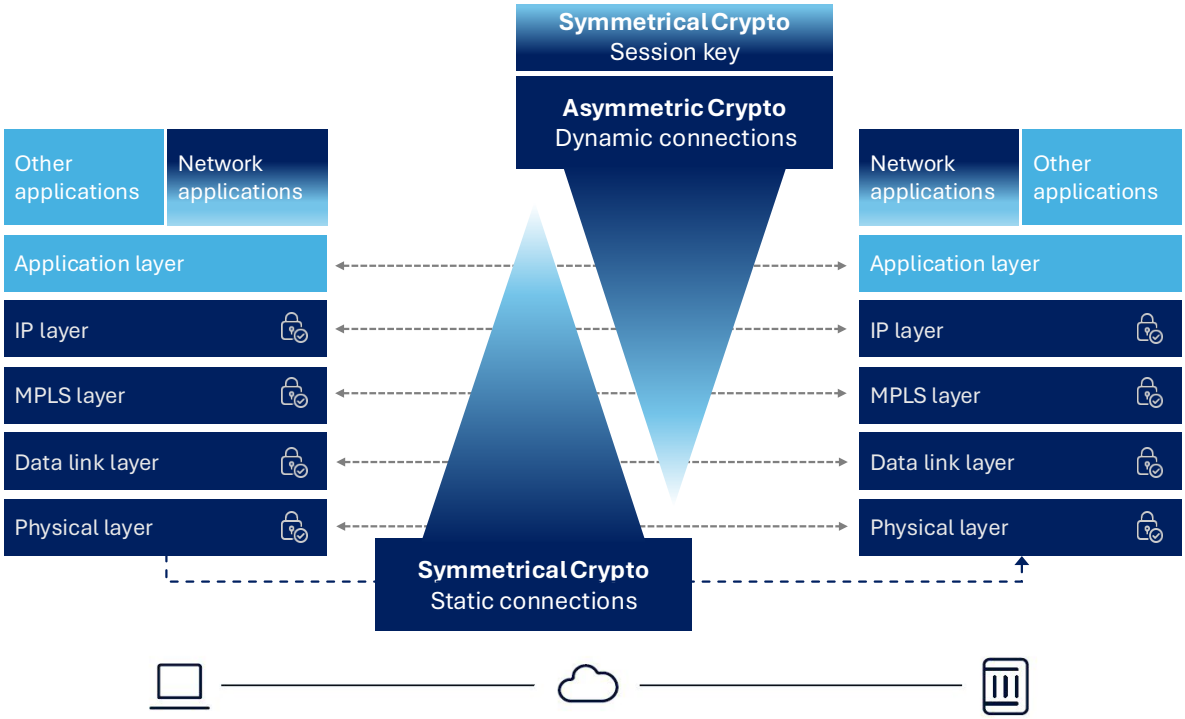

Figure 1: SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY IN THE DIFFERENT NETWORK LAYERS [5]

2.2 Overview of the post-quantum telecommunications ecosystem

14. The post-quantum transition of telecommunications operators cannot be considered in isolation. The vulnerabilities mentioned, and thus the PQC transition, belong to a complex ecosystem of cryptographic interdependencies amplifying the risks of propagation of quantum vulnerabilities. The cartography below [2] illustrates these dependency flows that determine the success of post-quantum migration.

15. Operators must establish the most complete cartography of their chains of cryptographic dependencies, assess the risks of cascading failure, and coordinate their migration plans with every player in their technological ecosystems.

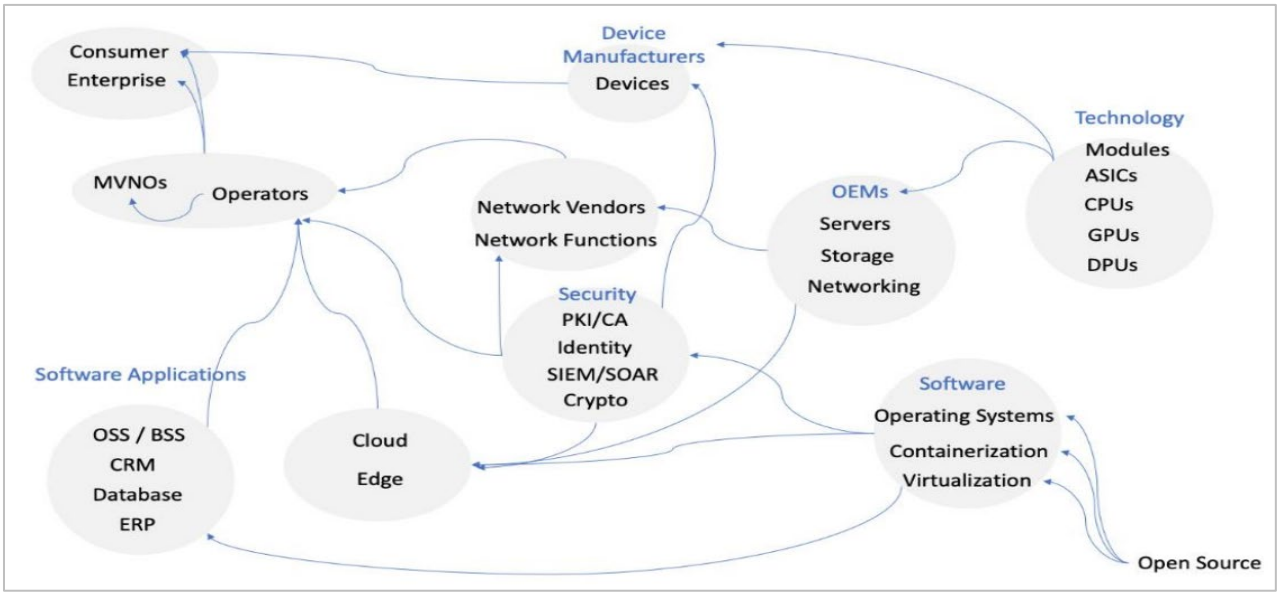

Figure 2: EXAMPLE OF STRUCTURE OF DEPENDENCIES OF THE POST-QUANTUM ECOSYSTEM [2]

3. PQC migration

16. Operators are encouraged to adopt a migration procedure that is made up of three phases in line with the good practices developed by ETSI " [6]" and in the TNO[3] Migration Handbook [4]. This approach facilitates a controlled and verifiable transition towards post-quantum crypto-systems.

Figure 3: THE 3 PHASES OF MIGRATION

[3] "TNO" stands for "Toegepast Natuurwetenschappelijk Onderzoek".

17. Phase 1: Assessment and diagnosis of the quantum vulnerabilities

- Inventory of cryptographic assets: exhaustive inventory of all cryptographic components, protocols and implementations deployed
- Analysis of quantum risks: assessment of the exposure of each asset to the quantum threat with classification by operational criticality

18. Operators must regularly keep their cryptographic inventory and quantum risk analyses up to date. This periodic review obligation is necessary given the constant evolution of IT environments and potential emergence of new quantum vulnerabilities. Furthermore, this approach is good practice in terms of IT security beyond quantum issues alone.

19. Phase 2: Migration planification

- Creation of a migration plan with deadlines and control milestones;
- Definition of migration priorities based on the risk analysis;
- Coordination with the ecosystem of technological suppliers and partners.

20. Phase 3: Execution of the migration

- Phased roll-out of the post-quantum solutions according to the plan;
- Conformity validation and interoperability tests;
- Maintaining operational continuity during the transition.

21. Although the migration to post-quantum algorithms is a necessary response to a quantum threat, this transition does not guarantee absolute security. Post-quantum implementations under real conditions will likely have inherent vulnerabilities including algorithmic flaws, sub-optimal choices of domain parameters, weak key generation, implementation bugs and vulnerabilities to attacks via subsidiary channels. These limitations emphasise the critical importance of cryptographic agility[4] as a resilience mechanism.

22. Cryptographic agility should enable operators to quickly respond to discovered vulnerabilities, the evolution of security recommendation and cryptanalytic advances. This adaptability is a key component of the post-quantum security strategy, making thus migration a permanent improvement process.

23. A successful post-quantum migration is thus based on the organisational capacity to understand and manage the technical and strategic challenges of this transition.

24. Operators must ensure that their teams have the knowledge needed to conduct the migration and maintain continuous technological monitoring of developments in post-quantum standards and emerging vulnerabilities.

[4] Cryptographic agility or crypto-agility describes the organisational and technical capacity enabling to replace the cryptographic algorithms in existing systems (protocols, applications, equipment, infrastructure) without having to systematically reconfigure or replace all systems, while maintaining security and operational continuity during the transition.[9]

3.1 Phase 1: Assessment and diagnosis in the face of the quantum threat

25. The assessment and diagnosis phase is an essential prerequisite for any post-quantum migration. This phase aims to establish a precise understanding of exposure to quantum risks and to structure the transition process. The objectives of this phase are the following:

- Identify the assets to be migrated in priority according to their operational criticality and quantum vulnerability;
- Map the existing dependencies within the technological ecosystem of the operator;
- Anticipate the potential impacts of migration on service continuity and performance.

26. Operators must adapt the order and granularity of the assessment activities to their operational constraints. In practice, several assessment or information gathering activities can be carried out in parallel. A step-by-step approach, starting with the analysis of the most critical systems, is an acceptable strategy to initiate the process while quickly generating value.

3.1.1 Inventory of cryptographic assets

27. An effective inventory approach is based on a structured discovery/exploration strategy for its assets covering all cryptographic usage contexts: source code and integrated libraries, operational systems and applications deployed, as well as network traffic and communication protocols.

28. The formalisation of the results in a standardised format such as the Cryptographic Bill of Materials (CBOM) facilitates the analysis, sharing and maintenance of the inventory. Automating the discovery, where technically possible, improves the reliability and completeness of the process while reducing the operational burden.

29. For telecommunications operators, a priority-based approach enables to focus initial efforts on the most critical components: network core infrastructure, signalling protocols, network access interfaces, and exposed management systems.

30. Operators must:

- Have a formalised cryptographic policy defining the rules governing cryptographic assets;
- Maintain a complete and up-to-date inventory of their cryptographic assets covering their entire infrastructure;
- Document cryptographic dependencies with their technology suppliers and partners;
- Periodically review this inventory to reflect changes in their environment.

3.1.2 Analysis of quantum risks

31. A structured analysis of quantum risks is based on the assessment of several dimensions: the intrinsic vulnerability of cryptographic primitives to quantum algorithms, the potential impact of a compromise on operations, and the complexity of migrating to post-quantum alternatives.

32. Methodologies such as the one developed by TNO [7] or the GSMA sectoral guidelines [1] provide assessment criteria and decision-support tools for better management of quantum risks. The use of these structured approaches makes it possible to systematise the analysis and ensure consistency of assessments in the prioritisation of migration actions.

33. Collaboration with experts in quantum cryptography and consultation of the recommendations of standardisation bodies enhance the quality and relevance of the analysis.

34. Operators must:

- Conduct a quantum risk analysis covering all of their inventoried cryptographic assets;
- Establish a criticality classification to prioritise migration actions;
- Document the reasons and criteria for the decisions made;
- Update this analysis as the quantum threat and infrastructures evolve.

3.2 Phase 2: Migration planification

35. Migration planning structures the transition to post-quantum cryptographic systems by defining priorities, resources and deadlines. This phase determines the appropriate migration strategies for each asset category and establishes the necessary coordination with the technology ecosystem.

36. Effective planning relies on the creation of a dedicated team with an identified migration manager, the allocation of the necessary budgetary and technical resources, and the establishment of a timetable that takes into account cross-system dependencies [4]. The definition of migration strategies adapted to the specificities of each component (hybrid approach, temporary isolation, hardware replacement) optimises the efficiency of the process.

37. Operators must:

- Formally appoint a post-quantum migration manager with a cross-functional view of the organisation;
- Establish a documented migration plan setting priorities based on the quantum risk analysis of phase 1.
- Define for each critical asset a migration strategy (hybrid[5], direct replacement, isolation).

[5] Hybridisation: an approach that simultaneously combines post-quantum algorithms with proven classical cryptographic algorithms to mitigate the risks associated with the relative youth of new cryptographic primitives while providing protection against the quantum threat. Recommended in particular by the ANSSI and BSI.

3.3 Phase 3: Execution of the migration

38. The execution of the migration implements the strategies defined during planning with a focus on approaches that minimise operational risk. This phase requires particular attention to validate the deployed solutions and maintain continuity of services.

39. The post-quantum migration process must maintain and strengthen cryptographic resilience throughout the transition phase. This resilience is based on a defence-in-depth approach, long-term security (anticipation of cryptanalytic developments), and cryptographic agility (rapid substitution of primitives according to security recommendations).

40. Operators must:

- Respect the order of priority established during the quantum risk analysis;
- Maintain a traceability record documenting each migration performed with dates and versions;
- Validate compliance and interoperability prior to production of each post-quantum solution.

3.4 Mapping of the GSMA recommendations and requirements set by the BIPT

41. This section links the recommendations made by the GSMA within the framework of its guidelines to the minimum requirements set by the BIPT in this document.

	GSMA RECOMMENDATIONS [1]	BIPT REQUIREMENTS
GOVERNANCE	Awareness at the decision-making level: raising awareness of the quantum threat within senior management and the board of directors.	Operators must: ▪ Immediately initiate the migration process. Any delay in initiating this procedure constitutes a breach of security obligations; ▪ Implement a governance dedicated to quantum risks; ▪ Define the roles and responsibilities related to PQC migration and its preparation.
	Organisational governance process: implement a cross-cutting governance process for quantum risk management.	
	Executive responsibility: formally appoint a post-quantum migration manager with a cross-functional view of the organisation.	

	GSMA RECOMMENDATIONS [1]	BIPT REQUIREMENTS
ORGANISATIONAL CAPACITY	Skills development: develop organisational capabilities to manage quantum risks and post-quantum transition.	Operators must: ▪ Ensure that their teams have the knowledge needed to conduct the migration and maintain continuous technological monitoring of developments in post-quantum standards and emerging vulnerabilities.
	Training and awareness: update the training programs to improve understanding of quantum challenges in the telecom context.	
	Technological monitoring: monitor the development of tools facilitating the transition, especially hybrid solutions and standards.	

	GSMA RECOMMENDATIONS [1]	BIPT REQUIREMENTS
RISK MANAGEMENT	Risk management Framework: adapt the existing risk management methodology to specifically integrate quantum risks. Analysis of quantum risks: conduct a complete and rigorous quantum risk analysis covering all of the inventoried cryptographic assets. Residual risk management: identify and manage residual risks during and after the transition.	Operators must: ▪ Have a formalised cryptographic policy defining the rules governing cryptographic assets; ▪ Conduct a quantum risk analysis covering all of their inventoried cryptographic asset; ▪ Periodically review this inventory to reflect changes in their environment; ▪ Update this analysis as the quantum threat and infrastructures evolve.

	GSMA RECOMMENDATIONS [1]	BIPT REQUIREMENTS
TRANSITION PLANNING	Cryptographic inventory: maintain a complete and up-to-date inventory of the cryptographic assets covering the entire infrastructure. Data classification: document cryptographic dependencies with technology suppliers and partners, identifying protection requirements and data longevity. Prioritisation: establish a criticality classification to prioritise migration actions based on a quantum risk analysis. Transition plan: establish a documented migration plan defining priorities, migration strategies for each critical asset, and meeting defined industry deadlines.	Operators must: ▪ Maintain a complete and up-to-date inventory of their cryptographic assets covering their entire infrastructure; ▪ Periodically review this inventory to reflect changes in their environment; ▪ Document cryptographic dependencies with their technology suppliers and partners; ▪ Establish a criticality classification to prioritise migration actions; ▪ Update the analyses and, where needed, the migration plan according to the evolution of the quantum threat and infrastructures; ▪ Document the reasons and criteria for the decisions made.

4. Timeline

42. The post-quantum transition is part of a coordinated European agenda.

43. Recommendation (EU) 2024/1101 [8] and the work of the EU PQC Workstream [3] provide a time frame for structuring this transition at European level, with targets for developing national roadmaps by 2026.

44. The European timeline developed by the EU PQC Workstream [3] establishes a progression in three major steps towards quantum resilience.

    The initiation phase, already under way in accordance with the joint declaration of 18 Member States "Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography" marks the coordinated beginning of the transition.

    By 2026, the planning of PQC transition and the pilot projects for high and medium risk use cases must be initiated.

    The critical milestone for 2030 is the completion of the PQC transition for high-risk use cases, with software and firmware updates incorporating quantum security enabled by default. This progress culminates in 2035 with the objective of a full quantum resilience of the European infrastructure.

45. On the basis of this European timetable, the following objectives and deadlines have been defined for the Belgian telecommunications sector :

    - Deadline 1 - Assessment (2027): Finalising the cryptographic inventory and quantum risk analysis;
    - Deadline 2 - Planning (2028): Development and validation of the post-quantum migration plans;
    - Deadline 3 - Implementation (2030): Phased roll-out of the post-quantum solutions according to the established priorities.

46. This sectoral timeline sets out the European objectives for critical telecommunications infrastructure, ensuring a coordinated and harmonised transition.

4.1 Monitoring timeline

47. To ensure that these objectives are achieved, a supervisory mechanism is provided. This monitoring timeline ensures the convergence of national efforts towards the common goal of quantum resilience by 2035.

48. 2027 - 2028 -- Audit of foundations:

- Verifying the inventory of cryptographic assets;
- Assessment of the quantum risk analyses;
- Assessment of drawn-up migration plans.

49. 2029 - 2030 – Control of quantum risk management systems:

- Monitoring the implementation of quantum risk management systems;
- Monitoring the progress of critical migrations;
- Assessment of the post-quantum governance.

50. 2031 - 2035 -- Inspection of high-risk systems:

- Verification of the migration of priority assets.

51. From 2036 onwards – Control of medium-risk and low-risk systems.

References

[1] Guidelines for quantum risk management for telco v1.0, 2023. Url: Guidelines for Quantum Risk Management for Telco

[2] GSMA, Post quantum Telco Network Impact Assessment - Whitepaper Version 1.0, 2023. Url: PQTN_1_Doc_006 PQTN White Paper CLEAN

[3] NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2025 ("NIS" stands for "Network and Information Systems"; Url: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future

[4] AIVD-CWI-TNO, The PQC Migration Handbook - guidelines for migrating to post-quantum cryptography, 2024. ("AIVD" stands for "Algemene Inlichtingen- en Veiligheidsdienst"; "CWI" stands for "Centrum Wiskunde & Informatica"; "TNO" stands for "Toegepast Natuurwetenschappelijk Onderzoek") Url: TNO-2024-pqc-en.pdf

[5] W. Coomans, D. Schoinianakis, R. Sohn, S. Chenard, A. Banerjee et M. Charbonneau, The road to quantum-safe networks, Nokia Bell Labs, 2025. Url: Nokia: The road to quantum-safe networks

[6] ETSI, Migration strategies and recommendations to Quantum Safe schemes, 2020.

Url: TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes

[7] TNO, Manon de Vries, Sven Bootsma, Vincent Dunning, and Marc van Vliet, Quantum risicomethodologie, 2024. Url: Quantum risicomethodologie voor cryptografie

[8] Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography; Url: Recommendation 2014 1101 Roadmap

[9] Elaine Barker (NIST), Lily Chen (NIST), David Cooper (NIST), Dustin Moody (NIST), Andrew Regenscheid (NIST), Murugiah Souppaya (NIST), William Newhouse (NIST), Russ Housley (Vigil Security), Sean Turner (sn3rd), Considerations for Achieving Cryptographic Agility: Strategies and Practices, 2025. Url: NIST CSWP 39 second public draft, Considerations for Achieving Crypto Agility: Strategies and Practices

Bernardo Herman
Member of the Council

Peggy Valcke
Member of the Council

Stefaan Vyverman
Member of the Council

Michel Van Bellinghen
Chairman of the Council