Telefónica

EU Roadmap on Post-Quantum Cryptography

September 29th, 2025

Introduction

Quantum technologies will offer transformative opportunities, enabling computational breakthroughs, ultra-secure communications and unparalleled measurement precision. However, the development of quantum computing presents a threat, particularly through 'store-now, decrypt-later' strategies that could exploit cryptographic vulnerabilities.

Telefónica welcomes the opportunity to comment on the EU roadmap on Post-Quantum cryptography published in June 2025 and to propose contributions as follow up of the EU Roadmap on PQC.

Feedback on the EU Roadmap for the Transition to Post-Quantum Cryptography

The publication of a roadmap helps raise awareness among companies and governments about potential future risks and encourages them to begin their preparations. The proposal outlines key concepts such as post-quantum cryptography (PQC) solutions, crypto-agility, the risk-based approach, and the need for early preparation for the future. But it should have been consulted with private stakeholders prior to its launch. Conducting the consultation only after the roadmap has already been adopted is not the most effective approach. We trust that, beyond setting objectives, future coordination and dialogue with industry on implementation measures will strengthen their practicality and impact.

The transition proposal must be proactive, fostering the development and deployment of European solutions while promoting technological sovereignty and, in the initial stages, supporting profitability or public funding. This underscores the importance of stronger coordination, long-term policy commitment, and sustained investment.

Statements suggesting that the transition to PQC solutions is already mandated by regulation do not facilitate this path; instead, they create significant uncertainty—particularly regarding the scope of so-called ‘high-risk cases’—at a time when the maturity of these technologies is still insufficient for full-scale deployment. Imposing obligations related to product and service development under frameworks such as the CRA, CSA, or NIS2 would be premature, risking constraints on industrial development and the creation of inefficiencies. As a public good, security must be actively supported and underpinned by adequate funding.

For detailed feedback, please refer to the responses provided in the consultation or in the **Annex**.

Experience & Background of Telefónica in Post-Quantum Cryptography

Telefónica's early engagement in quantum technology positions it at the forefront of preparing for both the security risks and the new opportunities that quantum computing will bring.

Telefónica has established a dedicated Centre of Excellence for quantum technologies. The company is already making strides towards quantum-safe networks by integrating an additional layer of protection through quantum-resistant technologies, combining traditional cryptographic methods with post-quantum cryptography (PQC). Going beyond the lab, Telefónica is also advancing future technologies such as Quantum Key Distribution (QKD), having deployed them operationally within the EuroQCI network, to accelerate their maturity. This effort has been

carried out in close collaboration with leading academic and research institutions, as well as in partnership with top network equipment manufacturers.

Telefónica is also collaborating with third parties. Several use cases were showcased at MWC25, including applications in healthcare, defence, and utilities, as well as broader efforts to build a robust quantum ecosystem. This includes partnerships with quantum computing manufacturers and collaboration with the Provincial Council of Biscay for example.

Telefónica Tech (June 2025) – Strategic preparation for Post Quantum Cryptography | Telefónica (March 2025) - Telefónica opens a dedicated Centre of Excellence for quantum technologies | Telefónica - Quantum-Safe Networks | Telefónica (October 2024) - QKD, cryptographic keys and quantum networks |Telefónica (March 2025) - Telefónica anticipates quantum challenges with an innovative demo at MWC |Telefónica (March 2025) - Telefónica and Vithas test shielding against quantum attacks in two hospitals |Telefónica (March 2025) - partner of Government of Biscay for development of its quantum technology industrial strategy

Abstract / Description of your proposed contribution

While we can contribute across a wide range of the proposed aspects, we have selected some of them for further development

1) **Strategic security bonds for national and European Communications Resilience.** Effective funding is key. We propose a new class of Security Bonds, modeled on the successful framework of European Green Bonds, to drive measurable investments in the security and resilience of public communications infrastructure.
2) **Accelerating Cryptographic Inventory Tools Across Europe.** A secure PQC transition requires clear risk awareness and cryptographic inventories. Standardized tools (e.g., CBOM/SBOM) integrated into IT systems will streamline migration, cut risks, and ensure compliance.
3) **Making Crypto-Agility Achievable in Real-World Systems.** As PQC standards evolve, systems must remain adaptable. Modular design, hybrid algorithms, migration toolkits, and interoperability testing enable crypto-agility, future-proofing Europe's digital infrastructure and ensuring smooth, risk-free transitions.
4) **Deployment guidelines.** Quantum-safe deployment should follow clear principles: workability, compatibility with existing systems, efficiency and flexibility across environments, and defined timelines for gradual transition.
5) **Testbeds for PQC.** Testbeds for PQC will be essential to raise awareness, trial solutions and real-world use cases, foster innovation, and validate scalability, performance, and interoperability, while ensuring that deployments in critical infrastructures remain cost-effective, resilient, and future proof.

---

1) Strategic security bonds for national and European Communications Resilience

The need for funding the quantum transition roadmap—and, more broadly, initiatives to strengthen resilience—is expected to grow. Establishing effective and straightforward funding mechanisms will be crucial.

We propose the creation of a new class of Security Bonds, modeled on the successful framework of European Green Bonds, to drive measurable investments in the security and resilience of public communications infrastructure at both national and EU levels. These Security Bonds would be publicly issued and allocated to operators and providers undertaking strategic projects to enhance the cybersecurity, integrity, and operational continuity of communications networks—such as deploying post-quantum cryptography (PQC), advanced threat mitigation, and secure update capabilities.

The mechanism is simple and effective: upon independent verification of predefined milestones—such as coverage of critical services, implementation of secure update processes, or achievement of resilience benchmarks—participants would receive Security Bonds that are transferable and redeemable for cash, targeted tax offsets, or other financial incentives. This approach ensures that investments are directly tied to strategic, auditable outcomes, providing operators with liquidity and financial certainty even in cases where market returns are limited, or obligations are preventive.

By leveraging the transparency, accountability, and impact measurement frameworks of Green Bonds, Security Bonds would mobilize both private and public capital toward the urgent goal of securing Europe's communication networks. The program would include clear eligibility criteria, independent verification, caps to prevent double funding, and claw-back provisions to guarantee sustained impact. This model aligns incentives, accelerates the adoption of advanced security measures, and ensures fair returns for early adopters, ultimately making Europe's digital infrastructure more resilient, competitive, and future-proof.

2) **Accelerating Cryptographic Inventory Tools Across Europe**

A secure and coordinated transition to post-quantum cryptography (PQC) requires organizations to have a comprehensive understanding of their existing cryptographic assets. Without visibility into where and how encryption is used, which algorithms are in place, and which assets are most at risk from future quantum threats, organizations cannot effectively plan migrations, prioritize upgrades, or comply with evolving regulations. Making cryptographic inventory tools widely available and easy to use is therefore essential.

Cryptographic inventory tools should automatically scan systems, applications, and devices, providing up-to-date, clear, and actionable insights. Key actions include:

- Developing open-source and commercial inventory solutions that integrate seamlessly with existing IT environments.
- Promoting the use of standardized formats (such as CBOM/SBOM) to ensure compatibility and facilitate the sharing of inventory data between organizations and regulators.
- Providing guidance and support for deployment, including templates, best practices, and training materials.
- Encouraging collaboration among public authorities, industry, and research institutions to continuously improve these tools and adapt them to new technologies and emerging threats.

This approach will help organizations gain full visibility of their cryptographic landscape, plan effective migrations to PQC, and mitigate risks associated with outdated or vulnerable encryption, thereby enhancing Europe's overall security and resilience.

3) **Making Crypto-Agility Achievable in Real-World Systems**

Crypto-agility—the ability to quickly and safely update security mechanisms as new threats or standards emerge—is essential, in particular given the current immaturity of quantum-safe solutions. Since post-quantum cryptography (PQC) standards, interoperability, and vendor implementations are still evolving, systems must be designed to adapt without major disruptions. Building crypto-agility now ensures that organizations are not locked into fragile or outdated approaches and can transition smoothly as technologies mature.

Key actions include:

- Establishing clear guidelines for modular security architectures, where cryptographic components are separated from business logic and can be replaced independently.
- Requiring that new products and services support multiple encryption algorithms, including hybrid modes that combine traditional and post-quantum methods.
- Supporting the development of migration toolkits and automated update mechanisms, so organizations can deploy new cryptographic standards quickly and securely.
- Facilitating interoperability testing and pilot projects at national and European levels to validate crypto-agile solutions in diverse environments before large-scale deployment.

By prioritizing crypto-agility, Europe can future-proof its digital infrastructure, enabling rapid and reliable adaptation to evolving security challenges while mitigating the risks of premature or fragmented PQC adoption.

4) **Deployment guidelines**

Deployment of quantum-safe solutions should be guided by clear principles to ensure smooth adoption: they must be compatible with existing systems, efficient and flexible across diverse environments, and include defined transition timelines that allow progressive adaptation. In addition, systematic risk and cost analyses are essential to guarantee that adoption is proportionate, sustainable, and aligned with both security needs and market realities.

We should ensure that such deployment guidelines are workable, interoperable and aligned with real-world operational constraints by sharing sector experience providing empirical input from pilots and early deployments of PQC algorithms, highlighting performance and interoperability challenges and mapping risk and priority areas where PQC transition is urgent (long-lived data, critical control systems) versus those suited to phased migration. In addition, they should:

- Contribute to reference architectures
- Propose sector-specific minimum guidelines, as which algorithms, key sizes, hybrid schemes, etc.
- Identify dependencies with legacy systems and propose migration pathways that avoid service disruption

5) **Testbeds for PQC**

Testbeds for PQC will be essential to raise awareness, trial solutions and real-world use cases, foster innovation, and validate scalability, performance, and interoperability, while ensuring that deployments in critical infrastructures remain cost-effective, resilient, and future proof. Defining a clear and supportive framework to promote, coordinate, fund and scale testbeds will be critical to maximise their impact.

The technical aim of such testbeds, should be provide support and information on:

- **Performance validation**: measuring latency, throughput and scalability of PQC algorithms in real workloads such as VPNs, TLS/IPSec tunnels and telecom signaling
- **Interoperability checks:** ensuring smooth integration between legacy algorithms, hybrid schemes, and PQC implementations across different vendor's equipment
- **Deployment scenarios:** simulating migration in critical use cases and identifying potential service disruptions.
- **Feedback loop:** providing the EU Commission with concrete evidence of what works, what fails and where additional guidance is needed
- **Cross-sector collaboration:** enabling joint testbeds with operators, vendors and research bodies to align practices across industries

ANNEX- Feedback on the EU Roadmap for the Transition to Post-Quantum Cryptography

What are the most useful parts of the roadmap?

The publication of a roadmap (or more precisely a set of objectives) helps raise awareness among companies and governments about potential future risks and encourages them to begin their preparations. The proposal outlines key concepts such as post-quantum cryptography (PQC) solutions, crypto-agility, the risk-based approach, and the need for early preparation for the future. But it should have been consulted with private stakeholders prior to its launch. Conducting the consultation only after the roadmap has already been adopted is not the most effective approach. We trust that, beyond setting objectives, future coordination and dialogue with industry on implementation measures will strengthen their practicality and impact.

The clear intended timeline (2026/2030/2035) and the structure of First/Next Steps approach are valuable for raising awareness, guiding future investments and aligning support with measurable milestones. However, this calendar and what is considered first, or next step may need to be revisited in particular depending on the maturity of the solutions, the progress of standardization, implementation costs, the public resources allocation and developments in quantum computing technology.

The recommendation to use hybrid approaches (including symmetric solutions depending on the use cases), a risk-based approach for the PQC transition and to promote crypto-agility in security solutions will help reduce implementation risks.

Pilot projects and testbeds will allow validation of maturity before scaling up, making it easier to introduce incentives and compensation linked to results, which is essential for efficient deployment in different sectors.

The allocation of public resources will be crucial not only for supporting the transition, but also for high-risk use cases, public procurement, and testbeds. Such resources should not be limited to the 'Next Steps' phase alone. A risk-based and cost-based approach, closely aligned with market demand, will be essential.

The need for transition planning is critical—including for complex systems such as PKIs—but its effectiveness will depend on the availability of existing solutions, the maturity of the technology (e.g., even RSA, despite being available for over 30 years, has required updates; while PQC still faces challenges such as limited interoperability, evolving standards, gaps in vendor availability, and the absence of certifications), as well as the resources available.

The need for transition planning is important (including complex systema such as PKIs), but planning well ahead for deployment or implementation is challenging at present, as it will depend on the availability of existing solutions, resources allocation and the maturity of the technology which could lead to implementation risks (e.g., even RSA, despite being available for more than 30 years, has required updates; and PQC still faces challenges such as limited interoperability, evolving standards, vendor limitations, and lack of certifications). Testbeds, pilots, and targeted use cases will be essential to support this process.

What areas of the roadmap need improvement or clarification?

In addition to the earlier comments on the need for coordination with private stakeholders, as well as on reviewing the planning process, the inclusion of elements in the First/Next Steps, and the allocation of resources, please find attached further comments.

The transition proposal must be proactive, fostering the development and deployment of European solutions while promoting technological sovereignty and, in the initial stages, supporting profitability or public funding. This underscores the importance of stronger coordination, long-term policy commitment, and sustained investment.

Statements suggesting that the transition to PQC solutions is already mandated by regulation do not facilitate this path; instead, they create significant uncertainty—particularly regarding the scope of so-called 'high-risk cases'—at a time when the maturity of these technologies is still insufficient for full-scale deployment. Imposing obligations related to product and service development under frameworks such as the CRA, CSA, or NIS2 would be premature, risking constraints on industrial development and the creation of inefficiencies. As a public good, security must be actively supported and underpinned by adequate funding.

Additionally:

1. Risk of Early Adoption and Compensation. The roadmap should explicitly acknowledge that adopting new security technologies at an early stage entails significant risks for companies. It is essential that those leading the transition receive appropriate support and compensation—whether through grants, tax incentives, or mechanisms that mitigate the financial impact of potential errors or the limited maturity of solutions.

2. Profitability and Preventive Obligations. If companies are required to implement preventive measures (e.g., strengthening security before maturity), it must be ensured that these investments are profitable (demand driven), or that fair compensation is provided when profitability is not achievable. This is particularly relevant in areas or services where revenues do not cover the costs of modernization.

3. Results-Oriented Funding. European support and funding should be tied to clear, measurable outcomes, such as deployment milestones, improvements in security, or expanded service coverage. This approach ensures that public investment generates tangible impact and allows companies to plan with greater certainty.

4. Support for Resilience and Modernisation. Investments in technological modernization and resilience—such as enhancing network security, preparing for incidents, or strengthening energy sustainability—should be recognized as eligible expenses and receive dedicated support.

Do you have any other comments or suggestions for improvement?

As noted earlier, coordination with the private sector will be essential, aiming to establish a European industrial baseline, promote a proactive rather than obligation-driven approach, support the development of European standards, secure appropriate funding mechanisms, and apply risk-based and cost-based analyses. In addition to the previous comments:

- **Public Sector as Adoption Leader:** The public sector should act as a driver of adoption, leading the way before expecting any non-market-driven adjustments from the private sector. It is essential for the public sector to lead through pilot projects and the dissemination of best practices, providing tools and models that can be replicated by the private sector.
- **Fairness and Sustainability, adopting public funding:** To ensure that the transition to new security technologies is fair and sustainable, we recommend establishing flexible financing instruments—such as dedicated funds or European bonds—enabling companies to manage modernization costs without compromising competitiveness.
- **Public-Private Collaboration:** Continuous dialogue between administrations and companies, both prior to and during implementation, is key to ensuring that obligations and objectives are realistic and achievable. This will provide a comprehensive understanding of the roadmap's feasibility and the most effective paths forward (e.g., the need for cryptographic inventory tools, funding, and other critical enablers).
- **Strategic Priorities:** The security and resilience of telecommunications and critical infrastructures should be an explicit priority in the roadmap, as they are fundamental for Europe's autonomy and competitiveness, while supported by flexibility and funding.