EUROSMART
The Voice of the Digital Security Industry

Europe's Competitive Edge: Leading the Charge in Post-Quantum Cryptography

The emergence of quantum technologies offers tremendous potential for scientific advancements, but it also poses a significant threat to global information infrastructure. Public-key cryptography, which is widely used today, relies on mathematical problems that are currently considered difficult to solve with existing and foreseeable computational power. However, well-known cryptographic methods—such as RSA and Elliptic Curve Cryptography— will be easily compromised by emerging quantum computing.

Quantum computing could swiftly render current security systems obsolete, significantly impacting the digital security industry, whose business model is built on keeping information and data secure. Efforts should be focused on deploying algorithms that are resistant to quantum computing attacks. Major national security agencies agree on the urgency of migrating to post-quantum cryptography: **mitigation plans must start now.**

> ***"ANSSI recommends introducing post-quantum defense-in-depth as soon as possible for security products aimed at offering a long-lasting protection of information (until after 2030) or that will potentially be used after 2030 without updates."*** [1]

> ***"From the BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer paramount. First post-quantum algorithms have been selected by NIST for standardisation and post-quantum cryptography will be used by default. Therefore, the migration to post-quantum cryptography should be pushed forward."*** [2]

[1] ANSSI views on the Post-Quantum Cryptography transition, ANSSI, 4th Janyary 2022 - https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

[2] Quantum Technologies and Quantum-Safe Cryptography, BSI, December 2021 - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html

> ***"A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors."*** [3]

What a mitigation plan is about

A mitigation plan consists of three main stages:

Each of this stage takes time to be conducted and would strongly benefit from a suitable methodology and automatic tooling.

Risk analysis should be sector-specific, considering the unique threats and constraints of each sector. This sector-specific risk analysis—whether based on use cases or industry verticals—should lead to the development and implementation of a migration and mitigation plan, which shall include a detailed strategy and timeline.

In parallel to a mitigation plan, implementing Crypto Agility must be meticulously implemented in any new project. Cryptographic agility refers to the ability to switch between multiple cryptographic primitives. This practice is well-known and considered good cyber hygiene when using cryptographic protocols. As explained by ENISA, the migration to post-quantum cryptography makes this capability even more crucial:

> ***"Carefully designed protocols will exhibit algorithm agility and secure version negotiation to support future development (but not at the expense of simplicity). Thus, lock in of cryptographic protocols and schemes for many years should be avoided. It should be relatively easy to upgrade cryptographic components, by designing protocols in a modular manner. Enabling components which are no longer deemed secure to be swapped out."*** [4]

[3] Quantum-Readiness: Migration to Post-Quantum Cryptography, NIST, 21st August 2023 - https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

[4] ENISA Study on Cryptographic Protocols, November 1014 https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols/%40%40download/fullReport

Post-Quantum Cryptography as a competitive advantage

As the global quantum computing landscape evolves, many worldwide initiatives are being undertaken to transition toward post-quantum cryptography. This results in positioning organisations at a competitive advantage by staying ahead of emerging threats

On December 21, 2022, President Biden signed into law the Quantum Computing Cybersecurity Preparedness Act, "To encourage the migration of Federal Government information technology systems to quantum-resistant cryptography." [5]

As a domino effect, several open-sources projects have pop-up and the launch of the Post-Quantum Cryptography Alliance (pqca.org) by the Linux Foundation as "an open and collaborative initiative to drive the advancement and adoption of post-quantum cryptography" is just an illustrative example.

In this context, it is likely that US public and private organizations undertake their migration ahead of their European counterparts. For suppliers, being post-Quantum ready will become a competitive advantage, not to say about the design of new cryptographic protocols that might mainly involve experts from US companies.

The US National Security Agency (NSA) announced the Commercial National Security Algorithm Suite (CNSA) 2.0, mandating Post Quantum cryptography for software and firmware updates. The transition to Post Quantum cryptography (NIST 800-208) should be started immediately with a preference to use CNSA 2.0 by 2025 and exclusive use of PQC algorithms for software and firmware updates by 2030.

The UK National Cyber Security Centre (NCSC) published a white paper highlighting the importance and implications of PQC migrating for system owners. The paper mentions several options for PQC algorithms, including NIST 800-208 for software and firmware digital signing.

Europe must stay in the race

The European Commission published on 11th April 2024 a Recommendation on Post-Quantum Cryptography [6], to encourage Member States to develop and implement a harmonised approach as the EU transitions to post-quantum cryptography. For this purpose, the Commission recommends the Member States to establish a sub-group of the NIS Cooperation group and to develop a Coordinated Implementation Roadmap addressing the transition to post-quantum cryptography within 2 years.

However, the EU's outlined schedule lacks specificity, which could leave Europe vulnerable to emerging quantum threats. To mitigate this risk, it is crucial for the European Commission to set clear deadlines, similar to the NSA's efforts and timetable for implementing CNSA 2.0. The NSA

[5] Quantum Computing Cybersecurity Preparedness Act, US Congress, 21st December 2022 - Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress

[6] Commission Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography C(2024) 2393, European Commission, 11th April 2024, https://ec.europa.eu/newsroom/dae/redirection/document/104249

communication provides detailed timelines for various technologies and components, such as software and firmware signing, web browsers/servers, cloud services, and traditional networking equipment. The European Commission should propose similar schedules, particularly for technologies critical to European industries, such as IoT, digital identity, and identity documents. By doing so, Europe can ensure a structured and secure transition to quantum-safe cryptography, tailored to the EU's technological landscape.

The development of such EU's coordinated implementation should involve relevant stakeholders, in this respect Eurosmart recommend to closely collaborate with the industry to facilitate the quick technical implementation.

Following the European Commission Communication on PQC, Eurosmart calls on the policy maker to implement concrete actions:

1. **The European Commission should mandate European institutions and agencies to undertake their mitigation plans, similar to the obligations placed on agencies and administrations in the United States.**

2. **The Commission should support and promote initiatives by European Standardisation Organisations (ESOs) to integrate post-quantum cryptography (PQC), as typically standardised by NIST, into their cryptographic protocols within a specified timeframe.**

3. **The Commission should setup dedicated PQC pilot projects in order to improve the readiness of key infrastructures and services to the major upcoming changes.**

4. **Eurosmart encourages the Commission to swiftly activate various expert groups that could provide valuable input on this matter, such as the High-Level Forum on Standardisation and the Multi-Stakeholder Platform on ICT Standardization. These groups can pave the way for further political and technical actions.**

5. **ENISA should play a crucial role by releasing guidelines to support organizations in implementing their mitigation plans and considering PQC guidelines of Cybersecurity Agencies in other countries (such as NIST and NCSC).**

6. **Finally, the Commission should enhance and maximise the influence of various EU actors in global forums and consortia that define cryptographic protocols.**

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com