EUROPOL

Quantum Safe Financial Forum

A CALL TO ACTION

Audience of this paper

The financial and payment industries and their Chief Information Security Officers (CISOs), policymakers, and society in general.

About the QSFF

In 2024, some members of the European Cybercrime Centre (EC3)'s Advisory Group on Financial Services proposed the creation of the QSFF to Europol. The Advisory Group's programme, created in 2013 by EC3, is a space for law enforcement and the private sector to discuss the latest cybercrime threats, as well as current and future challenges.

The QSFF is a multi-stakeholder effort, supported by Europol, to address the transition to PQC across the financial sector, with a particular focus in Europe. The QSFF is composed of experts from several major EU, UK and American commercial and central banks, other financial services providers, associations, and experts.

The aim of the QSFF is to share best practices and coordinate actions to address a safe transition to PQC. The QSFF is a safe space where its selected members can collaborate and help each other through this transition, fostering developments and addressing upcoming threats.

Find more information on the QSFF and become a member at Europol's website.
www.europol.europa.eu

EXECUTIVE SUMMARY

Modern cryptography is fundamental to securing the financial ecosystem. The emergence of quantum computers capable of breaking current cryptographic methods presents a challenge to the entire financial ecosystem. Addressing this challenge requires a transition to post-quantum cryptography (PQC). This transition also presents an opportunity to enhance cryptography management practices. Achieving this complex goal requires immediate action and a coordinated effort involving industry peers, vendors, policymakers, and society. The Quantum Safe Financial Forum (QSFF) is committed to supporting companies and policymakers in the transition to a quantum-safe financial sector.

The Quantum Safe Financial Forum recognises the growing global awareness of the quantum threat. However, without a common approach, the financial industry could face increased complexity and costs.

QSFF recommendations:

1. Financial institutions and policymakers should prioritise the transition to quantum-safe cryptography and actively support its implementation.

2. Coordination among different stakeholders will be key; ensuring alignment on their planning, roadmaps and the concrete implementation of the transition to PQC, establishing common goals and a shared view of the requirements to achieve them.

3. There is no need for additional legislation to be made; a voluntary framework established between regulators and the private sector would be sufficient to set guidelines for quantum-safe cryptography and promoting standardisation across institutions.

4. This transition presents an opportunity to enhance cryptography management practices. A forward-looking framework to cryptography management is needed.

5. Promoting collaboration, knowledge sharing and fostering a cohesive approach across jurisdictions at global scale is key to a secure transition. This means encouraging the industry — including the private and public sector actors — to partner up in the context of quantum-safe experiments, projects, Points of Contact (POCs) and any other relevant initiatives.

INTRODUCTION: THE THREAT QUANTUM COMPUTERS POSE TO CRYPTOGRAPHY

The development of the information society has been made possible due to the widespread use of cryptographic techniques, which ensure authentication, integrity, and confidentiality in digital communications and processes. The financial industry relies heavily on cryptography to provide secure services to customers and society.

Quantum computers, while offering exciting opportunities to solve complex problems, also pose significant challenges. A sufficiently advanced quantum computer could break current public key cryptographic algorithms, compromising the confidentiality of internet communications and the integrity of digital contracts.

These challenges have been identified by Europol and presented in the First Report on Encryption[1], published by the EU Innovation Hub, and The Second Quantum Revolution[2] report, published by Europol's Innovation Lab. Even though these reports focus on the law enforcement perspective, there are synergies that can also be applied to the financial industry.

For the financial industry, the advent of quantum computers poses a risk to customer confidentiality and peer communications, authentication processes, and trust in digital signatures which enable dynamic legal agreements. Quantum computers capable of posing such threats are expected to be available within the next 10 to 15 years, though this timeline could accelerate due to intense interest from both the public and private sectors[3].

WHERE IS THE FINANCIAL SECTOR TODAY?

The financial sector has started to work on this challenge. Conversations and information have been flowing in many forums, such as CFDIR[4], FS-ISAC[5], ETSI/IQC[6], EPA[7], as well as within the QSFF. Private firms within the financial sector have started preparing to update their use of cryptography. Some companies have started cryptography inventory efforts or are planning to do so, but not all have embarked on this journey yet.

A 2023 survey[8] conducted among 200 leaders in data, analytics, and innovation within the financial sector, indicates a significant lack of readiness for the next wave of cryptography. The survey showed that post-quantum cybersecurity specifically will be the biggest issue, with 86% of organisations acknowledging their unpreparedness. Additionally, 84% of the respondents anticipate the need to adopt post-quantum cybersecurity measures within the next two to five years.

1 First Report on Encryption https://www.europol.europa.eu/publications-events/publications/first-report-encryption, 2024, 31/01/2025

2 The Second Quantum Revolution https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement, 2024, 31/01/2025

3 See Global Risk Institute report https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/, 2023, 31/01/2025

4 https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-forum-digital-infrastructure-resilience-cfdir ,31/01/2025

5 https://www.fsisac.com/knowledge/pqc ,31/01/2025

6 https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event, 31/01/2025

7 EPA Asia https://emergingpaymentsasia.org/wp-content/uploads/2024/04/25-April-EPAA-Press-Release-WG-QSC.pdf 2024, 31/01/2025

8 https://www.moodys.com/web/en/us/about/what-we-do/quantum-computing/quantum-survey-report.html 31/01/2025

THE TIMELINE: FROM TODAY TO THE MID-2030'S

The US National Institute of Standards and Technology (NIST) has steered the standardisation of PQC, replacing cryptographic algorithms which are believed to be resistant to quantum computers, with the first standards published in 2024.

The critical path for any organisation to accomplish this transition is defined by Mosca's theorem[9], and guided by two factors:

1. **Shelf-life time** (number of years the data must remain secure): The financial sector is often required to maintain confidential data or signed contracts for several years.

2. **Migration time** (number of years it will take to securely upgrade the systems guarding the data). Transitioning to PQC and retiring obsolete cryptography is a complex task that could take decades, as seen with algorithms and protocols like 3DES[10], SHA1[11] or versions of TLS prior to 1.3[12], which remain in use despite newer standards have been available.

The sum of these two times would mark the end of the transition, which must be completed before the risk materialises. The US administration has set 2035[13] as the deadline for Federal Agencies to achieve quantum resistance.

When discussing timelines, it is important to mention the threat of "store now, decrypt later" (or harvest now, decrypt later), in which criminals collect data today, with the intention to decrypt it in the future when quantum computers are available. Sensitive information such as merger and acquisition plans, trade secrets, or long-term investment strategies require confidentiality for extended periods. If any of this information is intercepted and stored by malicious actors today, it could be decrypted in the future, potentially causing significant financial losses and reputational damage.

9 https://uwaterloo.ca/institute-for-quantum-computing/profiles/michele-mosca, 2025, 31/01/2025

10 ANSI X9.52-1998: Triple Data Encryption Algorithm Modes of Operation, American National Standards Institute, July 30, 1998, 31/01/2025

11 Secure Hash Standard (SHS), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, April 8, 1995, 31/01/2025

12 The Transport Layer Security (TLS) Protocol Version 1.3, https://www.rfc-editor.org/rfc/rfc8446, August 2018, 31/01/2025

13 https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF 2024, 31/01/2025

THE CHALLENGE: MAKING THE TRANSITION A GLOBAL PRIORITY

Cybersecurity is paramount for the financial sector. Ransomware attacks, data leaks, and AI pose new challenges, requiring immediate attention and resources. Simultaneously, the financial sector is adopting standards such as DORA[14] and NIS2[15]. Amidst these priorities, managing the quantum transition may seem like something that can be postponed, leading to so called crypto-procrastination, but it is essential to integrate it into current roadmaps.

Cryptography secures communications within and between organisations. However, due to the need for backwards compatibility with outdated software, systems and configurations, the use of obsolete cryptographic methods is often extended. No single financial organisation can complete the transition to quantum-safe cryptography on its own. They are interdependent on the financial ecosystem and vice versa - this may delay the complete decommission of vulnerable cryptography.

The primary risks to the global transition to quantum-safe cryptography are twofold; underestimating the project's complexity, and assuming it can be accomplished independently. Success hinges on collaboration among organisations, vendors, policymakers, and society at large to tackle the transition in a committed and coordinated manner.

The Quantum Safe Financial Forum recognises the growing global awareness of the quantum threat. However, without a common approach, the financial industry could face increased complexity and costs.

14 Digital Operations Resilience Act https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554, 2022, 31/01/2025

15 NIS2 Directive, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1738337361289, 2022, 31/01/2025

Public institutions have already started to address this transition:

- In Europe: The Digital Operational Resilience Act (DORA regulation) establishes requirements to improve cryptography management in the financial sector. It entered into force on 16 January 2023. The European Commission released a recommendation on a "Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography"[16], which encourages EU member states to coordinate efforts among relevant stakeholders, public and private, including Europol.
- In the UK: The Financial Conduct Authority (FCA) in collaboration with the World Economic Forum (WEF) produced the report "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches"[17], building on views from regulators, central banks, industry players and academia. The report identifies four guiding principles along with a roadmap to serve as a blueprint to reduce complexity and align stakeholders' activities and calls for an open dialogue between regulatory authorities and industry.
- In the USA: the White House has published the "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"[18].
- In Singapore: The Monetary Authority of Singapore (MAS) has issued an advisory to financial institutions urging them to implement quantum security[19].

16 https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography, 2024, 31/01/2025

17 https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/, 2024, 31/01/2025

18 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, 2022, 31/01/2025

19 https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf, 2024, 31/01/2025

QSFF RECOMMENDATIONS: A ROADMAP TO A QUANTUM-SAFE FINANCIAL SECTOR

1. **Financial institutions and policymakers should prioritise the transition to quantum-safe cryptography and actively support its implementation. The complexity of the transition project should not be underestimated. Firms should establish and initiate their transition plans by:**

- raising awareness on the need to update how cryptography is managed;
- upskilling IT teams to understand cryptography and its associated new challenges;
- dedicating resources to manage the transition, with support from top management.

2. **Coordination among different stakeholders will be key; ensuring alignment on roadmaps and concrete implementation, establishing common goals and a shared view of the requirements to achieve them.**

- A successful transition requires collaboration among organisations, vendors, and policymakers, to develop coordinated transition roadmaps. Law enforcement, as a sector, needs to balance the short, medium and long-term implications of the quantum threat, ensuring a coordinated transition across the financial sector, identifying dependencies and critical paths, or key providers.
- The transition also requires enhanced knowledge-sharing between financial institutions, allowing a unified approach to managing any risks associated with quantum threats.

3. **There is no need for additional legislation to be made, a voluntary framework established between regulators and the private sector would be sufficient, by setting guidelines for quantum-safe cryptography and promoting standardisation across institutions.**

- The existing regulatory framework on operational resilience and cyber risks, including DORA and GDPR, is sufficient to manage the quantum threat, aligning quantum-safe cryptography with existing regulations without adding regulatory burden.
- Regulators, working with the private sector, could help by providing clear guidance that would ensure consistent cryptography management practices in the sector, like common practices or standards.
- Additionally, regulators should recommend the use of hybrid cryptography, which combines classical and post-quantum algorithms, to facilitate a gradual transition while maintaining existing security guarantees. Financial services firms are starting to adopt and migrate to the recent NIST FIPS publications, and standardising that across the financial ecosystem would reinforce this direction.

4. **This transition presents an opportunity to enhance cryptography management practices. A forward-looking framework to cryptography management is needed. It is recommended that financial institutions:**

- Integrate cryptography management into general IT asset management;
- Maintain an inventory of cryptographic assets as part of the IT asset inventory;
- Implement checks to ensure compliance with applicable policies;
- Develop contingency and exit plans to achieve crypto-agility.

5. **Promote collaboration, knowledge sharing and fostering a cohesive approach across jurisdictions at global scale. This means encouraging the industry, including private and public sector actors, to partner up in the context of quantum-safe experiments, projects, Points of Contact (POCs) and other initiatives.**

The QSFF is committed to supporting the transition to a quantum-safe financial sector. It seeks to empower the ecosystem to meet the challenge and ensure the seamless preparation of the next wave of cryptographic transitions.

EUROPOL

QUANTUM SAFE FINANCIAL FORUM – A CALL TO ACTION

PDF | ISBN 978-92-95236-98-1 | doi:10.2813/5052685 | QL-01-25-004-EN-N

Luxembourg: Publications Office of the European Union, 2025

The present position paper has been produced by QSFF. The opinions expressed in this paper are a consensus reached by the QSFF as a collective and do not necessarily reflect the individual position of each member. As such, this paper may not be considered exclusively as a work product of either Europol or Europol's European Cybercrime Centre (EC3), which currently hosts the Secretariat of QSFF.

Cite this publication: Europol (2025), Quantum Safe Financial Forum – A Call to Action, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu