Post Quantum Cryptography Transition Best Practice Recommendations

Version: October 2025

Background

JPMorgan Chase & Co. (“JPMC”) is providing this document pursuant to the Department of Homeland Security (DHS) and the Department of Commerce’s National Institute of Standards and Technology (NIST) roadmap to help organizations protect their data and systems and to reduce risks related to the advancement of quantum computing technology. This document serves as a resource to support JPMC supplier organizations to transition to Post Quantum Cryptography (PQC), emphasizing alignment with recognized standards and practices. It outlines expectations for collaborative efforts to integrate quantum-safe cryptographic practices into operations, while maintaining alignment with JPMC to protect our data, information, networks and systems.

This guidance is intended to assist suppliers to prepare for the transition to PQC and does not replace or override any existing cryptographic procedures within a supplier’s organization. Specific actions should be tailored to each organization's unique circumstances, including size, scope, and impact.

Supplier Alignment with PQC Strategy

Suppliers should establish a comprehensive approach to align their cryptographic practices with recognized and evolving quantum-safe standards. This approach includes ensuring teams are well-versed in quantum-safe practices and actively engaging with JPMC to maintain alignment.

As outlined in JPMC's Minimum Control Requirements, suppliers are expected to protect our Highly Confidential and Confidential Information using industry-standard cryptography and manage cryptographic keys throughout their lifecycle. With the advent of quantum computing, practices must be reassessed to ensure adoption of quantum-safe methods that keep pace with industry advancements.

Key Expectations

- Align cryptographic practices and migration timelines with recognized quantum-safe standards to support the transition to quantum-safe methods.
- Align with industry and regulatory standards for PQC to maintain consistency with best practices.
- Engage actively with JPMC, participating in discussions and information sessions where applicable.
- Educate teams about quantum-safe standards and prepare them for the PQC transition.

Preparing for the PQC Transition

Suppliers should take proactive steps for a successful transition to quantum-safe cryptography. This involves assessing and updating cryptographic practices to align with recognized standards.

For further guidance and direction, suppliers can refer to established timelines and directives from the below recognized authorities:

- **Bank for International Settlements (BIS)**: This strategic framework supports the financial system's transition to quantum-safe cryptographic infrastructures. It emphasizes cryptographic agility, defense-in-depth, and coordinated planning to ensure the resilience of the global financial system against quantum threats. Link: Quantum-readiness for the Financial System: a Roadmap
- **Cyber Coordination Group (CMORG)**: This guidance is tailored for the UK financial sector, offering insights into adopting quantum-safe cryptographic practices. It highlights the urgency of the transition and provides a roadmap for financial institutions to assess vendor readiness and develop migration strategies in alignment with national cybersecurity standards. Link: Guidance for Post-Quantum Cryptography
- **European Union (EU)**: This roadmap details the transition to post-quantum cryptography across the European Union, emphasizing coordinated efforts and cryptographic agility. It outlines a timeline for Member States to initiate and complete the transition, ensuring cybersecurity resilience against emerging quantum threats. Link: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Communication and Collaboration

Effective communication and collaboration between suppliers and JPMC is crucial during the transition to quantum-safe cryptography. Suppliers are encouraged to engage openly and proactively to ensure alignment with JPMC.

Suppliers should establish a formal internal communication procedure, so their teams are familiar with their roles and responsibilities in the PQC transition. A dedicated team of subject matter experts and senior management with the authority and responsibility to communicate with JPMC is essential for timely dissemination of information. Expectations for supplier collaboration include:

- Remain attentive to communications from JPMC regarding PQC updates and initiatives.
- Participate in discussions and meetings, when requested, to achieve alignment and shared understanding.
- Share information openly and provide updates on progress in planning and implementing PQC.
- Proactively seek clarification, ask questions, and raise concerns to JPMC to support a successful and coordinated implementation of PQC.

Resources and Support

Suppliers should leverage resources provided by JPMC to achieve alignment with quantum-safe cryptographic standards. Additionally, regular communication and collaboration with your JPMC relationship contact are essential for understanding timelines and plans, as well as sharing your own strategies to maintain alignment. Continuous dialogue and coordination will help facilitate a smooth transition to quantum-safe cryptography.

Technical Details

As outlined in NIST's IR 8547 initial public draft[1], the expectation is to prioritize the migration to quantum-resistant key-establishment schemes as an initial phase (aka, confidentiality phase). Authentication use cases (which include X.509 certificates etc.) can transition on a different timeline. This is reflected in the tables below which summarize some of the technical details the industry is converging on.

For TLS 1.3, the table below lists named groups that support both prioritized quantum-resistant and classic algorithms. To maximize security, we recommend configuration of the named groups in the order shown in the table.

TLS 1.3 Named Groups (supported_groups extension) (descending order of preference – preferred group is at the top)	**Hex Code**
X25519MLKEM768	{0x11EC}
SecP256r1MLKEM768	{0x11EB}
SecP384r1MLKEM1024	{0x11ED}
x25519	{0x001D}
secp256r1	{0x0017}
x448	{0x001E}
secp384r1	{0x0018}

While TLS 1.3 is required for quantum-resistant cryptography, we also recommend that support is maintained for TLS 1.2 to ensure backward compatibility where needed. The table below provides details on the overall configuration (to be used in combination with the above table).

Cipher Suite (descending order of preference – preferred cipher suite is at the top)	**Hex Code**
TLS 1.3 Cipher Suites	
TLS_AES_256_GCM_SHA384	{0x13,0x02}
TLS_AES_128_GCM_SHA256	{0x13,0x01}
TLS_CHACHA20_POLY1305_SHA256	{0x13,0x03}
TLS 1.2 Cipher Suites	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2F}
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{0xC0,0x30}
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2B}
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{0xC0,0x2C}

[1] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

Timeline

For guidance, key dates for quantum-readiness have been provided by the US National Security Agency[2].

Important Disclaimer

This document is provided for informational purposes only to support JPMC suppliers' alignment with emerging industry-recognized post-quantum cryptography transition practices. This information is being provided on an "AS IS" basis and JPMC disclaims any and all liability. This document does not amend or supersede your contractual requirements with JPMC.

[2] https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF