Post-Quantum Use In Protocols
Internet-Draft
Intended status: Informational
Expires: 21 January 2026

K. Kwiatkowski
20 July 2025

Guidance for migration to Post-Quantum Cryptography
draft-kwiatkowski-pquip-pqc-migration-00

Abstract

This document provides guidance on migration to post-quantum cryptography (PQC) in internet protocols. It outlines the challenges and considerations that protocol designers and implementers should take into account when transitioning from traditional cryptographic algorithms to PQC algorithms, which are designed to be secure against quantum computer attacks.

It is intended for cryptographic protocol designers within the IETF community, as well as technology developers and implementers responsible for deploying PQC standards.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-kwiatkowski-pquip-pqc-migration/.

Discussion of this document takes place on the Post-Quantum Use In Protocols Working Group mailing list (mailto:pquip@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/pqc/. Subscribe at https://www.ietf.org/mailman/listinfo/pquip/.

Source for this draft and an issue tracker can be found at https://github.com/kriskwiatkowski/draft-kwiatkowski-pqc-migration.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Advances in quantum computing pose a growing threat to systems that rely on widely deployed internet security protocols, which use cryptographic mechanisms to secure communications, verify authenticity, and protect sensitive data at rest and in transit. While a cryptographically relevant quantum computer (CRQC) capable of breaking these protections may still be years away, initiating the transition to post-quantum cryptography (PQC) now is essential to

ensure adequate time for planning and implementation.

2. Awareness

Before embarking on the transition to post-quantum cryptography (PQC), organizations must first evaluate whether to begin the migration immediately or adopt a phased timeline. This decision depends on factors such as the duration required for migration, the expected shelf-life of sensitive data, and the projected timeline for quantum threats. Data with long-term confidentiality requirements may increase the urgency, as adversaries could collect encrypted information today and decrypt it in the future using a cryptographically relevant quantum computer (CRQC). Even in the absence of a direct harvest-now-decrypt-later threat, organizations must still prepare to protect data integrity and authenticity against future quantum-enabled attacks.

To guide this process, organizations should clearly define their PQC migration objectives, starting with an assessment of their risk tolerance - how much risk they are willing to accept in safeguarding data and assets. This assessment will shape the choice of PQC algorithms, protocols, and implementation paths. It’s important to recognize that PQC migration is not a one-off upgrade but a continuous effort that requires ongoing threat monitoring, periodic reassessments, and adaptability as quantum technology evolves.

3. Key exchange

Key exchange is a fundamental component of security protocols that allows two entities to securely exchange keys over an insecure channel to derive symmetric session keys.

The development of cryptanalytically relevant quantum computers (CRQCs) threatens current systems, necessitating a migration to post-quantum cryptography (PQC). A key concern driving this migration, particularly for key exchange, is the "harvest-now-decrypt-later" threat. Adversaries may collect and store sensitive data encrypted with keys established using quantum-vulnerable methods today, with the intention of decrypting it later once CRQCs are available. This threat specifically impacts the confidentiality of communications, which is protected by keys derived during the key exchange process.

PQ/T hybrid KEMs are widely recommended because resilience that they offer: even if one of the underlying algorithms is broken (e.g., the traditional or post-quantum scheme), the confidentiality of the session remains protected as long as the other holds. This property is essential in practice, since encrypted data captured today could be decrypted in the future if a single algorithm fails. Migrating

from PQ/T hybrid to post-quantum KEMs has lower cost comparing to digital signatures, as in most cases KEMs are ephemeral and used only during session setup, without long-term identity ties. In contrast, signatures involve persistent keys, certificates, and complex trust infrastructure, making their transition more disruptive.

The expectation is that importance of PQ/T hybrid KEMs will diminish in time as confidence in post-quantum algorithms grows.

4. Digital signatures

Digital signatures remain a vital component of cryptographic protocols, ensuring authenticity, integrity, and non-repudiation. As such, post-quantum digital signature schemes are necessary in a future-proof internet infrastructure. However, the urgency to deploy them is relatively lower compared to key encapsulation mechanisms (KEMs).

Unlike key exchange, authentication cannot be broken retrospectively, meaning quantum-safe signatures are only needed once cryptanalytically relevant quantum computers (CRQCs) become available. As a result, the migration to post-quantum digital signatures is less time-sensitive than for KEMs, allowing for a more deliberate and carefully planned transition. Since post-quantum signature schemes often involve larger keys and signatures, greater computational overhead, and increased implementation complexity, their deployment may incur higher costs - reinforcing the importance of keeping the migration as simple and efficient as possible.

TODO: migration strategies, hybrid signatures vs dual signatures, etc.

4.1. PQ/T hybrid digital signatures

PQ/T hybrid digital signatures, which combine traditional and post-quantum algorithms, aim to provide resilience against future quantum threats by ensuring that if either algorithm remains secure, the signature remains valid. This dual-layer approach offers protection in the face of current uncertainty around newly standardized post-quantum schemes and implementations of them. However, hybrid signatures introduce considerable implementation and operational complexity:

* The number of possible hybrid combinations leads to interoperability challenges and increased implementation burden.

* If one scheme is compromised, forgery is only a concern while the corresponding public key remains trusted— most systems already revoke or rotate compromised keys.

* Long-term protection through hybrids may be limited in practice due to standard key management practices.

Instead of relying solely on hybrids, protocols should prioritize cryptographic agility-embedding algorithm identifiers in keys and supporting efficient key rollover. While signature migration should be planned proactively, broad deployment of PQC signature schemes can be aligned with infrastructure readiness and the availability of well-vetted, efficient standards.

5. Infrastructure costs

Migrating to post-quantum cryptography (PQC) necessitates potentially significant updates to an organization’s cryptographic infrastructure. The process requires careful planning and resource allocation to address various financial and operational costs.

A key aspect of PQC migration involves identifying and budgeting for discovery initiatives, which aim to understand the organization’s cryptographic assets and their PQC relevancy. This includes building a comprehensive inventory of cryptographic use and associated assets. The process of inventorying may require specific tools and methods, which also factor into the initial costs.

A major cost driver is determining whether PQC updates can be implemented through software updates or will necessitate more expensive hardware replacements or upgrades. Engaging with system vendors is crucial to confirm migration needs, inquire about the cost of new PQC solutions, and understand the anticipated business impact of implementation efforts. For custom or niche systems, organizations may need to budget for the cost of developing internal PQC-compliant solutions.

Specific infrastructure components and systems require updates, leading to associated costs:

* Network Protocols and Systems: Protocols like TLS, SSH, and QUIC, widely used in telecom networks and general IT infrastructure, need to integrate PQC for key exchange and authentication. While the computational performance impact of PQC Key Encapsulation Mechanisms (KEMs) like ML-KEM on handshake speed is often minimal or even faster compared to traditional methods, the size of PQC artifacts is much larger, which can lead to increased bandwidth usage, increased number of extra round trips and potential delays. While tweaking network parameters can alleviate some issues, it involves trade-offs, which relate to operational network costs.

* Message Processing: Post-quantum signature algorithms often handle messages differently from the traditional "digest-then-sign" model, typically processing the entire message internally. This can degrade performance for large messages, particularly when streaming data to constrained signing environments such as HSMs via interfaces like PKCS#11. While pre-hashing messages can mitigate performance issues, it introduces additional complexity— requiring applications to adapt to algorithms that support streaming processing to reduce memory usage. Managing these varied processing approaches across systems increases both development and operational overhead.

* Public Key Infrastructure (PKI): The PKI supporting systems needs to be updated to handle PQC keys and certificates. This involves changes to Certificate Authorities (CAs), certificate formats (e.g., X.509), and related processes. Various hybrid certificate formats are being explored to facilitate the transition, each with different complexity and potential overhead. The deployment of new Trust Anchors can also be a time-consuming and costly process.

* Constrained Devices: Devices with long operational lifetimes in environments like industrial control systems, vehicles, satellites, smart meters, and smart cards present unique challenges and potential costs. Upgrading cryptographic capabilities on such devices may be difficult or even impossible due to resource constraints, physical location, or immutability features, potentially requiring expensive field updates or device replacement. For guidance on integrating Post-Quantum Cryptography (PQC) into such constrained environments, see [I-D.ietf-pquip-pqc-hsm-constrained].

* Hybrid Implementations: While motivated by security concerns during the transition period, hybrid scheme strategies can introduce increased complexity and potential overhead in terms of data size. The combinatorial explosion of combining various traditional and PQC schemes adds complexity to implementation and testing.

* Continuous monitoring and evaluation are also necessary to track migration progress and adapt to evolving quantum capabilities, requiring ongoing resource commitment and increasing hardware cost.

In addition to complexity, PQ/T hybrid schemes can incur higher migration costs. Organizations adopting hybrids will eventually need to migrate again to pure post-quantum schemes once confidence in these algorithms solidifies, deferring some costs rather than eliminating them. This means maintaining dual algorithm infrastructure (e.g., certificate chains, key management, validation logic) during the hybrid phase, followed by another transition with its own cost, testing, and operational risks. For many deployments- especially constrained or high-assurance environments— this two-step migration may be more burdensome than a single, well-timed switch to a vetted post-quantum alternative.

Adopting principles like cryptographic agility is highlighted as a way to manage costs in the long term by designing systems that can undergo multiple cryptographic transitions without major architectural changes, thereby reducing the cost of future updates. However, achieving true agility requires effort in standardization and implementation to support simultaneous use or dynamic negotiation of algorithms.

6. Standards Compliance

Protocol designers are encouraged to prioritize solutions that conform to established, widely trusted standards such as FIPS. This helps ensure compatibility with regulatory requirements and facilitates future certification. Migration strategies should align with guidance such as CMVP, and anticipate the certification process for post-quantum algorithms.

With the NIST standardization of post-quantum algorithms (e.g., [NIST-FIPS-203], [NIST-FIPS-204], [NIST-FIPS-205] and [NIST-SP-800-208]), the certification pathway is becoming clearer and more structured. However, during the transitional period— while post-quantum implementations mature— it may be beneficial to adopt PQC/T approaches. These offer several advantages:

* They provide defense in depth by enabling fallback to a well-established, thoroughly vetted implementations of traditional schemes.

* Since the certification process is typically lengthy, using already-certified traditional implementations alongside post-quantum algorithms still undergoing certification is a practical approach for deployments that require approved component schemes.

NIST guidance documents such as [NIST-SP-800-56C] and [NIST-SP-800-135] offer precedents for this approach. For example, in key agreement schemes, hybrid shared secrets can be formed by combining output from a NIST-approved algorithm with that of a non-approved one. [NIST-SP-800-56C] specifically endorses simple concatenation as an acceptable method for deriving hybrid shared secrets, provided at least one component is generated by an approved mechanism.

7. Migration Pitfalls

Several practices should be avoided during PQC migration:

* Key reuse across modes: Using the same keypair for PQ/T hybrid and traditional signatures risks downgrade attacks.

* Dynamic algorithm negotiation: Negotiating algorithm types at runtime (e.g., in TLS) can allow downgrade or confusion attacks. Algorithm identifiers should be part of the public key structure.

* Excessive hybridization: Supporting too many hybrid combinations introduces combinatorial complexity and compatibility issues.

* Ignoring key lifecycle: Systems that do not account for key expiration and revocation are particularly vulnerable in post-quantum scenarios.

Robust protocol design, infrastructure readiness, and clear separation of cryptographic roles are essential to avoid these anti-patterns.

8. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

9. Security Considerations

TODO

10. IANA Considerations

This document has no IANA actions.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[rfc7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/rfc/rfc7748>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[rfc9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

11.2. Informative References

[I-D.ietf-pquip-pqc-hsm-constrained] Reddy.K, T., Wing, D., S, B., and K. Kwiatkowski, "Adapting Constrained Devices for Post-Quantum Cryptography", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-hsm-constrained-01, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-hsm-constrained-01>.

[NIST-FIPS-203] "Module-lattice-based key-encapsulation mechanism standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.203, August 2024, <https://doi.org/10.6028/nist.fips.203>.

[NIST-FIPS-204] "Module-lattice-based digital signature standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.204, August 2024, <https://doi.org/10.6028/nist.fips.204>.

[NIST-FIPS-205]
"Stateless hash-based digital signature standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.205, August 2024, <https://doi.org/10.6028/nist.fips.205>.

[NIST-SP-800-135]
Dang, Q., "Recommendation for existing application-specific key derivation functions", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-135r1, 2011, <https://doi.org/10.6028/nist.sp.800-135r1>.

[NIST-SP-800-208]
Cooper, D., Apon, D., Dang, Q., Davidson, M., Dworkin, M., and C. Miller, "Recommendation for Stateful Hash-Based Signature Schemes", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-208, October 2020, <https://doi.org/10.6028/nist.sp.800-208>.

[NIST-SP-800-56C]
Barker, E., Chen, L., and R. Davis, "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-56cr2, August 2020, <https://doi.org/10.6028/nist.sp.800-56cr2>.

[tlsiana] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-14, 16 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-14>.

Author’s Address

Kris Kwiatkowski
Email: kris@amongbytes.com