Internet Engineering Task Force (IETF)
Request for Comments: 9794
Category: Informational
ISSN: 2070-1721
June 2025

F. Driscoll
M. Parsons
UK National Cyber Security Centre
B. Hale
Naval Postgraduate School

# Terminology for Post-Quantum Traditional Hybrid Schemes

## Abstract

One aspect of the transition to post-quantum algorithms in cryptographic protocols is the development of hybrid schemes that incorporate both post-quantum and traditional asymmetric algorithms. This document defines terminology for such schemes. It is intended to be used as a reference and, hopefully, to ensure consistency and clarity across different protocols, standards, and organisations.

## Status of This Memo



## Copyright Notice



## Table of Contents

Authors’ Addresses

# 1. Introduction

The mathematical problems of integer factorisation and discrete logarithms over finite fields or elliptic curves underpin most of the asymmetric algorithms used for key establishment and digital signatures on the Internet. These problems, and hence the algorithms based on them, will be vulnerable to attacks using Shor’s Algorithm on a sufficiently large general-purpose quantum computer, known as a Cryptographically Relevant Quantum Computer (CRQC). Current predictions vary on when, or if, such a device will exist. However, it is necessary to anticipate and prepare to defend against such a development. Data encrypted today (in 2025) with an algorithm vulnerable to a quantum computer can be stored for decryption by a future attacker with a CRQC. Signing algorithms in products that are expected to be in use for many years, and that cannot be updated or replaced, are also at risk if a CRQC is developed during the operational lifetime of that product.

Ongoing responses to the potential development of a CRQC include modifying established (or standardised) protocols to use asymmetric algorithms that are designed to be secure against quantum computers as well as today’s classical computers. These algorithms are called "post-quantum", while algorithms based on integer factorisation, finite-field discrete logarithms, or elliptic-curve discrete logarithms are called "traditional cryptographic algorithms". In this document, "traditional algorithm" is also used to refer to this class of algorithms.

At the time of publication, the term "post-quantum" is generally used to describe cryptographic algorithms that are designed to be secure against an adversary with access to a CRQC. Post-quantum algorithms can also be referred to as "quantum-resistant" or "quantum-safe" algorithms. There are merits to the different terms. For example, some prefer to use the terms quantum-resistant or quantum-safe to explicitly indicate that these algorithms are designed to be secure against quantum computers. Others disagree and prefer to use the term post-quantum, in case of compromises against such algorithms that could make the terms quantum-resistant or quantum-safe misleading. Similarly, some prefer to refer specifically to Shor’s Algorithm or to the mathematical problem that is being used to prevent attacks. Post-Quantum Cryptography (PQC) is commonly used amongst the cryptography community, and so it will be used throughout this document. Similarly, the term "traditional algorithm" will be used throughout the document as, at the time of publication, it is widely used in the community, though other terms, including classical, pre-quantum, or quantum-vulnerable, are preferred by some.

To mitigate risks, there may be a requirement for protocols that use both algorithm types, either during the transition from traditional to post-quantum algorithms or as a general solution. When the risk of deploying new algorithms is above the accepted threshold for their use case, a designer may combine a post-quantum algorithm with a traditional algorithm, with the goal of adding protection against an attacker with a CRQC to the security properties provided by the traditional algorithm. They may also implement a post-quantum algorithm alongside a traditional algorithm for ease of migration from an ecosystem where only traditional algorithms are implemented and used, to one that only uses post-quantum algorithms. Examples of solutions that could use both types of algorithm include, but are not limited to, [RFC9370], [HYBRID-TLS], [COMPOSITE-KEM], and [RFC9763].

Schemes that combine post-quantum and traditional algorithms for key establishment or digital signatures are often called "hybrids". For example:

* The National Institute of Standards and Technology (NIST) defines hybrid key establishment to be a "scheme that is a combination of two or more components that are themselves cryptographic key-establishment schemes" [NIST_PQC_FAQ].

* The European Telecommunications Standards Institute (ETSI) defines hybrid key exchanges to be "constructions that combine a traditional key exchange ... with a post-quantum key exchange ... into a single key exchange" [ETSI_TS103774].

The word "hybrid" is also used in cryptography to describe encryption schemes that combine asymmetric and symmetric algorithms [RFC9180], so using it in the post-quantum context overloads it and risks misunderstandings. However, this terminology is well-established amongst the Post-Quantum Cryptography (PQC) community. Therefore, an attempt to move away from its use for PQC could lead to multiple definitions for the same concept, resulting in confusion and lack of clarity. At the time of publication, hybrid is generally used for schemes that combine post-quantum and traditional algorithms; it will be so used throughout this document, though some have alternative preferences such as double-algorithm or multi-algorithm.

This document provides language for constructions that combine traditional and post-quantum algorithms. Specific solutions for enabling the use of multiple asymmetric algorithms in cryptographic schemes may be more general than this, allowing the use of solely traditional or solely post-quantum algorithms. However, where relevant, we focus on post-quantum traditional combinations as these are the motivation for the wider work in the IETF. This document is intended as a reference terminology guide for other documents, in order to add clarity and consistency across different protocols, standards, and organisations. Additionally, this document aims to reduce misunderstandings about the use of the word "hybrid" and to define a shared language for different types of post-quantum and traditional hybrid constructions.

In this document, a "cryptographic algorithm" is defined, as in [NIST_SP_800-152], to be a "well-defined computational procedure that takes variable inputs, often including a cryptographic key, and produces an output". Examples include RSA, Elliptic Curve Diffie-Hellman (ECDH), Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) (formerly known as Kyber), and Module-Lattice-Based Digital Signature Algorithm (ML-DSA) (formerly known as Dilithium). The expression "cryptographic scheme" is used to refer to a construction that uses a cryptographic algorithm or a group of cryptographic algorithms to achieve a particular cryptographic outcome, e.g., key agreement. A cryptographic scheme may be made up of a number of functions. For example, a Key Encapsulation Mechanism (KEM) is a cryptographic scheme consisting of three functions: Key Generation, Encapsulation, and Decapsulation. A cryptographic protocol incorporates one or more cryptographic schemes. For example, TLS [RFC8446] is a cryptographic protocol that includes schemes for key agreement, record layer encryption, and server authentication.

## 2. Primitives

This section introduces terminology related to cryptographic algorithms and to hybrid constructions for cryptographic schemes.

Traditional asymmetric cryptographic algorithm:
An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms, elliptic curve discrete logarithms, or related mathematical problems.

A related mathematical problem is one that can be solved by solving the integer factorisation, finite field discrete logarithm, or elliptic curve discrete logarithm problem.

Where there is little risk of confusion, traditional asymmetric cryptographic algorithms can also be referred to as "traditional algorithms" for brevity. Traditional algorithms can also be called "classical" or "conventional" algorithms.

Post-quantum asymmetric cryptographic algorithm:
An asymmetric cryptographic algorithm that is intended to be secure against attacks using quantum computers as well as classical computers.

Where there is little risk of confusion, post-quantum asymmetric cryptographic algorithms can also be referred to as "post-quantum algorithms" for brevity. Post-quantum algorithms can also be called "quantum-resistant" or "quantum-safe" algorithms.

As with all cryptography, it always remains the case that attacks, either quantum or classical, may be found against post-quantum algorithms. Therefore, it should not be assumed that an algorithm will not be compromised just because it is designed to provide post-quantum cryptography. Should an attack be found against a post-quantum algorithm, it is commonly still referred to as a "post-quantum algorithm", as they were designed to protect against an adversary with access to a CRQC, and the labels are referring to the designed or desired properties.

There may be asymmetric cryptographic constructions that are neither post-quantum nor asymmetric traditional algorithms according to the definitions above. These are out of scope of this document.

Component asymmetric algorithm:
Each cryptographic algorithm that forms part of a cryptographic scheme.

An asymmetric component algorithm operates on the input of the cryptographic operation and produces a cryptographic output that can be used by itself or jointly to complete the operation. Where there is little risk of confusion, component asymmetric algorithms can also be referred to as "component algorithms" for brevity, as is done in the following definitions.

Single-algorithm scheme:
A cryptographic scheme with one component algorithm.

A single-algorithm scheme could use either a traditional algorithm or a post-quantum algorithm.

Multi-algorithm scheme:
A cryptographic scheme that incorporates more than one component algorithm, where the component algorithms have the same cryptographic purpose as each other and as the multi-algorithm scheme.

For example, a multi-algorithm signature scheme may include multiple signature algorithms, or a multi-algorithm Public Key Encryption (PKE) scheme may include multiple PKE algorithms. Component algorithms could be all traditional, all post-quantum, or a mixture of the two.

Post-Quantum Traditional (PQ/T) hybrid scheme:
A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

Components of a PQ/T hybrid scheme operate on the same input message and their output is used together to complete the cryptographic operation either serially or in parallel. PQ/T hybrid scheme design is aimed at requiring successful breaking of all component algorithms to break the PQ/T hybrid scheme's security properties.

PQ/T hybrid Key Encapsulation Mechanism (KEM):
A multi-algorithm KEM made up of two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm. The component algorithms could be KEMs or other key establishment algorithms.

PQ/T hybrid Public Key Encryption (PKE):
A multi-algorithm PKE scheme made up of two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm. The component algorithms could be PKE algorithms or other key establishment algorithms.

The standard security property for a PKE scheme is indistinguishability under chosen-plaintext attack (IND-CPA) [BDPR]. IND-CPA security is not sufficient for secure communication in the presence of an active attacker. Therefore, in general, PKE schemes are not appropriate for use on the Internet, and KEMs, which provide indistinguishability under chosen-ciphertext attack (IND-CCA) [BDPR], are required.

PQ/T hybrid digital signature:
A multi-algorithm digital signature scheme made up of two or more component digital signature algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

Note that there are many possible ways of constructing a PQ/T hybrid digital signature. Examples include parallel signatures, composite signatures, or nested signatures.

PQ/T hybrid KEMs, PQ/T hybrid PKE, and PQ/T hybrid digital signatures are all examples of PQ/T hybrid schemes.

Post-Quantum Traditional (PQ/T) hybrid composite scheme:
A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm, and where the resulting composite scheme is exposed as a singular interface of the same type as the component algorithms.

A PQ/T hybrid composite can be referred to as a "PQ/T composite". An example of a PQ/T hybrid composite is a single KEM algorithm comprised of a PQ KEM component and a traditional KEM component, for which the result presents as a KEM output.

PQ/T hybrid combiner:
A method that takes two or more component algorithms and combines them to form a PQ/T hybrid scheme.

PQ/PQ hybrid scheme:
A multi-algorithm scheme where all components are post-quantum algorithms.

The definitions for types of PQ/T hybrid schemes can be adapted to define types of PQ/PQ hybrid schemes, which are multi-algorithm schemes where all component algorithms are post-quantum algorithms. These are designed to mitigate risks when the two post-quantum algorithms are based on different mathematical problems. Some prefer to refer to these as PQ/PQ multi-algorithm schemes, and reserve the term "hybrid" for PQ/T hybrids.

In cases where there is little chance of confusion between other types of hybrid cryptography (e.g., as defined in [RFC4949]) and where the component algorithms of a multi-algorithm scheme could be either post-quantum or traditional, it may be appropriate to use the phrase "hybrid scheme" without PQ/T or PQ/PQ preceding it.

Component scheme:
Each cryptographic scheme that makes up a PQ/T hybrid scheme or PQ/T hybrid protocol.

## 3. Cryptographic Elements

This section introduces terminology related to cryptographic elements and their inclusion in hybrid schemes.

Cryptographic element:
Any data type (private or public) that contains an input or output value for a cryptographic algorithm or for a function making up a cryptographic algorithm.

Types of cryptographic elements include public keys, private keys, plaintexts, ciphertexts, shared secrets, and signature values.

Component cryptographic element:
A cryptographic element of a component algorithm in a multi-algorithm scheme.

For example, in [HYBRID-TLS], the client’s keyshare contains two component public keys: one for a post-quantum algorithm and one for a traditional algorithm.

Composite cryptographic element:
A cryptographic element that incorporates multiple component cryptographic elements of the same type for use in a multi-algorithm scheme, such that the resulting composite cryptographic element is exposed as a singular interface of the same type as the component cryptographic elements.

For example, a composite cryptographic public key is made up of two component public keys.

PQ/T hybrid composite cryptographic element:
A cryptographic element that incorporates multiple component cryptographic elements of the same type for use in a multi-algorithm scheme, such that the resulting composite cryptographic element is exposed as a singular interface of the same type as the component cryptographic elements, where at least one component cryptographic element is post-quantum and at least one is traditional.

Cryptographic element combiner:
A method that takes two or more component cryptographic elements of the same type and combines them to form a composite cryptographic element.

A cryptographic element combiner could be concatenation, such as where two component public keys are concatenated to form a composite public key as in [HYBRID-TLS], or something more involved such as the dualPRF defined in [BINDEL].

## 4. Protocols

This section introduces terminology related to the use of post-quantum and traditional algorithms together in protocols.

PQ/T hybrid protocol:
A protocol that uses two or more component algorithms providing the same cryptographic functionality, where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

For example, a PQ/T hybrid protocol providing confidentiality could use a PQ/T hybrid KEM such as in [HYBRID-TLS], or it could combine the output of a post-quantum KEM and a traditional KEM at the protocol level to generate a single shared secret, such as in [RFC9370]. Similarly, a PQ/T hybrid protocol providing authentication could use a PQ/T hybrid digital signature scheme, or it could include both post-quantum and traditional single-algorithm digital signature schemes.

A protocol that can negotiate the use of either a traditional algorithm or a post-quantum algorithm, but not the use of both types of algorithm, is not a PQ/T hybrid protocol. Protocols that use two or more component algorithms but with different cryptographic functionalities, for example, a post-quantum KEM and a Pre-Shared Key (PSK), are also not PQ/T hybrid protocols.

PQ/T hybrid protocol with composite key establishment:
A PQ/T hybrid protocol that incorporates a PQ/T hybrid composite scheme to achieve key establishment, in such a way that the protocol fields and message flow are the same as those in a version of the protocol that uses a single-algorithm scheme.

For example, a PQ/T hybrid protocol with composite key establishment could include a single PQ/T hybrid KEM, such as in [HYBRID-TLS].

PQ/T hybrid protocol with composite data authentication:
A PQ/T hybrid protocol that incorporates a PQ/T hybrid composite scheme to achieve data authentication, in such a way that the protocol fields and message flow are the same as those in a version of the protocol that uses a single-algorithm scheme.

For example, a PQ/T hybrid protocol with composite data authentication could include data authentication through the use of a PQ/T composite hybrid digital signature, exposed as a single interface for PQ signature and traditional signature components.

PQ/T hybrid protocol with composite entity authentication:
A PQ/T hybrid protocol that incorporates a PQ/T hybrid composite scheme to achieve entity authentication, in such a way that the protocol fields and message flow are the same as those in a version of the protocol that uses a single-algorithm scheme.

For example, a PQ/T hybrid protocol with composite entity authentication could include entity authentication through the use of PQ/T Composite Hybrid certificates.

In a PQ/T hybrid protocol with a composite construction, changes are primarily made to the formats of the cryptographic elements, while the protocol fields and message flow remain largely unchanged. In implementations, most changes are likely to be made to the cryptographic libraries, with minimal changes to the protocol libraries.

PQ/T hybrid protocol with non-composite key establishment:
A PQ/T hybrid protocol that incorporates multiple single-algorithm schemes to achieve key establishment, where at least one uses a post-quantum algorithm and at least one uses a traditional algorithm, in such a way that the formats of the component cryptographic elements are the same as when they are used as a

part of a single-algorithm scheme.

For example, a PQ/T hybrid protocol with non-composite key establishment could include a traditional key exchange scheme and a post-quantum KEM. A construction like this for the Internet Key Exchange Protocol Version 2 (IKEv2) is enabled by [RFC9370].

PQ/T hybrid protocol with non-composite authentication:
A PQ/T hybrid protocol that incorporates multiple single-algorithm schemes to achieve authentication, where at least one uses a post-quantum algorithm and at least one uses a traditional algorithm, in such a way that the formats of the component cryptographic elements are the same as when they are used as part of a single-algorithm scheme.

For example, a PQ/T hybrid protocol with non-composite authentication could use a PQ/T parallel PKI with one traditional certificate chain and one post-quantum certificate chain.

In a PQ/T hybrid protocol with a non-composite construction, changes are primarily made to the protocol fields, the message flow, or both, while changes to cryptographic elements are minimised. In implementations, most changes are likely to be made to the protocol libraries, with minimal changes to the cryptographic libraries.

It is possible for a PQ/T hybrid protocol to be designed with both composite and non-composite constructions. For example, a protocol that offers both confidentiality and authentication could have composite key agreement and non-composite authentication. Similarly, it is possible for a PQ/T hybrid protocol to achieve certain cryptographic outcomes in a non-hybrid manner. For example, [HYBRID-TLS] describes a PQ/T hybrid protocol with composite key agreement, but with single-algorithm authentication.

PQ/T hybrid protocols may not specify non-composite aspects, but can choose to do so for clarity, in particular, if including both composite and non-composite aspects.

PQ/T hybrid composite protocol:
A PQ/T hybrid protocol that only uses composite constructions can be referred to as a "PQ/T hybrid composite protocol".

An example of this is a protocol that only provides entity authentication, and achieves this using PQ/T hybrid composite entity authentication. Similarly, another example is a protocol that offers both key establishment and data authentication, and achieves this using both PQ/T hybrid composite key establishment and PQ/T hybrid composite data authentication.

PQ/T hybrid non-composite protocol:
A PQ/T hybrid protocol that does not use only composite constructions can be referred to as a "PQ/T hybrid non-composite protocol".

For example, a PQ/T hybrid protocol that offers both confidentiality and authentication and uses composite key agreement and non-composite authentication would be referred to as a "PQ/T hybrid non-composite protocol".

## 5. Properties

This section describes some properties that may be desired from or achieved by a PQ/T hybrid scheme or a PQ/T hybrid protocol. Properties of PQ/T hybrid schemes are still an active area of research and development, e.g., in [BINDELHALE]. This section does not attempt to be comprehensive, but rather covers a basic set of properties.

It is not possible for one PQ/T hybrid scheme or PQ/T hybrid protocol to achieve all of the properties in this section. To understand what properties are required, a designer or implementer will think about why they are using a PQ/T hybrid scheme. For example, a scheme that is designed for implementation security will likely require PQ/T hybrid confidentiality or PQ/T hybrid authentication, while a scheme for interoperability will require PQ/T hybrid interoperability.

PQ/T hybrid confidentiality:
: The property that confidentiality is achieved by a PQ/T hybrid scheme or a PQ/T hybrid protocol as long as at least one component algorithm that aims to provide this property remains secure.

PQ/T hybrid authentication:
: The property that authentication is achieved by a PQ/T hybrid scheme or a PQ/T hybrid protocol as long as at least one component algorithm that aims to provide this property remains secure.

The security properties of a PQ/T hybrid scheme or protocol depend on the security of its component algorithms, the choice of PQ/T hybrid combiner, and the capability of an attacker. Changes to the security of a component algorithm can impact the security properties of a PQ/T hybrid scheme providing hybrid confidentiality or hybrid authentication. For example, if the post-quantum component algorithm of a PQ/T hybrid scheme is broken, the scheme will remain secure against an attacker with a classical computer, but will be vulnerable to an attacker with a CRQC.

PQ/T hybrid protocols that offer both confidentiality and authentication do not necessarily offer both hybrid confidentiality and hybrid authentication. For example, [HYBRID-TLS] provides hybrid confidentiality but does not address hybrid authentication. Therefore, if the design in [HYBRID-TLS] is used with single-algorithm X.509 certificates as defined in [RFC5280], only authentication with a single algorithm is achieved.

PQ/T hybrid interoperability:
: The property that a PQ/T hybrid scheme or a PQ/T hybrid protocol can be completed successfully provided that both parties share support for at least one component algorithm.

: For example, a PQ/T hybrid digital signature might achieve hybrid interoperability if the signature can be verified by either verifying the traditional or the post-quantum component, such as the approach defined in Section 7.2.2 of [ITU-T-X509-2019]. In this example, a verifier that has migrated to support post-quantum algorithms is required to verify only the post-quantum signature, while a verifier that has not migrated will verify only the traditional signature.

In the case of a protocol that aims to achieve both authentication and confidentiality, PQ/T hybrid interoperability requires that at least one component authentication algorithm and at least one component algorithm for confidentiality is supported by both parties.

It is not possible for a PQ/T hybrid scheme to achieve both PQ/T hybrid interoperability and PQ/T hybrid confidentiality without additional functionality at a protocol level. For PQ/T hybrid interoperability, a scheme needs to work whenever one component algorithm is supported by both parties, while to achieve PQ/T hybrid confidentiality, all component algorithms need to be used. However, both properties can be achieved in a PQ/T hybrid protocol by building in downgrade protection external to the cryptographic schemes. For example, in [HYBRID-TLS], the client uses the TLS supported groups extension to advertise support for a PQ/T hybrid scheme, and the server can select this group if it supports the scheme. This is protected using TLS's existing downgrade protection, so it achieves PQ/T hybrid confidentiality, but the connection can still be made if either the client or server does not support the PQ/T hybrid scheme, so PQ/T hybrid interoperability is achieved.

The same is true for PQ/T hybrid interoperability and PQ/T hybrid authentication. It is not possible to achieve both with a PQ/T hybrid scheme alone, but it is possible with a PQ/T hybrid protocol that has appropriate downgrade protection.

PQ/T hybrid backwards compatibility:
The property that a PQ/T hybrid scheme or a PQ/T hybrid protocol can be completed successfully provided that both parties support the traditional component algorithm, while also using both algorithms if both are supported by both parties.

PQ/T hybrid forwards compatibility:
The property that a PQ/T hybrid scheme or a PQ/T hybrid protocol can be completed successfully using a post-quantum component algorithm provided that both parties support it, while also having the option to use both post-quantum and traditional algorithms if both are supported by both parties.

Note that PQ/T hybrid forwards compatibility is a protocol or scheme property only.

## 6. Certificates

This section introduces terminology related to the use of certificates in hybrid schemes.

PQ/T hybrid certificate:
A digital certificate that contains public keys for two or more component algorithms where at least one is a traditional algorithm and at least one is a post-quantum algorithm.

A PQ/T hybrid certificate could be used to facilitate a PQ/T hybrid authentication protocol. However, a PQ/T hybrid authentication protocol does not need to use a PQ/T hybrid certificate; separate certificates could be used for individual component algorithms.

The component public keys in a PQ/T hybrid certificate could be included as a composite public key or as individual component public keys.

The use of a PQ/T hybrid certificate does not necessarily achieve hybrid authentication of the identity of the sender; this is determined by properties of the chain of trust. For example, an end-entity certificate that contains a composite public key, but which is signed using a single-algorithm digital signature scheme, could be used to provide hybrid authentication of the source of a message, but would not achieve hybrid authentication of the identity of the sender.

Post-quantum certificate:
A digital certificate that contains a single public key for a post-quantum digital signature algorithm.

Traditional certificate:
A digital certificate that contains a single public key for a traditional digital signature algorithm.

X.509 certificates as defined in [RFC5280] could be either traditional or post-quantum certificates depending on the algorithm in the Subject Public Key Info. For example, a certificate containing a ML-DSA public key, as defined in [ML-DSA], would be a post-quantum certificate.

Post-quantum certificate chain:
A certificate chain where all certificates include a public key for a post-quantum algorithm and are signed using a post-quantum digital signature scheme.

Traditional certificate chain:
A certificate chain where all certificates include a public key for a traditional algorithm and are signed using a traditional digital signature scheme.

PQ/T hybrid certificate chain:
A certificate chain where all certificates are PQ/T hybrid certificates and each certificate is signed with two or more component algorithms with at least one being a traditional algorithm and at least one being a post-quantum algorithm.

A PQ/T hybrid certificate chain is one way of achieving hybrid authentication of the identity of a sender in a protocol, but it is not the only way. An alternative is to use a PQ/T parallel PKI as defined below.

PQ/T mixed certificate chain:
A certificate chain containing at least two of the three certificate types defined in this document (PQ/T hybrid certificates, post-quantum certificates, and traditional certificates).

For example, a traditional end-entity certificate could be signed by a post-quantum intermediate certificate, which in turn could be signed by a post-quantum root certificate. This may be desirable due to the lifetimes of the certificates, the relative difficulty of rotating keys, or for efficiency reasons. The security properties of a certificate chain that mixes post-quantum and traditional algorithms would need to be analysed on a case-by-case basis.

PQ/T parallel PKI:
Two certificate chains, one that is a post-quantum certificate chain and one that is a traditional certificate chain, and that are used together in a protocol.

A PQ/T parallel PKI might be used to achieve hybrid authentication or hybrid interoperability depending on the protocol implementation.

Multi-certificate authentication:
Authentication that uses two or more end-entity certificates.

For example, multi-certificate authentication may be achieved using a PQ/T parallel PKI.

## 7. Security Considerations

This document defines security-relevant terminology to be used in documents specifying PQ/T hybrid protocols and schemes. However, the document itself does not have a security impact on Internet protocols. The security considerations for each PQ/T hybrid protocol are specific to that protocol and should be discussed in the relevant specification documents. More general guidance about the security considerations, timelines, and benefits and drawbacks of the use of PQ/T hybrids is also out of scope of this document.

## 8. IANA Considerations

This document has no IANA actions.

## 9. Informative References


[BDPR] Bellare, M., Desai, A., Pointcheval, D., and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes", June 2001, <https://www.cs.ucdavis.edu/~rogaway/papers/relations.pdf>.

[BINDEL] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., and D. Stebila, "Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange", Post-Quantum Cryptography, PQCrypto 2019, Lecture Notes in Computer Science, vol. 11505, pp. 206-226, DOI 10.1007/978-3-030-25510-7_12, July 2019, <https://doi.org/10.1007/978-3-030-25510-7_12>.

[BINDELHALE] Bindel, N. and B. Hale, "A Note on Hybrid Signature Schemes", Cryptology ePrint Archive, Paper 2023/423, 23 July 2023, <https://eprint.iacr.org/2023/423.pdf>.

[COMPOSITE-KEM] Ounsworth, M., Gray, J., Pala, M., Klaussner, J., and S. Fluhrer, "Composite ML-KEM for use in X.509 Public Key Infrastructure and CMS", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-kem-06, 18 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-kem-06>.

[ETSI_TS103774] European Telecommunications Standards Institute (ETSI), "CYBER; Quantum-safe Hybrid Key Exchanges", ETSI TS 103 744 v1.1.1, December 2020, <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf>.

[HYBRID-TLS] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-12, 14 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-12>.

[ITU-T-X509-2019] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, October 2019, <https://www.itu.int/rec/T-REC-X.509-201910-I>.

[ML-DSA] Massimo, J., Kampanakis, P., Turner, S., and B. E. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-11, 22 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-11>.

[NIST_PQC_FAQ] NIST, "Post-Quantum Cryptography (PQC) FAQs", 31 January 2025, <https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs>.

[NIST_SP_800-152]
Barker, E., Smid, M., and D. Branstad, "A Profile for U. S. Federal Cryptographic Key Management Systems", NIST SP 800-152, DOI 10.6028/NIST.SP.800-15, October 2015, <https://doi.org/10.6028/NIST.SP.800-152>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/info/rfc9180>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/info/rfc9370>.

[RFC9763] Becker, A., Guthrie, R., and M. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", RFC 9763, DOI 10.17487/RFC9763, June 2025, <https://www.rfc-editor.org/info/rfc9763>.

## Acknowledgments

This document is the product of numerous fruitful discussions in the IETF PQUIP group.  Thank you in particular to Mike Ounsworth, John Gray, Tim Hollebeek, Wang Guilin, Rebecca Guthrie, Stephen Farrell, Paul Hoffman, and Sofa Celi for their contributions.  This document is inspired by many others from the IETF and elsewhere.

## Authors’ Addresses

Florence Driscoll
UK National Cyber Security Centre
Email: florence.d@ncsc.gov.uk

Michael Parsons
UK National Cyber Security Centre
Email: michael.p1@ncsc.gov.uk

Britta Hale
Naval Postgraduate School
Email: britta.hale@nps.edu