Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 4 June 2026

S. Farrell
Trinity College Dublin

1 December 2025

Post-Quantum Guidance for current deployments of IETF protocols. draft-farrell-tls-pqg-04

Abstract

We provide guidance on the use of post-quantum algorithms for those currently deploying applications using IETF protocols with support for such algorithms.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 June 2026.

Copyright Notice

Table of Contents

1. Introduction

[[This is not an "official" work item anywhere, the -00 was proposed to TLS as such, but this version generalises to more than just TLS. This was discussed at the IETF-124 secdispatch session and the outcome was that further discussion should be on the general security area list. (saag@ietf.org) The source for this is in https://github.com/sftcd/pqg/ PRs are welcome there too.]]

Due to concerns about the possible future existence of a cryptographically relevant quantum computer (CRQC), a number of IETF working groups have defined ways in which post-quantum (PQ) cryptographic algorithms can be used with IETF protocols such as TLS, SSH, IPsec, OpenPGP and others and with the public key infrastructure (PKI) that supports a number of these protocols. Implementers have also made headway in incorporating these changes into sometimes widely used implementations.

However, once supported by implementations, these changes support many different configurations so those deploying post-quantum algorithms now can be faced with an overly-broad set of choices, some of which might lead to worse interoperability or even lesser security than others. This document provides current guidance on a very high-level set of deployment choices that are recommended for use today.

It is reasonably likely that this guidance will change in the not-too distant future, as post-quantum support in protocols and implementations matures, so this document may well be updated in the relatively near future.

The format of this document is to provide very concise guidance in Section 3, and follow that with background material. A reader pressed for time may be able to stop reading at the end of Section 3. Some more specialised implementations and environments may have to meet other requirements that conflict with this guidance - in such cases those deploying will need to do more research in order to select good options. More detailed background is provided in [RFC9794] and [I-D.ietf-pquip-pqc-engineers].

The audience for this document are those deploying systems now. This guidance is not aimed at those developing IETF protocols, nor implementations of those. Given that it seems that the latter groups (protocol developers and implementers) seem determined to define and implement almost every possible combination of PQ everything, those deploying systems now, that have such PQ all kinds of everything, can benefit from simple guidance that addresses the most important aspect of the PQ transition.

2. Terminology

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.

3. Recommendations

3.1. Start using hybrid KEMs

We RECOMMEND moving as soon as practical to use of PQ/T hybrid Key Encapsulation Mechanisms (KEMs).

Once it becomes practical to use hybrid KEMs, such as X25519MLKEM768 for TLS, we do NOT RECOMMEND use of non-hybrid/classic groups or "pure" PQ KEMs.

3.2. Do nothing for now on signatures

For almost all deployments, we RECOMMEND taking no action at all at this point in time in relation to deployment of PQ signatures.

4. Background and Justifications

Many additional IANA codepoints (dozens) have been defined by IETF working groups for algorithms that are hoped to remain secure even in the face of a CRQC. Adding code-points to some relevant IANA registries doesn't require IETF consensus. This means that, in such case, anyone can register code-points for their favoured approach, typically so long as there is some specification for the algorithm concerned. For example, anyone can register a PQ algorithm in the TLS named group registry with the RECOMMENDED column set to 'n'

Various government entities in different countries have made contradictory recommendations in this space, leading to potential confusion for those deploying applications using PQ algorithms.

Hybrid KEMs are combinations of two or more KEMs with the goal of providing security as long as one of the component KEMs is able to provide security. Hybrid KEMs therefore typically consist of a newer, presumed post-quantum secure KEM (such as ML-KEM), to guard against attacks by a CRQC, as well as an established traditional KEM (such as variations of ECDH-KEM), to guard against rapid cryptanalysis of the post-quantum KEM.

Any reasonable Hybrid KEM construction provides greater security guarantees than single KEMs, but they may differ in the exact scenarios in which they provide such guarantees (e.g. only cryptanalysis against one KEM vs. some implementation faults in one KEM) and in how they are used in specific protocols. Generally, the IETF WG responsible for a specific protocol will have done the analysis as to how to safely incorporate hybrid KEMs.

Whereas key establishment needs to guard against passive attacks, which may be conducted long after online communication has taken place (i.e. harvest now, decrypt later attacks), signatures are typically only required to guard against active attacks. Therefore, a traditional signature scheme can secure protocols for as long as CRQCs do not exist.

Systems dealing with signatures that are required to still be usefully verifiable in the timeframe that might include a CRQC are rare and complex and are not further considered here. Systems that need to select a signature verification public key (and hence algorithm) now, for use in some years time, are also not covered by this guidance.

5. Security Considerations

As we transition from RSA and ECC based algorithms to newer approaches, we will necessarily gather implementation experience and learn from failures. Those deploying such systems are therefore advised to regularly monitor cryptanalytic advancements as well as attacks against natural implementations of newer schemes, and guard against failures using hybrid constructions such as the ones indicated above.

6. Acknowledgements

Thanks to Thomas Bellebaum for (subsequently heavily edited) background text. All errors, opinions, and ommisions of course remain the fault of the author.

7. IANA Considerations

TBD, but probably not needed.

8. References

8.1. 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/info/rfc2119>.

[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/info/rfc8174>.

8.2. Informative References

[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/info/rfc9794>.

[I-D.ietf-pquip-pqc-engineers] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

Author’s Address

Stephen Farrell
Trinity College Dublin
Dublin
2
Ireland
Phone: +353-1-896-2354
Email: stephen.farrell@cs.tcd.ie