Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 23 April 2026

S. Farrell
Trinity College Dublin

20 October 2025

Post-Quantum Guidance for current deployments of IETF protocols. draft-farrell-tls-pqg-03

Abstract

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

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 23 April 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 so is being proposed to the secdispatch list. The author does not expect that the current text will garner rough consensus, but wonders if we could get something useful that would without adding many words. 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), additional IANA [RFC8446] codepoints have been defined for algorithms that are hoped to remain secure even in the face of a CRQC. Adding code-points for to the relevant IANA registries often doesn't require IETF consensus. This means that anyone can register code-points for their favoured approach. In particular various government entities in various countries have made contradictory recommendations in this space, leading to potential confusion for those deploying applilcations using TLS. For example, anyone can register a PQ algorithm in the TLS registries with the RECOMMENDED column set to 'n'

This document sets out a deliberately concise set of recommendations for typical uses of post-quantum algorithms. This assumes the reader is familiar with the topic. Some implementations and environments may have to meet other requirements that conflict with this guidance.

Note that 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.

It is quite likely this guidance will need to be updated with a short-ish period (perhaps about two years).

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. Start using hybrid KEMs

The main recommendation is to move as soon as practical to use of hybrid KEMs, such as X25519MLKEM768.

Once it becomes practical to do the above, we do not recommend use of non-hybrid groups or "pure" PQ KEMs.

4. 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.

TODO: Define "almost all" somewhat better, but tersely.

5. Security Considerations

TBD

6. Acknowledgements

TBD

7. IANA Considerations

TBD, but probably not needed.

8. 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>.

[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>.

Author’s Address

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