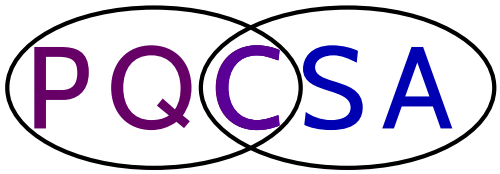

Post-Quantum Cryptography Support Action

Project number: Digital Europe 101190512

D2.1
Survey of PQC protocols.

Due date of deliverable: 2025-11-30
Actual submission date: 2025-11-30

WP contributing to the deliverable: WP2

Start date of project: 1. January 2025 Duration: 3 years

Coordinator:
Eindhoven University of Technology
https://pqcsa.eu

Revision 1.0

Project co-funded by the European Commission within Digital Europe		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	
SEN	Sensitive	

Survey of PQC protocols.

Stephen Farrell
Trinity College Dublin
stephen.farrell@cs.tcd.ie

2025-11-30
Revision 1.0

The work described in this report has been funded (in part) by the European Union in the DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC call in project 101190512 PQCSA. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
0.1	2025-10-26	First circulated version
1.0	2025-11-30	First published version

Abstract

There are many IETF protocols that are being extended in reaction to the possible future existence of a cryptographically relevant quantum computer. This report outlines the state of play for notable protocols involved and related IETF activities. The overall conclusion is a recommendation to devote effort to mitigatig the "harvest-now-decrypt-later" threat and (for most applications) to only monitor threats to authentication.

Keywords: WP2, IETF and PQ

Contents

1 Introduction **5**

2 PQ activities in IETF WGs and IRTF RGs **7**

2.1 Post-Quantum Use In Protocols Working Group (PQUIP) 8
2.2 SSH maintenance Working Group (SSHM) 8
2.3 Transport Layer Security Working Group (TLS) 9
2.4 OpenPGP Working Group (OpenPGP) 10
2.5 Hybrid Public Key Encryption Working Group (HPKE) 11
2.6 Limited Additional Mechanisms for PKIX and SMIME Working Group (LAMPS) 11
2.7 Message Level Security (MLS) 12
2.8 IP Security Maintenance and Extensions (IPSECME) 12
2.9 DNS operations Working Group (DNSOP) 13
2.10 Javascript Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) 14
2.11 Lightweight Authenticated Key Exchange Working Group (LAKE) 14
2.12 SIDR Operations (SIDROPS) 15
2.13 Common Authentication Technology Next Generation (KITTEN) 15
2.14 CryptoForum Research Group (CFRG) 15

3 Issues and points of disagreement **17**

3.1 Immediacy 17
3.2 How to document cryptographic algorithms 17
3.3 Fears of another Dual-EC 18
3.4 Combinatorics 19
3.5 KEM Combiners 20
3.6 Seeds 20

4 Interim conclusions and state of play **21**

Appendices **33**

List of Acronyms

ACME Automated Certificate Management Environment

AS Autonomous System

BGP Border Gateway Protocol

CA Certification Authority

CFRG CryptoForum Research Group

CMS Cryptographic Message Syntax

COSE CBOR Object Signing and Encryption

CRQC Cryptographically Rulevant Quantum Computer

DNSOP DNS operations Working Group

DNSSEC DNS Security Extensions

DNS Domain Name System

ECDH Elliptic Curve Diffie Hellman

EDHOC Ephemeral Diffie-Hellman Over COSE

EUF-CMA Existential Unforgeability under Chosen Message Attack

HPKE Hybrid Public Key Encryption Working Group

IANA Internet Assigned Numbers Authority

IETF Internet Engineering Task Force

IKE Internet Key Exchange

IPSECME IP Security Maintenance and Extensions

IPsec IP Security Extensions

IRTF Internet Research Task Force

JOSE Javascript Object Signing and Encryption

KEM Key Encapsulation Mechanism

KITTEN Common Authentication Technology Next Generation

LAKE Lightweight Authenticated Key Exchange Working Group

LAMPS Limited Additional Mechanisms for PKIX and SMIME Working Group

LoC Lines of code

MLS Message Level Security

NIST the USA's National Institure for Standards and Technology

OID ASN.1 Object Identifier

OpenPGP OpenPGP Working Group

PGP Pretty Good Privacy

PKI Public Key Infrastructure

PQC Post-Quantum Cryptography

PQUIP Post-Quantum Use In Protocols Working Group

PQ Post-Quantum

PSK Pre-Shared (symmetric) Key

RFC Request For Comments

RG Research Group

RIR Regional Internet Registry

RPKI Resourece PKI

SIDROPS SIDR Operations

SSHM SSH maintenance Working Group

SUF-CMA Strong Unforgeability under Chosen Message Attack

TLS Transport Layer Security Working Group

WG Working Group

Chapter 1

Introduction

In recent years there has been a lot of activity in various Internet Engineering Task Force (IETF) Working Group (WG)s aiming to handle protocol changes needed if there is ever a Cryptographically Rulevant Quantum Computer (CRQC). Typically, this involves relatively straightforward protocol changes to allow for the use of post-quantum Key Encapsulation Mechanism (KEM), usually in hybrid form, as part of session establishment, but also more complex changes to authentication where changes to signature schemes and Public Key Infrastructure (PKI) would be needed. This document outlines some of the set of Post-Quantum (PQ) protocol changes under way in the IETF and includes commentary on the current state of the work.[1]

The intent here is not to provide a full catalogue of all PQ work ongoing within the IETF or Internet Research Task Force (IRTF), but rather to highlight areas where work is reaching maturity, and areas where substantial work remains to be done before PQ-enabled protocols will be ready for widespread deployment.

There are of course PQ developments in other standards fora, such as CCSDS, ETSI and ITU-T, but the focus here is on developments in the IETF.

[1]The author of this report is a co-chair of both the IETF SSHM and OpenPGP, each of which are tackling these issues, and is also an active participant in some other WGs, so is not an entirely impartial reporter.

Chapter 2

PQ activities in IETF WGs and IRTF RGs

This chapter describes PQ activities in individual IETF WGs and IRTF Research Group (RG)s. The IRTF is a related organisation that has a number of RGs with the CFRG currently the only one doing PQ work.

Table 2.0.1 lists those covered in this document. The WG/RG name/acronym links to the relevant charter, where links to documents, meeting resources and for subscribing to the relevant mailing lists may be found. Note that anyone can subscribe to any of these mailing lists and participate in the work, though of course, such participation requires significant effort in terms of time. Effective participation also requires detailed knowledge of the relevant protocol. Appendix 4 provides a (non-exhaustive) synopsis of relevant IETF and IRTF process steps.

Table 2.0.1: IETF WGs and IRTF RGs with active PQ work

WG	Details
PQUIP	Section 2.1 This WG aims to provide general guidance on PQC
SSHM	Section 2.2 This WG does maintenance for the SSH protocol
TLS	Section 2.3 This WG develops and maintains the TLS protocol
OpenPGP	Section 2.4 This WG develops and maintains the PGP protocol
HPKE	Section 2.5 This WG develops and maintains the HPKE “encrypt-to-public-key” format
LAMPS	Section 2.6 This WG endlessly extends X.509 based PKI and CMS protocols
MLS	Section 2.7 This WG develops and maintains the MLS protocol
IPSECME	Section 2.8 This WG maintains the IPsec protocol
DNSOP	Section 2.9 This WG is the fallback place for DNS protocol discussions (at present)
JOSE COSE	Section 2.10 These WGs develop cryptographic tools for JSON and CBOR and are quite entwined in PQ terms
LAKE	Section 2.11

Continued on next page

Table 2.0.1: IETF WGs and IRTF RGs with active PQ work (Continued)

WG	Details
	This WG works on Lightweight Authenticated Key Exchange
SIDROPS	Section 2.12 This WG maintains RPKI protocols and produces operational guidance
KITTEN	Section 2.13 This WG maintains Kerberos and related protocols
CFRG	Section 2.14 This IRTF research group provides cryptographic support and research related to IETF interests

2.1 PQUIP

The PQUIP aims to provide general guidance for use of PQ in other IETF work. This group doesn't develop new protocols, nor extend existing ones, but for example works on documents providing design and operational guidance that aims to benefit other IETF WGs that are tackling PQ issues.

The WG maintain https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc which is an occasionally updated collation of links to IETF PQ drafts and activities. (Similar to this report, but with the aim of being comprehensive rather than opinionated.)

PQUIP has finished work on one document defining terminology: Request For Comments (RFC) 9794[1], and for example defines terms such as "PQ/T hybrid" where the "T" stands for "traditional." This is intended to help with consistency across IETF documents. We don't strictly follow that terminology here.

Another document aims to describe PQ issues in terms more easily understood by engineers [2] is in the RFC editor queue. This document provides useful background for protocol designers and implementers, though the recommendations do not describe feasible transition mechanisms for authentication. (That's not the fault of the authors, feasible transition mechanisms for authentication is a yet-unsolved problem in this author's opinion.)

PQUIP has also developed a document describing the "spectrum" of hybrid PQ/T-signatures [3] that is also in the RFC editor queue. This document is the first (but not last) that we'll mention that includes a justification for "immediate post-quantum algorithm selection" (section 1.2.2 of [3]). Section 3.1 discusses this general issue.

PQUIP is also developing documents offering guidance on implementing PQ algorithms on resource-constrained devices [4] and on backup and state-management for hash based signatures [5]. These are at an earlier stage of development.

There are also other Internet-drafts that may be the subject of subsequent WG adoption calls, or, based on discussion at the recent IETF meeting (https://datatracker.ietf.org/meeting/124/proceedings) this WG may declare victory and go dormant, as a number of WG participants expressed the opinion that this WG isn't the right place to develop generic guidance for PQ protocols. Discussions on that topic are ongoing.

2.2 SSHM

The charter for SSHM includes work to document the already-deployed sntrup761x25519-sha512 hybrid KEM. [6] That document is now in the RFC editor's queue, so has passed all stages of IETF approvals. Although this hybrid KEM has been deployed for some years, the processing of this document was controversial, partly due to the "normal" documenting-algorithms issues (see Section 3.2) but also because the NTRU Prime algorithm was not a

"winner" the USA's National Institure for Standards and Technology (NIST) Post-Quantum Cryptography (PQC) competition.

Another SSHM draft [7] defines three ML-KEM hybrids (with x25519, p256 and p384) and at the time of writing has passed working group last-call (WGLC). The mlkem768x25519-sha256 variant is expected to eventually become widely deployed, whether or not the NIST-curve ones do, remains to be seen. That WGLC was less controversial than might have been expected, perhaps indicating IETF/WG participants are becomming more sanguine about PQ disagreements, hopefully a sign that positions are maturing. (Though there still was some angst related to Section 3.2.)

There are also non-WG Internet-drafts that propose PQ schemes for authentication (e.g. [8]), additional hybrid KEMs (e.g. [9]) and even "pure" (non-hybrid) PQ KEMs (e.g. [10]). Whether or not any of those progress within the WG is uncertain - the SSHM WG charter calls for only progressing documents that have "broad implementer interest" and that is not so far evident for any of those.

2.3 TLS

The TLS WG has a draft [11] defining the abstract way to combine Elliptic Curve Diffie Hellman (ECDH) with any PQ KEM, that (with some restrictions) allows an ECDH or PQ KEM key_share to be used in multiple combined KEMs, so a TLS ClientHello[1] can contain, e.g. one ECDH key_share and two KEM public keys and the TLS session might end up using a combined KEM formed using the catention of the ECDH key_share with either of the PQ KEM pk's. This reduces the size of the ClientHello. This abstract hybrid draft is now in the RFC editor's queue and has passed all stages of IETF review.

The currently most important PQ draft [12] within the TLS WG defines hybrid KEMs for X255519MLKEM768, SecP256r1MLKEM768 and SecP384r1MLKEM1024, while also obsoleting code-points for earlier equivalents using Kyber rather than ML-KEM. Of these, the X25519MLKEM768 option is by now extremely widely deployed in browsers and widely used TLS libraries (such as OpenSSL) many of which only support that single hybrid KEM in the TLS protocol. Even though this hybrid KEM is so widely deployed, the Internet-draft has still to undergo many steps of IETF approval processes, though it is extremely unlikely to undergo other than editorial changes, given that widespread deployment.

There is also a formally adopted TLS draft [13] specifying how to use the three size variants of ML-KEM as a standalone, "pure" PQ KEM. Some WG participants see this as an uncontroversial thing simply defining an option that will be ready to be used once confidence in "pure" ML-KEM has reached a sufficient level. Others regard formally adopting such a document as extremely unwise, given there are many who do not currently have such confidence in standalone use of ML-KEM. The adoption of this document has been the subject of multiple appeals, and appeals about appeal handling and general IETF processes. How the resulting mess will be resolved may be an interesting experiment in IETF processes, but formal adoption of the document is not needed to allocate the relevant code-point (which has been allocated) so those who might want to follow this approach can already do so and likely achieve interoperability. There is no indication at this time that any widely used software plans to do this, but it will likely be an option for those willing to go off-piste. See also Section

[1] The ClientHello message in TLS is the first sent, contains many cryptographic parameters and is quite size-sensitive (a too-large ClientHello might affect error rates).

3.3 for more discussion on the substantive aspect of this controversy. This draft is currently undergoing an thoroughly controversial WGLC.

Another relevant TLS WG draft, [14] also in the RFC editor queue sets out the that intent of the TLS WG is that all PQ enhancements will only apply to TLSv1.3 and later, and that no effort will be devoted to PQ enhancements to TLSv1.2 or earlier versions. Time will tell whether that goal will be adhered to or not. There is a history of revisiting such decisions if practical deployment challenges indicate that it causes sufficiently impactful weaknesses, e.g. [15].

To date, the TLS WG has not devoted much time to discussion of PQ authentication in TLS and there are no adopted WG drafts on that topic. There is one very recent proposal [16] but the approach(es) that the TLS WG will take on this topic cannot yet be predicted.

2.4 OpenPGP

The OpenPGP has its main PQ draft [17] at the IETF last-call stage in the IETF approval process. That draft defines a hybrid of either X25519 or X448 with ML-KEM and signature schemes based on EdDSA with ML-DSA or, lastly, SLH-DSA as an optional-to-implement standalone PQ signature scheme. This PQ specification consumes 7 code-points of the relevant single-octet code-point space (for ML-DSA-65+Ed25519, ML-DSA-87+Ed448, SLH-DSA-SHAKE-128s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-256s, ML-KEM-768+X25519 and ML-KEM-1024+X448). This constrained code-point space, together with PQ's combinatorics is partly why the OpenPGP WG has split the PQ work over multiple drafts, so that works-in-progress can re-use the limited code-points available for experiments. See also Section 3.4 for discussion of the general issue of combinatorics related to PQ protocols.

The PQ interoperability situation for OpenPGP users is complicated by the existence of a "split" in the implementer community, where a, (or perhaps "the"), major implementation chose to disengage from the IETF process during the work to evolve RFC 4880 [18] into what became RFC 9580 [19]. We therefore have the "official" OpenPGP specification RFC 9580 [19] (with good interoperability among different implementations) but we also have Pretty Good Privacy (PGP) as specified by one project ("LibrePGP") where the equivalent specification is being handled as a personal Internet-draft [20] that is periodically updated according to the wishes of that project, and that also includes some PQ features. A shorthand way to consider these is, that RFC 4880 defines version 4 (of relevant packet types), the LibrePGP project maintains a personal Internet-draft that defines a version 5, and RFC 9580 defines version 6. (IETF participants moved to version 6 so as to preserve the possibility of "healing the schism" in the future.)

The different use-cases and versions of OpenPGP packets also lead to some subtle issues with where PQ features can be used, for example, based on an extended discussion in the OpenPGP WG, section 3.5 of [17] currently says: "All PQ(/T) asymmetric algorithms are to be used only in v6 (and newer) keys and certificates, with the single exception of ML-KEM-768+X25519 (algorithm ID 35), which is also allowed in v4 encryption- capable subkeys."

There is an additional OpenPGP WG draft [21] still being processed within the WG that currently aims to allocate another ten code-points for hybrid KEMs and signatures using NIST or brainpool curves with ML-KEM and ML-DSA. The final set of code-points to allocate is still under discussion in the WG, though discussions are close to complete. This draft is primarily motivated by anticipated regulatory requirements to support those curves.

2.5 HPKE

RFC 9180 [22] defines a "Hybrid Public Key Encryption" (HPKE) format that is used by TLS for Encrypted ClientHello (ECH) [23] and by the Message Layer Security (MLS) protocol [24] which provides primitives intended to be used in instant-messaging group communications, such as those being defined in the IETF's MIMI WG.[2] Note that the word "hybrid" in HPKE is used in a different sense than when generally used in a PQ context - "hybrid" in this case means using a KEM, a KDF and a symmetric cipher to encrypt a possibly-large application-layer message or other protocol artefact "to" a public key. The HPKE WG is chartered to add PQ KEMs to the list of those available, and its charter specifically calls for both hybrids (in the PQ sense) with ML-KEM, and "pure" ML-KEM options to be added.

As HPKE is a lower level construct, the simple "concatenation" combiner used in e.g., TLS hybrid KEMs might not be sufficiently secure given that the HPKE format could be used in various protocols that might not provide such good cryptographic binding between the various protocol artefacts, so the WG draft [25] defining new HPKE KEMs has a dependency on the more generic work being done on KEM combiners in CFRG (see Sections 2.14, and 3.5). The work in the HPKE WG has been so-far uncontroversial amongst the set of participants involved, and so will likely be completed soon after the related CFRG document [26] is finished. (Though it remains possible that the IETF last-call could prove controversial due to enabling "pure" PQ KEMs.)

2.6 LAMPS

The LAMPS WG maintains X.509-based PKI specifications flowing from RFC 5280 [27] and the Cryptographic Message Syntax (CMS) [28] used by S/MIME [29] and some other IETF protocols.[3] LAMPS has many drafts and some RFCs related to PQ topics.

RFC 9708 [30] defines how to use the LMS hash-based signing algorithm for CMS and RFC 9802 [31] does the same work for X.509 PKIs. The author is unaware of implementations or deployments of those, but given that there are many uses of S/MIME and X.509-based PKI that are for enterprise networks or other internal uses, possibly within government networks, there could well be some.

There is a cluster of LAMPS adopted Internet-drafts and a couple of RFCs defining how to use "pure" ML-KEM, ML-DSA and SLH-DSA, in both CMS and X.509-based PKIs that mainly register algorithm ASN.1 Object Identifier (OID)s, public key formats and related structures (e.g. S/MIME capabilities) and sometimes other protocol numbers (e.g. keyUsage bits) for the relevant algorithms [32, 33, 34, 35, 36]. RFC 9814 [37] defines how to use SLH-DSA with CMS, and RFC 9629 [38] defines how to use KEMs (in general) with CMS. Documents in this cluster are at different levels of advancement in the IETF process, but many are reaching the stage where they will soon be at or beyond IETF last call. In many cases, these drafts deal with multiple different strengths/lengths for the algorithms (see also Section 3.4).

One of the obvious ideas to consider for a PQ transition for X.509-based PKI is to use hybrid signatures. (Whether or not this is a good idea is another matter.) A LAMPS

[2] See https://datatracker.ietf.org/wg/mimi/about/

[3] When it was originally formed the "Limited" in the name and charter was intended to discourage scope-creep and never-ending updates, but that is not how things have evolved, sadly.

draft [39] aims to enable this by defining hybrids of ML-DSA (3 strengths) with each of RSASSA-PKCS1-v1.5 (3072 and 4096), RSASSA-PSS (3071 and 4096), ECDSA (p256, p384 and p521) Ed25519, and Ed448. That adds up to a total of 18 new signature algorithm identifiers. There is also some generic disagreement about the desirable properties of hybrid signature schemes, for example related to Existential Unforgeability under Chosen Message Attack (EUF-CMA) and Strong Unforgeability under Chosen Message Attack (SUF-CMA), basically reducing to whether or not it is acceptable for a single message to have multiple valid signatures under the same signing key. So this draft also says: "Composite ML-DSA is NOT RECOMMENDED for use in applications where it is has not been shown that EUF-CMA is acceptable." That is on the basis that the scheme proposed is not SUF-CMA in the presence of a CRQC, thus quite possibly motivating a very recently posted personal draft aimed at CFRG [40]. The LAMPS draft [39] has passed WGLC and will likely soon proceed to IETF last-call, unless the new CFRG approach quickly becomes a more attractive alternative.

Another draft [41] defining hybrids for ML-KEM with any of RSA-OAEP, ECDH, X25519, and X448, takes the same define-lots-of-options approach and by not quite doing every possible option creates 12 hybrid KEM options. None of these hybrid KEMs use the KEM combiners being developed by CFRG. This draft has yet to reach WGLC.

It seems noteworthy that those last two drafts alone define 30 new algorithm identifiers - including the earlier cluster this WG alone must be approaching adding 50 new algorithm identifiers to generic cryptographic libraries. (See also Section 3.4.)

In many cases these documents also define private key formats and have struggled with the problem of how to represent private keys when there is both a KeyGen() and a KeyGen(seed) interface defined, and where not all libraries or devices might support both. (See also Section 3.6.)

2.7 MLS

The MLS protocol is designed to provide a standardised security layer suited for achieving interoperability for group instant messaging. The MLS protocol uses HPKE so should inherit PQ features once those are deployed. In addition, the WG has two PQ drafts, one [42] defining 7 new MLS cipher-suites, three as hybrid KEMs that are combinations of ML-KEM with X25519, P256 and P384, and four that are "pure" ML-KEM cipher-suites. Five of these suites are intended to be paired with traditional signing algorithms (Ed25519 or ECDSA variants) while two are intended to be paired with ML-DSA. This draft is essentially mapping code-points from MLS to HPKE.

Another draft [43] describes an MLS-specific way to amortize the cost of PQ operations via the use of exporters. The idea is to run two MLS sessions with the same group, the first of which uses PQ algorithms, to export a key from that and use that key as a Pre-Shared (symmetric) Key (PSK) in the second MLS session. The benefit should be overhead reductions if the PQ session can be updated less frequently.

Both MLS drafts are still being processed within the WG.

2.8 IPSECME

The IPSECME WG maintains the IP Security Extensions (IPsec) protocol and has ongoing work on PQ topics. RFC 8784 [44], from 2020, defines a way to use a "Post Quantum

Pre-Shared Key" (PPK), shared out-of-band between the parties and assumed to not be vulnerable to a CRQC, in order to increase the security of an Internet Key Exchange (IKE) exchange. [4]There is also a current WG draft [45] that enhances that PPK protection to allow mixing of new PPKs into active security associations.

RFC 9370 [46] defines a way to do additional key exchanges in IKE, so that a PQ KEM can be used after a traditional ECDH exchange, resulting in a hybrid PQ/T KEM, with the final shared secret being based on all of the component key exchange secrets. There is a WG draft [47] defining how to use ML-KEM in this manner, as the "first used" KEM in a hybrid comnbination, instead of e.g. X25519. That draft defines how to use ML-KEM512 for the initial key exchange if a "pure" PQ KEM is desired, but, based on sizes, recommends against use of ML-KEM768 for this purpose.

There are personal drafts defining how to do the same thing with FrodoKEM, [48] Classic McElliece, [49] and NTRU. [50]

There is a WG draft [51] on how to use ML-DSA or SLH-DSA for authentication that defines 15 variants of those algorithms for use as a "pure" PQ signature authentication mechanism.

There is also a personal draft [52] defining how to use the hybrid signature schemes specified in the LAMPS composite signatures draft [39], and that may sometimes also depend on RFC 9763 [53] to handle cases where the relevant public keys are present in individual X.509 certificates. This draft seems to be at an early stage and the authors are unclear as to how it is perceived in the IPSECME WG.

2.9 DNSOP

The DNSOP WG maintains the Domain Name System (DNS) protocol and considers general operational issues related to the DNS protocol and services built on that. The DNSOP WG as yet has not adopted any work on PQ signatures for DNS Security Extensions (DNSSEC). There have been informal discussions on the topic [5] in "side-meetings" at recent IETF meetings, but as this is quite a hard problem, it is unclear what approaches to take. There have been some personal drafts that considered the topic [54, 55] - the first of those is an expired draft (from early 2025) that sets out a "research agenda" for the topic, which perhaps indicates the level of maturity in this space. The second describes an SLH-DSA signing scheme that uses Merkle trees based on a personal draft being proposed for adoption by CFRG. [56] As such a scheme would be far from a drop-in replacement for current DNSSEC signature validation, it would likely be quite some time before it would be mature. (There are also some not-too-onerous looking IPR declarations filed on both drafts.)

There is also another strategy draft [57] that was discussed at the DNSOP WG session at IETF-124 (`https://datatracker.ietf.org/meeting/124/proceedings`). This draft proposes a path forward similar to the above, to continue work on the Merkle-tree ideas, but to also investigate NIST "onramp" signature algorithms such as MAYO [6].

[4] IKE is the IPsec equivalent of the TLS handshake protocol that may be more familiar to some readers.

[5] See `https://wiki.ietf.org/en/group/pq-dnssec`.

[6] `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/mayo-spec-web.pdf`

2.10 JOSE and COSE

The JOSE and COSE WGs develop quite similar cryptographic specifications for JSON and CBOR encodings of application data, with a fair degree of functional and participant overlap, so are discussed together here. As one might guess, JOSE deals with JSON and COSE deals with CBOR - and the specifications deal with cryptographic formats (encryption artefacts, signatures etc.) for those data representations. The results include so-called JSON Web Tokens (JWTs) that are widely used in systems that make use of OAuth. CBOR, as a more compressed encoding, sees similar outputs used in applications for constrained devices.

The JOSE WG has a WG draft [58] defining PQ KEMs for JOSE and COSE that defines "pure" usage of ML-KEM's 3 strengths with or without key wrapping, so a total of six algorithm code-points.

A personal draft [59] describes how to use hybrid KEMs via use of HPKE in JOSE or COSE. HPKE is mapped to JOSE [60] and COSE [61] in two confusingly similar WG drafts.

There are also COSE WG drafts specifying how to use ML-DSA [62], FN-DSA [63] and SLH-DSA [62] for both JOSE and COSE with a total of 8 new algorithm identifiers for each.

The above drafts only support the "seed" variant ML-KEM/ML-DSA private key format. (See Section 3.6.)

2.11 LAKE

The LAKE WG's main product is the Ephemeral Diffie-Hellman Over COSE (EDHOC) protocol, [64] which can be considered a highly byte-optimised equivalent to TLS, intended for use in networks where bandwidth (and other) constraints are much more significant than on the general Internet.

As with IPsec, there is a WG draft [65] that specifies how to use an out-of-band distributed PSK to provide quantum resistance. The draft also notes that, in the face of a CRQC, not all protocol security features survive (e.g. identity protection) despite the use of a PSK.[7] A personal draft [66] specifies how to use PQ algorithms with EDHOC, including ML-DSA for authentication and ML-KEM for key distribution. This re-uses the COSE PQ work referenced above.

EDHOC was specifically designed to minimise the number of bytes transmitted, and PQ signatures or KEMs basically seem to destroy those efficiencies, so it would seem that it would be wise to revisit the requirements [8] that gave rise to EDHOC. One would wonder if the size of the PQ artefacts means that devices, even in constrained networks, may as well use PQ features of TLS and no longer benefit significantly from the efficiencies of EDHOC.

[7] This specification is currently "frozen" until about March 2026 at draft-06 in order to allow time for formal analyses to be done. This WG tends to do this for core specifications such as this one. The TLS WG does similarly for anything affecting the keys derived in the handshake. See https://mailarchive.ietf.org/arch/msg/lake/A4YOMyFDQunzYDVSlsjt_C6yaRE/ for details.

[8] The author was a co-chair of the LAKE WG when it developed a WG draft [67] capturing requirements, with the plan being to reach rough consensus on the requirements, but to not publish the WG draft as an RFC.

2.12 SIDROPS

The Resourece PKI (RPKI) protocol aims to improve the security of the Border Gateway Protocol (BGP), via digitally signed objects that bind Autonomous System (AS) numbers to addresses with a PKI that chains up to a Certification Authority (CA) operated by a Regional Internet Registry (RIR). Thus far there are no PQ drafts related to this activity, and an active IETF participant in this space has informed the author that the RPKI community are not yet considering the CRQC threat. This seems sensible, and this WG is included here as one of the many examples of things that are quite reasonably not yet considering that threat.

2.13 KITTEN

The KITTEN WG's name is not an acronym, its precursor was the Common Authentication Technology (CAT) WG, and kittens are the offspring of cats. The WG maintains the specifications for the Kerberos and SASL protocols and some related RFCs. There are currently no PQ drafts for this WG, but recently one participant asked on the mailing list whether there were any plans for considering the impact of a CRQC on the Kerberos PKINIT mechanism. The response was to the effect that a draft on using PQ KEMs with Kerberos may be forthcoming in future. (See https://mailarchive.ietf.org/arch/msg/kitten/n98sw1dKr7JmJ6gY2CZ8gZp2WLQ/.)

2.14 CFRG

The CFRG is not a part of the IETF, but is rather a research group (RG) in the IRTF.[9] CFRG is an unusual RG in that it acts to serve as a bridge between theory and practice and provides advice to IETF WGs and also develops specifications where significant cryptographic expertise is needed that is often not available amongst the set of active participants in an IETF WG. CFRG is also useful as a venue where academic cryptographers can interact with protocol designers and implementers. It is therefore natural that multiple IETF WGs depend on work in CFRG when it comes to PQ issues.

In 2018 CFRG produced RFC 8391 [68] which defines the XMSS stateful hash-based signature scheme, followed by another (LMS) in RFC 8554 [69] in 2019. While both schemes are believed secure, as stateful hash-based signatures, they come with significant deployment challenges, so are not suited for use in many IETF protocols.

CFRG work on PQ/T hybrid KEM combiners has been slow and somewhat controversial (see also Section 3.5), with various generic and more specific proposals having been made, some being documented as quite generic KEM combiners, [70] and others being very specific [71] and tied to a specific hybrid KEM. In early 2024 the CFRG chairs created a design team[10] to try to agree on a plan of action for CFRG to handle this topic. The eventual result was two CFRG documents, one defining generic KEM combiner constructions [72] and another [26] defining three hybrid KEMs (currently named MLKEM768-P256, MLKEM768-X25519 and MLKEM1024-P384) that can be used in IETF protocol documents such as [25].

[9] There are 15 other RGs, but to the author's knowledge, none of those are currently working explicitly on PQ topics.

[10] The author was a member of that design team.

Very recently, there are early signs that a similar process may be needed with respect to combiners for hybrid signature schemes as two personal Internet-drafts [40, 73] targeting CFRG have been published, perhaps partly in reaction to a LAMPS WG draft (See Section 2.6) on composite signatures for use in X.509 PKI [39] being on the cusp of reaching the stage of IETF last-call.

There are also other personal drafts targeting CFRG specifying FrodoKEM [74] and an NTRU based KEM [75], one setting out some security considerations related to use of ML-KEM [76], and a very recent one on combining multiple input keys to produce one output key [77]. The future progress (or lack thereof) of all of those is unclear.

Otherwise, there are many CFRG drafts at various process stages that may over time be extended to consider a CRCQ in their threat models - many do not at this time - or for which the existence of a CRQC is not relevant.

Chapter 3

Issues and points of disagreement

This chapter describes issues and point of disagreement that recur in multiple WGs as PQC topics are discussed.

3.1 Immediacy

There is very broad agreement that countering the "harvest-now-decrypt-later" attack is something to address immediately. There is much less agreement, and much less clarity, when it comes to countering the authentication challenges that would be raised were there a CRQC. However, there are a significant number of IETF participants who do argue we ought try tackle this issue immediately. For example, section 1.2.2 of the LAMPS WG "composite signatures" draft [3] includes a justification for "immediate post-quantum algorithm selection" The problem with that justification is that it seems to only apply to deployments where:

- One must pick signature (verification) algorithms today that cannot be changed for the lifetime of the device, and,
- Those devices are likely to still be deployed when a CRQC is available

The problem with this characterisation is that it elevates a niche into what is claimed to be a common scenario, potentially causing systems that can benefit from further research and engineering to be prematurely deployed, with bugs, leading to a loss of security/privacy.

For example, it is not clear that good PQ algorithm choices can be made before we have credible transition plans for web or mail servers, for the Automated Certificate Management Environment (ACME) protocol and for handling PKI, and we don't as yet, have those credible plans worked out.

3.2 How to document cryptographic algorithms

The IETF doesn't develop new cryptographic algorithms and hence algorithms are generally documented in externally referenced documents. But sometimes those are pay-walled, or not in English, or aren't suitable for implementers, and in those cases, having an RFC that describes the algorithm can be useful, e.g. RFC 8032 [78] describes the EdDSA signature algorithm in a form much more suited for implementers than the original academic papers.

There are also sometimes national cryptographic standards that implementers of IETF protocols need to support, e.g. RFC 8734 [79] documents the use of the German "brainpool" curves in TLSv1.3. In other cases protocol code-points are allocated without there being an RFC to document their use, e.g. the "X25519Kyber768Draft00" HPKE kem_id is defined in draft-02 of an expired Internet-draft [80] (for which a draft-03 also exists!) and that is perhaps unlikely to become an RFC in future as Kyber has been superceded by ML-KEM. In theory, any sufficiently stable reference could be used rather than documenting the algorithm in an RFC. Historically, some algorithm RFCs have also been processed via the Independent submissions route as the IETF didn't really have change-control over their content, e.g. RFC 3174 [81].

Some participants consider that documenting an algorithm with an RFC indicates a level of IETF approval of that algorithm and so, should, or shouldn't, be done, depending on their opinion of the algorithm. Other participants support, or oppose, the viewpoint that for Internet Assigned Numbers Authority (IANA) registries where an RFC is not absolutely required, then it's better to use some other stable reference (such as a specifically numbered Internet-draft) and avoid the additional work of producing an RFC.

There are additional issues around the level of support desired for an algorithm - in some cases protocols will require implementation of some mandatory-to-implement (MTI) set of algorithms, or may indicate that some algorithm is or is not recommended to be implemented, or that an algorithm should be deprecated. Those indicators may be embedded in RFC text, or may be specified in an IANA registry, or both. Again, cases where participants do or do not like an algorithm cause friction in making or changing such recommendations.

In the PQ space, we additionally have the following aspects, where sets of IETF participants have conflicting opinions as to the consequences of the following:

- whether or not a PQ algorithm is a NIST PQC "winner"
- whether or not a PQ algorithm is required (or suspected or claimed to be required) to meet some regulatory regime
- whether or not some hybrid combination is favoured by cryptographers, implementers or regulators, and which
- whether or not there is sufficient confidence in some "pure" PQ algorithm proposal

This all leads to controversy, especially as different sets of IETF participants take different positions on the above points. The SSH NTRU Prime hybrid [6] was a case that involved most of these points of contention, but similar issues have arisen and will continue to arise in other working groups.

3.3 Fears of another Dual-EC

The "Dual-EC" [82] fiasco, where the NSA and NIST published a (subsequently retracted) US standard for a random number generator that produced values that were predictable by a party holding the keys to the backdoor, has left some people extremely wary of the concept of using any "pure" KEM defined (essentially) under the control of those same entities, such as ML-KEM. (This concern generalises to other nationally standardised PQ KEMs.) The Dual-EC fiasco seems to have involved the US government paying companies to include the broken

random number generator in then-popular cryptographic libraries [83], VPN code-bases that seem to have been modified to make exploitation of Dual-EC easier [84] (and were further modified by unknown entities who changed the backdoor keys), and there seem to have been failed attempts to modify IETF protocols to similarly ease exploitation [85].

Based on all the above, some IETF participants have expressed worries that encouraging use of "pure" KEMs might represent a repeat of that kind of tactic as part of some campaign to subvert uses of cryptography, especially given the demonstrated PQ KEM implementation bugs [86], which make it extremely hard to understand a justification for not recommending hybrid KEMs for safety.

There are also concerns that new cryptanalytic results might weaken e.g. ML-KEM sufficiently that using the "pure" PQ KEM approach could later turn out to be unwise, and an earlier hybrid KEM experiment that used a later-broken PQ-KEM [87] is offered as an example of how use of a "pure" PQ-KEM could be devastating.

The above arguments are part of the substance of the plethora of appeals (see `https://datatracker.ietf.org/group/iesg/appeals/` for the state of those) that have been submitted related to the relevant TLS draft. [13] Some of these issues were also raised during the processing of SSHM WG drafts, and one might expect that, should they not be resolved in some general manner, these objections will continue to be raised.

At the time of writing it is unclear if any of these appeals will have any substantive effect, other than annoying many IETF participants.[1] That said, the set of IETF participants who have actively expressed the above concerns is, while small, non-negligible. There are also some (perhaps a larger number of) IETF participants who have explicitly said that they do not share the above concerns. And lastly, there is so far, no indication that adoption of "pure" PQ KEMs will be widespread.

3.4 Combinatorics

Between all the new algorithms, strength-levels, hybrid options and protocols above, there must be more than 100 new options being defined that may be added to any general cryptographic protocol library. If we assume 300 Lines of code (LoC) for each new cryptographic option (including configuration choices) that amounts to an estimated 30kLoC, almost all of which will be rarely or never used. That is a fine recipe for bugs and vulnerabilities.

Aside from the potential for bugs and vulnerabilities, having too many options also causes security, interop and portability problems. For any given protocol, if there is no MTI PQ algorithm (which is likely as these are too new), and if there are many options then that increases the probability that two protocol participants do not have a common PQ algorithm and so may fall back to use of only traditional key exchanges thus being vulnerable to a CRQC. Or perhaps the two protocol peers might just not have any algorithms in common and simply won't interop. Lastly, different packages will support different sets of algorithms and if e.g. a server has existing keys deployed, then one can only replace the server software with those packages that also support the relevant algorithm(s) and the more choices there are, the more likely that this restricts the usable packages.

A general cryptographic agility goal may be to have, for each purpose, one "primary" algorithm/suite widely deployed and used, and have a second (ideally with some "distance"

[1] The annoyance is, in the author's opinion, caused by the appeals being littered with unfounded process appeal points that are nothing but distractions.

between the two) also widely deployed so we can switch if needed. It should never be a goal to have 15 alternatives, yet that is what we are currently doing in the PQ space.

3.5 KEM Combiners

When considering hybrid KEMs, the issue of how to combine the outputs from the traditional (ECDH) and PQ KEM components, before feeding the combined value into e.g. a KDF, needs an answer. Simple concatenation of the output secret values can work in some contexts (e.g. TLS) but in others, this could lead to security issues, or at least with problems in proving the security features provided by the hybrid construct. This leads to a desire to include e.g. public values, lengths, context strings and other inputs in the combined value that gets fed into a KDF, possibly hashing some of the values before generating the KDF input. All in all, this creates many potential KEM combiners, with there being no "always-best" answer given the different protocols for which KEM combiners are required, for example issues related to efficiency if multiple hash function calls are required have been raised and debated without reaching an obviously good conclusion.

3.6 Seeds

Some of the NIST PQ "winner" algorithms support two variants for a private key format - one where the private values can be (re-)generated from a seed value, and another where the structured private key values are generated/stored independently. As with virtually all degrees of cryptographic "freedom" this causes problems. Specifically, an implementation that only supports seeds can't usefully be presented with a structured private key. The opposite is less true, if the seed -> structured private key mechanism is well-defined. The different possibilities also lead to issues with portability of private keys between different implementations. And it seems that even though both forms of private key are defined in NIST documents, they may not be equal when it comes to FIPS conformance. (Though that may change or may be inaccurate.) Open-source software developers have also made their choices in terms of what they will support here, and some of those were in conflict with the choices that IETF protocol designers had made at the time. (And sadly, the debate as to how to structure a choice between seeds or structured private keys was lengthy, contentious and uninformative - common enough when the stakes are so low.)

Chapter 4

Interim conclusions and state of play

To conclude, some of the IETF work on PQ topics is mature and has already been widely deplpoyed, but many significant details remain in flux. And those details count, the landscape for those deploying systems and services using IETF protocols, who are concerned about PQ authentication can at best be described as "confused".

It would seem (to this auhtor) that the "harvest-now-decrypt-later" issue is the proper place on which to focus efforts, and so to encourage specifications, implementatons and deployments that aim to mitigate that particular attack.

Bibliography

[1] F. Driscoll, M. Parsons, and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes," RFC 9794 (Informational), RFC Editor, Fremont, CA, USA, Jun. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9794.txt

[2] A. Banerjee, T. Reddy.K, D. Schoinianakis, T. Hollebeek, and M. Ounsworth, "Post-Quantum Cryptography for Engineers," Internet Engineering Task Force, Internet-Draft draft-ietf-pquip-pqc-engineers-14, Aug. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers-14

[3] N. Bindel, B. Hale, D. Connolly, and F. D, "Hybrid signature spectrums," Internet Engineering Task Force, Internet-Draft draft-ietf-pquip-hybrid-signature-spectrums-07, Jun. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums-07

[4] T. Reddy.K, D. Wing, B. S, and K. Kwiatkowski, "Adapting Constrained Devices for Post-Quantum Cryptography," Internet Engineering Task Force, Internet-Draft draft-ietf-pquip-pqc-hsm-constrained-02, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-hsm-constrained-02

[5] T. Wiggers, K. Bashiri, S. Kölbl, J. Goodman, and S. Kousidis, "Hash-based Signatures: State and Backup Management," Internet Engineering Task Force, Internet-Draft draft-ietf-pquip-hbs-state-01, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-hbs-state-01

[6] M. Friedl, J. Mojzis, and S. Josefsson, "Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512," Internet Engineering Task Force, Internet-Draft draft-ietf-sshm-ntruprime-ssh-06, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-sshm-ntruprime-ssh-06

[7] P. Kampanakis, D. Stebila, and T. Hansen, "PQ/T Hybrid Key Exchange with ML-KEM in SSH," Internet Engineering Task Force, Internet-Draft draft-ietf-sshm-mlkem-hybrid-kex-04, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-sshm-mlkem-hybrid-kex-04

[8] S. Josefsson, "Stateless Hash-Based Signatures for Secure Shell (SSH)," Internet Engineering Task Force, Internet-Draft draft-josefsson-ssh-sphincs-01, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-ssh-sphincs-01

[9] ——, "Secure Shell Key Exchange Method Using Chempat Hybrid of Classic McEliece and X25519 with SHA-512: mceliece6688128x25519-sha512," Internet Engineering Task Force, Internet-Draft draft-josefsson-ssh-mceliece-02, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-ssh-mceliece-02

[10] A. Harrison, A. Benhase, and P. Kampanakis, "Module-Lattice Key Exchange in SSH," Internet Engineering Task Force, Internet-Draft draft-harrison-sshm-mlkem-00, Jun. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-harrison-sshm-mlkem-00

[11] D. Stebila, S. Fluhrer, and S. Gueron, "Hybrid key exchange in TLS 1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-hybrid-design-16, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design-16

[12] K. Kwiatkowski, P. Kampanakis, B. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-ecdhe-mlkem-03, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem-03

[13] D. Connolly, "ML-KEM Post-Quantum Key Agreement for TLS 1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-mlkem-05, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem-05

[14] R. Salz and N. Aviram, "TLS 1.2 is in Feature Freeze," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-tls12-frozen-08, Apr. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-tls12-frozen-08

[15] D. Benjamin and A. Popov, "Legacy RSASSA-PKCS1-v1_5 codepoints for TLS 1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-tls13-pkcs1-06, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-tls13-pkcs1-06

[16] T. Reddy.K, T. Hollebeek, J. Gray, and S. Fluhrer, "Use of Composite ML-DSA in TLS 1.3," Internet Engineering Task Force, Internet-Draft draft-reddy-tls-composite-mldsa-05, Jul. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-reddy-tls-composite-mldsa-05

[17] S. Kousidis, J. Roth, F. Strenzke, and A. Wussler, "Post-Quantum Cryptography in OpenPGP," Internet Engineering Task Force, Internet-Draft draft-ietf-openpgp-pqc-14, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-openpgp-pqc-14

[18] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," RFC 4880 (Proposed Standard), RFC Editor, Fremont, CA, USA, Nov. 2007, obsoleted by RFC 9580, updated by RFC 5581. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4880.txt

[19] P. Wouters (Ed.), D. Huigens, J. Winter, and Y. Niibe, "OpenPGP," RFC 9580 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jul. 2024. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9580.txt

[20] W. Koch and R. Tse, "LibrePGP Message Format," Internet Engineering Task Force, Internet-Draft draft-koch-librepgp-04, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-koch-librepgp-04

[21] Q. Dang, S. Ehlen, S. Kousidis, J. Roth, and F. Strenzke, "PQ/T Composite Schemes for OpenPGP using NIST and Brainpool Elliptic Curve Domain Parameters," Internet Engineering Task Force, Internet-Draft draft-ietf-openpgp-nist-bp-comp-02, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-openpgp-nist-bp-comp-02

[22] R. Barnes, K. Bhargavan, B. Lipp, and C. Wood, "Hybrid Public Key Encryption," RFC 9180 (Informational), RFC Editor, Fremont, CA, USA, Feb. 2022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9180.txt

[23] E. Rescorla, K. Oku, N. Sullivan, and C. Wood, "TLS Encrypted Client Hello," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-25, Jun. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni-25

[24] W. Roome, S. Randriamasy, Y. Yang, J. Zhang, and K. Gao, "An Extension for Application-Layer Traffic Optimization (ALTO): Entity Property Maps," RFC 9240 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jul. 2022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9240.txt

[25] R. Barnes and D. Connolly, "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE," Internet Engineering Task Force, Internet-Draft draft-ietf-hpke-pq-03, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-hpke-pq-03

[26] D. Connolly and R. Barnes, "Concrete Hybrid PQ/T Key Encapsulation Mechanisms," Internet Engineering Task Force, Internet-Draft draft-irtf-cfrg-concrete-hybrid-kems-02, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-concrete-hybrid-kems-02

[27] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," RFC 5380 (Proposed Standard), RFC Editor, Fremont, CA, USA, Oct. 2008. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5380.txt

[28] R. Housley, "Cryptographic Message Syntax (CMS)," RFC 5652 (Internet Standard), RFC Editor, Fremont, CA, USA, Sep. 2009, updated by RFCs 8933, 9629. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5652.txt

[29] J. Schaad, B. Ramsdell, and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification," RFC 8551 (Proposed Standard), RFC Editor, Fremont, CA, USA, Apr. 2019, updated by RFC 9788. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8551.txt

[30] R. Housley, "Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS)," RFC 9708 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jan. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9708.txt

[31] D. V. Geest, K. Bashiri, S. Fluhrer, S. Gazdag, and S. Kousidis, "Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure," RFC 9802 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jun. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9802.txt

[32] B. S, A. R, and D. Geest, "Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-cms-ml-dsa-07, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-ml-dsa-07

[33] J. Massimo, P. Kampanakis, S. Turner, and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-dilithium-certificates-13, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates-13

[34] P. Julien, M. Ounsworth, and D. Geest, "Use of ML-KEM in the Cryptographic Message Syntax (CMS)," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-cms-kyber-13, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kyber-13

[35] S. Turner, P. Kampanakis, J. Massimo, and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-kyber-certificates-11, Jul. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates-11

[36] K. Bashiri, S. Fluhrer, S. Gazdag, D. Geest, and S. Kousidis, "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-x509-slhdsa-09, Jun. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-x509-slhdsa-09

[37] R. Housley, S. Fluhrer, P. Kampanakis, and B. Westerbaan, "Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)," RFC 9814 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jul. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9814.txt

[38] R. Housley, J. Gray, and T. Okubo, "Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS)," RFC 9629 (Proposed Standard), RFC Editor, Fremont, CA, USA, Aug. 2024. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9629.txt

[39] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-sigs-13, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs-13

[40] L. Prabel, G. WANG, J. Janneck, T. Reddy.K, and J. Mattsson, "Hybrid Digital Signatures with Strong Unforgeability," Internet Engineering Task Force, Internet-Draft draft-prabel-cfrg-suf-hybrid-sigs-00, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-prabel-cfrg-suf-hybrid-sigs-00

[41] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, "Composite ML-KEM for use in X.509 Public Key Infrastructure," Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-kem-10, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem-10

[42] R. Mahy and R. Barnes, "ML-KEM and Hybrid Cipher Suites for Messaging Layer Security," Internet Engineering Task Force, Internet-Draft draft-ietf-mls-pq-ciphersuites-01, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-pq-ciphersuites-01

[43] X. Tian, B. Hale, M. Mularczyk, and Joël, "Amortized PQ MLS Combiner," Internet Engineering Task Force, Internet-Draft draft-ietf-mls-combiner-02, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-combiner-02

[44] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security," RFC 8784 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jun. 2020. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8784.txt

[45] V. Smyslov, "Mixing Preshared Keys in the IKE_INTERMEDIATE and in the CREATE_CHILD_SA Exchanges of IKEv2 for Post-quantum Security," Internet Engineering Task Force, Internet-Draft draft-ietf-ipsecme-ikev2-qr-alt-10, May 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-qr-alt-10

[46] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. V. Geest, O. Garcia-Morchon, and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9370 (Proposed Standard), RFC Editor, Fremont, CA, USA, May 2023. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9370.txt

[47] P. Kampanakis, "Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)," Internet Engineering Task Force, Internet-Draft draft-ietf-ipsecme-ikev2-mlkem-03, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-mlkem-03

[48] G. WANG, L. Bruckert, and V. Smyslov, "Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM," Internet Engineering Task Force, Internet-Draft draft-wang-ipsecme-hybrid-kem-ikev2-frodo-02, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-wang-ipsecme-hybrid-kem-ikev2-frodo-02

[49] V. Smyslov and Y. Nir, "Using Classic McEliece in the Internet Key Exchange Protocol Version 2 (IKEv2)," Internet Engineering Task Force, Internet-Draft draft-smyslov-ipsecme-ikev2-mceliece-01, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-smyslov-ipsecme-ikev2-mceliece-01

[50] Y. Fukagawa, H. Kosuge, M. Saito, S. Fluhrer, and A. Nagai, "Post-quantum Hybrid Key Exchange with NTRU in the Internet Key Exchange Protocol Version 2 (IKEv2)," Internet Engineering Task Force, Internet-Draft draft-skyline-ipsecme-ntru-ikev2-00, Jul. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-skyline-ipsecme-ntru-ikev2-00

[51] T. Reddy.K, V. Smyslov, and S. Fluhrer, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC," Internet Engineering Task Force, Internet-Draft draft-ietf-ipsecme-ikev2-pqc-auth-06, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-pqc-auth-06

[52] J. Hu, Y. Morioka, and G. WANG, "Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in the Internet Key Exchange Version 2 (IKEv2)," Internet Engineering Task Force, Internet-Draft draft-hu-ipsecme-pqt-hybrid-auth-03, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth-03

[53] A. Becker, R. Guthrie, and M. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol," RFC 9763 (Proposed Standard), RFC Editor, Fremont, CA, USA, Jun. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9763.txt

[54] A. Fregly, R. Rijswijk-Deij, M. Müller, P. Thomassen, C. Schutijser, and T. Chung, "Research Agenda for a Post-Quantum DNSSEC," Internet Engineering Task Force, Internet-Draft draft-fregly-research-agenda-for-pqc-dnssec-02, Dec. 2024, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-fregly-research-agenda-for-pqc-dnssec-02

[55] A. Fregly, J. Harvey, B. Kaliski, and D. Wessels, "Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC," Internet Engineering Task Force, Internet-Draft draft-fregly-dnsop-slh-dsa-mtl-dnssec-05, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-fregly-dnsop-slh-dsa-mtl-dnssec-05

[56] J. Harvey, B. Kaliski, A. Fregly, S. Sheth, and D. McVicker, "Merkle Tree Ladder (MTL) Mode Signatures," Internet Engineering Task Force, Internet-Draft draft-harvey-cfrg-mtl-mode-08, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode-08

[57] S. Sheth, T. Chung, and B. Overeinder, "Post-Quantum Cryptography Strategy for DNSSEC," Internet Engineering Task Force, Internet-Draft draft-sheth-pqc-dnssec-strategy-00, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-sheth-pqc-dnssec-strategy-00

[58] T. Reddy.K, A. Banerjee, and H. Tschofenig, "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE," Internet Engineering Task Force, Internet-Draft draft-ietf-jose-pqc-kem-04, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-jose-pqc-kem-04

[59] T. Reddy.K and H. Tschofenig, "PQ/T Hybrid KEM: HPKE with JOSE/COSE," Internet Engineering Task Force, Internet-Draft draft-reddy-cose-jose-pqc-hybrid-hpke-08, Jul. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-reddy-cose-jose-pqc-hybrid-hpke-08

[60] T. Reddy.K, H. Tschofenig, A. Banerjee, O. Steele, and M. Jones, "Use of Hybrid Public Key Encryption (HPKE) with JSON Object Signing and

Encryption (JOSE)," Internet Engineering Task Force, Internet-Draft draft-ietf-jose-hpke-encrypt-14, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-jose-hpke-encrypt-14

[61] H. Tschofenig, O. Steele, Ajitomi, Daisuke, and L. Lundblade, "Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)," Internet Engineering Task Force, Internet-Draft draft-ietf-cose-hpke-18, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cose-hpke-18

[62] M. Prorock, O. Steele, and H. Tschofenig, "SLH-DSA for JOSE and COSE," Internet Engineering Task Force, Internet-Draft draft-ietf-cose-sphincs-plus-06, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus-06

[63] ——, "FN-DSA for JOSE and COSE," Internet Engineering Task Force, Internet-Draft draft-ietf-cose-falcon-03, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cose-falcon-03

[64] G. Selander, J. P. Mattsson, and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)," RFC 9528 (Proposed Standard), RFC Editor, Fremont, CA, USA, Mar. 2024. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9528.txt

[65] E. Lopez-Perez, G. Selander, J. Mattsson, R. Marin-Lopez, and F. Lopez-Gomez, "EDHOC Authenticated with Pre-Shared Keys (PSK)," Internet Engineering Task Force, Internet-Draft draft-ietf-lake-edhoc-psk-06, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lake-edhoc-psk-06

[66] G. Selander and J. Mattsson, "Quantum-Resistant Cipher Suites for EDHOC," Internet Engineering Task Force, Internet-Draft draft-spm-lake-pqsuites-01, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-spm-lake-pqsuites-01

[67] M. Vučinić, G. Selander, J. Mattsson, and D. Garcia-Carillo, "Requirements for a Lightweight AKE for OSCORE," Internet Engineering Task Force, Internet-Draft draft-ietf-lake-reqs-04, Jun. 2020, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lake-reqs-04

[68] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme," RFC 8391 (Informational), RFC Editor, Fremont, CA, USA, May 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8391.txt

[69] D. McGrew, M. Curcio, and S. Fluhrer, "Leighton-Micali Hash-Based Signatures," RFC 8554 (Informational), RFC Editor, Fremont, CA, USA, Apr. 2019. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8554.txt

[70] S. Josefsson, "Chempat: Generic Instantiated PQ/T Hybrid Key Encapsulation Mechanisms," Internet Engineering Task Force, Internet-Draft draft-josefsson-chempat-04, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-chempat-04

[71] D. Connolly, P. Schwabe, and B. Westerbaan, "X-Wing: general-purpose hybrid post-quantum KEM," Internet Engineering Task Force, Internet-Draft draft-connolly-cfrg-xwing-kem-09, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-connolly-cfrg-xwing-kem-09

[72] D. Connolly, R. Barnes, and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms," Internet Engineering Task Force, Internet-Draft draft-irtf-cfrg-hybrid-kems-07, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-hybrid-kems-07

[73] S. Josefsson, "Mothma: Generic Instantiated PQ/T Hybrid Signatures," Internet Engineering Task Force, Internet-Draft draft-josefsson-cfrg-mothma-00, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-josefsson-cfrg-mothma-00

[74] P. Longa, J. Bos, S. Ehlen, and D. Stebila, "FrodoKEM: key encapsulation from learning with errors," Internet Engineering Task Force, Internet-Draft draft-longa-cfrg-frodokem-01, Sep. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-longa-cfrg-frodokem-01

[75] S. Fluhrer, M. Prorock, S. Celi, J. Gray, X. Keita, and H. Kosuge, "NTRU Key Encapsulation," Internet Engineering Task Force, Internet-Draft draft-fluhrer-cfrg-ntru-03, Jul. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-fluhrer-cfrg-ntru-03

[76] S. Fluhrer, Q. Dang, J. Mattsson, K. Milner, and D. Shiu, "ML-KEM Security Considerations," Internet Engineering Task Force, Internet-Draft draft-sfluhrer-cfrg-ml-kem-security-considerations-04, Nov. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-sfluhrer-cfrg-ml-kem-security-considerations-04

[77] G. WANG and H. Wang, "HMAC Based Hybrid Key Combiners for Multiple Keys," Internet Engineering Task Force, Internet-Draft draft-wang-cfrg-key-combiners-00, Oct. 2025, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-wang-cfrg-key-combiners-00

[78] S. Josefsson and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)," RFC 8032 (Informational), RFC Editor, Fremont, CA, USA, Jan. 2017. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8032.txt

[79] L. Bruckert, J. Merkle, and M. Lochter, "Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS) Version 1.3," RFC 8734 (Informational), RFC Editor, Fremont, CA, USA, Feb. 2020. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8734.txt

[80] B. Westerbaan and C. Wood, "X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE," Internet Engineering Task Force, Internet-Draft draft-westerbaan-cfrg-hpke-xyber768d00-03, May 2024, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-westerbaan-cfrg-hpke-xyber768d00-03

[81] D. Eastlake 3rd and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," RFC 3174 (Informational), RFC Editor, Fremont, CA, USA, Sep. 2001, updated by RFCs 4634, 6234. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3174.txt

[82] S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, and M. Fredrikson, "On the practical exploitability of dual EC in TLS implementations," in *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*, K. Fu and J. Jung, Eds. USENIX Association, 2014, pp. 319–335. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/checkoway

[83] ——, "On the practical exploitability of dual {EC} in {TLS} implementations," in *23rd USENIX security symposium (USENIX security 14)*, 2014, pp. 319–335.

[84] S. Checkoway, J. Maskiewicz, C. Garman, J. Fried, S. Cohney, M. Green, N. Heninger, R.-P. Weinmann, E. Rescorla, and H. Shacham, "A systematic analysis of the juniper dual ec incident," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 468–479.

[85] E. Rescorla and M. Salter, "Extended Random Values for TLS," Internet Engineering Task Force, Internet-Draft draft-rescorla-tls-extended-random-02, Mar. 2009, work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-rescorla-tls-extended-random-02

[86] D. J. Bernstein, K. Bhargavan, S. Bhasin, A. Chattopadhyay, T. K. Chia, M. J. Kannwischer, F. Kiefer, T. Paiva, P. Ravi, and G. Tamvada, "Kyberslash: Exploiting secret-dependent division timings in kyber implementations," *Cryptology ePrint Archive*, 2024.

[87] A. Genêt, N. L. de Guertechin, and N. Kaluđerović, "Full key recovery side-channel attack against ephemeral sike on the cortex-m4," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2021, pp. 228–254.

Appendices

Appendix A: Acknowledgments

The author would like to thank the following for incisive comments that have improved the text: Tanja Lange, Matthieu Rivain.

All errors and omissions of course remain the fault of the author.

Appendix B: The IETF

As with all Standards Development Organisations (SDOs), the IETF has its own peculiar methods for organising work. As not all readers may be familiar with those, and as they affect the status of many of the specifications referred to here, it's worhwhile including a short explanation for some relevant IETF organisational practices. This text is intentionally a far from complete description of IETF processes, and is solely intended to explain the terms used earlier in this document.

The IETF is organised into "areas" by topic, such as "security" or "routing" and though the set and definition of areas does change slowly, it is roughly stable over 5-10 years, with most area-level changes relating to protocols relatively higher up the stack, such as application protocols like HTTP or WebRTC.

Within areas, work is organised into Working Groups (WG), each of which has a charter that defines its technical scope and expected outcomes.

The main outputs from IETF work are specifications published in the RFC series. Prior to being finalised draft specifications are published as Internet-drafts, which can have various differet statuses as they evolve:

- individual draft: anyone can publish anything they want as an individual Internet-draft - such drafts have no particular formal status, as work has to start somewhere. Some individual drafts may be quite important and very likely to becomre standards-track RFCs, while others are irrelevancies - knowing which is which is context specific. (Sometimes these may be referred to as non-WG drafts or personal drafts.)

- adopted draft: the chairs of a WG may issue a "WG call for adoption" for an individual draft, and if there is rough consensus, then the draft becomes a WG draft, and is much more likely to become an RFC. (Sometimes these may be referred to as WG drafts.)

- Working Group Last Call (WGLC): when the editors and WG chairs are happy that work on a specification is complete, then the chairs can start a typically two-week WGLC (run on the WG mailing list) to check if there are any remaining issues before the WG consider the specification ready for publication as an RFC. Some WGLCs are calm and uneventful, others result in unexpected technical comments that set the work back and yet others are entirely expectedly controversial.

- IETF last call (IETF LC): typically, after a successful WGLC there is a quick review of the specificaton by the relevant "area director" (the person who appoints WG chairs and has other management roles) that can result in an iteration of the draft specification, before another round of IETF-wide review (run on the mailto:last-call@ietf.org mailing list) as check that the work of a specific WG doesn't cause problems for people involved in unrelated IETF activities (other WGs). Again, most IETF LCs pass uneventfully, but some are very controversial.

- Internet Engineering Steering Group (IESG) reivew: following IETF LC, specifications are reviewed by the IESG, which consists of the set of IETF area directors. This review can uncover new technical or process issues and can involve iterations between the authors/editors of the WG that produced the specification and the IESG until issues are addressed.

- RFC-editor queue: once a document is approved by the IESG, then it enters the RFC editor queue, where RFC production staff do copy-editing in conjunction with the authors/editors. This phase may take some time if a specification has a normative reference to some other document that is e.g. still a WG draft. Such "clusters" of specifications in the RFC editor queue are not uncommon, and can lead to some delay, if e.g. one document on which others depend gets "put back" in the process.

- Independent Stream RFCs: The RFC series (having existed since 1969) includes oddities, and a subset of the RFC series are documents from what is now called the "Independent stream" that includes April 1st RFCs (mostly inane jokes, but sometimes tellingly inane), but also specifications of useful proprietary protocols, or "paths-not-taken" by the IETF. The Independent stream has in the past also been used to document protocols using national cryptographic standards or algorithms that (at the time) were not openly available. There is an ongoing tension where people whose specifications fail to become IETF RFCs might try get that text published as an Independent stream RFC. Sometimes that is a vanity problem, and other times publishing such text is useful for the Internet; it is not easy to draw a hard and fast rule that distinguishes those cases. [1]

Note that, at any of these stages, a specification can "go backwards" to earlier stages, typically if some new information indicates previously unknown problems.

[1] The author of this report is currently a member of the Independent stream editor's editorial board so has a little influence when it comes to publishing (or declining to publish) specifications on the Independent stream.)