Draft text for a PQ Maintenance WG

See https://github.com/rdanyliw/ietf-pq-maintenance/blob/main/pqm-charter.md for the latest version. This is an annotated and exported PDF companion to the "How should the IETF approach Post-Quantum security?" presentation at the IETF 111 SAAG presentation (July 27, 2021).

Placeholders

[Planned WG name] = choose a name

[Planned WG acronym]

[Post Quantum work collaborators] = ??

[Protocols requiring attention without an active WG] = ?? Secure Shell (SSH), JOSE, DNSSEC, XML Digital Signatures and XML Encryption, Kerberos, ??

[Liaison organizations] = ??

Draft Text

Continued advancements in the capabilities of quantum computers will reduce or compromise assurances provided by many widely deployed cryptographic algorithms, especially those relying on public key cryptography. Many IETF protocols currently rely on these vulnerable cryptographic mechanisms.

Active work is underway at the US National Institute of Standards and Technology, IRTF CFRG, and [Quantum Work Collaborators] to develop and validate Post-Quantum (PQ) cryptographic mechanisms expected to be resilient to the cryptanalysis capabilities of future quantum computing environments. The [Planned WG Name] working group ([Planned WG Acronym]) is chartered as a maintenance WG to analyze; and adapt or update IETF protocols, registries, and associated code points with PQ cryptographic mechanism.

The [Planned WG Acronym] WG will be the working group of last resort for this PQ work. If a given protocol or technology has an active WG in the IETF, any updates or required protocol maintenance should be done in that WG as the predominance of the expertise is expected to be there.

All PQ updates need not be done in the [Planned WG Acronym] WG. Differences in performance, input or output size, or reliability for example, may prevent new PQ cryptographic mechanisms from being simple swaps with existing classical mechanisms found in current IETF

protocols. After analysis in the [Planned WG Acronym] WG, the complexity of some protocol adaptations may require the chartering of new, dedicated WGs.

The [Planned WG Acronym] WG will not define new PQ algorithms and methods. It will only standardize the usage of PQ algorithms and methods that received review from [Post Quantum work collaborators].

In making changes to protocols and registries, the [Planned WG Acronym] WG may encounter outdated algorithm options, and the WG may propose deprecation of such algorithms. Additionally, the WG may document operational practices relevant to protocol operations and management in a hybrid (classic and PQ) environment.

The WG is currently focused on updating [Protocols requiring attention without an active WG].

The [Planned WG Acronym] WG will liaise with [Liaison organizations]. It will also coordinate, as needed, with LAMPS on PQ work in CMS and PKIX.