Additional PQC Next Steps Side Meeting

Materials: https://github.com/rdanyliw/ietf-pqc-transition

IETF 115

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Agenda

1. Welcome, Objectives, and Introductions

2. “PQC Transition Support” WG Proposal

3. What other PQC tasks need to happen?

4. Do we need a PQC Directorate?

“PQC Transition Support” WG Proposal

- History – SecDispatch and pqc@ietf
- Proposal

  https://github.com/rdanyliw/ietf-pqc-transition/blob/main/pqct-charter.md
- Discussion
  - Is this problem clear?
  - Addressing a problem the IETF should tackle? now?
  - What is the right scope?
  - Are there volunteers?

Charter Text: Framing & Scope

Some IETF protocols rely upon cryptographic mechanisms that are considered secure given today's "classical computers" but would be vulnerable to attacks by a Cryptographically Relevant Quantum Computer (CRQC). These mechanisms rely upon algorithms based on integer factorization or the discrete logarithm problem. Outside of the IETF, active work is underway to develop and validate Post-Quantum Cryptography (PQC) mechanisms that are expected to be resilient to the cryptanalysis capabilities of future CRQCs. Select IETF WGs (e.g., LAMPS, TLS, IPSECME, COSE) have already begun standardizing revised protocol behaviors.

The focus of this WG is to support this growing body of work in the IETF to facilitate the evolution of IETF protocols and document associated operational guidance to PQC.

Charter Text: Approach

The WG will provide a standing venue to discuss PQC transition issues and experiences to date relevant to IETF work. The WG will also provide a venue of last resort to discuss PQC-related issues in IETF protocols that have no associated maintenance WGs. This WG will not update existing protocols, specify new protocols, define new cryptographic mechanisms, or assess whether a given cryptographic mechanism is quantum-resistant.

The WG will document operational and design guidance which supports PQC transition. The general process of elaboration through documentation will be for issues to be identified and discussed on the mailing list, and presentations made at WG meetings. When topics merit more coherent documentation, the WG will adopt documents to capture the information in Internet-Drafts. If the working group consensus is that the material of the Internet-Draft is generally useful for archival purposes, the WG will seek publication of the work items as Informational RFCs. At any point, from early discussion of topics through later documentation stages, the WG may identify a more appropriate WG for the matter, and with coordination, dispatch it there.

Charter Text:
“Guardrails” & Milestones

The IESG is establishing this working group on an experimental basis, and in 2 years, the IESG intends to review it for rechartering to continue or else closure.

Milestones

- WG Adoption of an Informational document that defines terminology for (hybrid) PQC schemes
- WG Adoption of an Informational document on ‘PQC for engineers’

Needed PQC Tasks?

Has a Home (Protocol or Activity / WG)		Needs a Home
TLS	TLS	SSH
IPsec	IPSECME	?
CMS	LAMPS	
X.509	LAMPS	
COSE	COSE	
DNSSEC	DNSOP	
?		

☝ What is the scale of the work?

Source: https://github.com/rdanyliw/ietf-pqc-transition/blob/main/ietf115-pqc-next-steps-side-meeting-work-homes.md

Do we need a PQC Directorate?

- (Possible) Goals
  - Review documents for PQC resiliency and consistent framing/terminology
  - Support
    - “Early-review” of WG documents
    - IETF LC/IESG Review cadence
- Discussion
  - Is there a current need? If so:
  - Relationship to/coordination with SECDIR or CFRG
  - What is the right scope?
  - Are there volunteers?