PQUIP Working Group

Sofia Celi and Paul Hoffman

IETF 116, Yokohama
March 2023

Basics

- Post-Quantum Use In Protocols (pquip) Working Group
- Mailing list: pqc@ietf.org
- From the WG charter: “The output of this WG is expended to inform protocol work and guidance developed by other WGs in the IETF. Consistent with other IETF WGs, this WG will also rely on outside entities (e.g., CFRG) to define and assess new PQC mechanisms.”

The “note well” on IETF policies

- You already agreed to this when you registered
- It is worth reading again: https://www.ietf.org/about/note-well/

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)

The IETF code of conduct

- Please treat each other with respect
- It is worth reading: https://www.ietf.org/about/administration/policies-procedures/code-of-conduct/

Excerpts from the code of conduct

- IETF participants extend respect and courtesy to their colleagues at all times
- IETF participants have impersonal discussion
- IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments

Agenda

- Hybrid terminology document - 10 min
- PQC for engineers document - 10 min
- Grand list of WGs and protocols looking at PQC algorithms - 45 minutes
- Other WG business - remainder

Status of hybrid terminology document

- Good discussion about terminology
- Disagreement about whether we should create new (hopefully better) terminology or reuse current terminology but give better definitions
- Chairs believe this is ready to become a WG document

PQC for engineers document

- Very early stages
- Some of this material is already in RFC 9340 "Architectural Principles for a Quantum Internet"
  - We will **not** be discussing QI or QKD in this WG
- X9 also has a long introductory document
- We need to decide the scope of the document
  - Maybe we do a very short "look elsewhere" document
- Some volunteers to do the writing
- Chairs believe it is too early to adopt

The grand list of PQC and IETF

- https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc
- This is intentionally not an Internet Draft, and won't become an RFC
- Will evolve as the rest of the IETF starts dealing with PQC
- Done as a README.md, can be displayed outside of GitHub

List structure

- Protocol-independent algorithm or cryptography specifications
- PQC support in protocols and migration techniques
- Improvements adjacent to PQC
- Implementations and interop testing for these specs
- Security Area protocols with no PQC-specific action needed

Evolution of the list

- What topics are missing?
- What line items are missing?

Other WG business

- Others