OpenPGP at IETF 118

Prague
2023-11-09

Co-chairs:
Daniel Kahn Gillmor
Stephen Farrell

Note Well

[https://www.ietf.org/about/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.

- 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)

IETF Hybrid Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho
  - (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- Keep audio and video off if not using the onsite version

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

IETF Code of Conduct (RFC 7154)

- “IETF participants extend respect and courtesy to their colleagues at all times.”
- Native English speakers “communicat[e] clearly, including speaking slowly and limiting the use of slang”
- “reasoned argument rather than through intimidation or personal attack”
- “best solution for the whole Internet, not just the best solution for any particular network, technology, vendor, or user.”
- “Individuals are prepared to contribute to the ongoing work of the group”

Agenda

- Crypto-refresh since IETF 117
- Rechartering status
  - Topic poll recap
  - Milestones
- Post-Quantum Cryptography
- AOB

Crypto-refresh since IETF 117

- Draft -11 (from more WGLC feedback and AD review):
  - Fix errata: 2208, 2214, 2222, 2226, 2235, 2236, 2238
  - Make S2K type registry's "Generate" column normative
  - Armor handling: mandate ignoring whitespace
  - Clearsigning Framework (CSF): strict validation (avoid risky garbage headers)
  - Reintroduce size limits on hash algorithms for ECDSA and EdDSA
  - DSA sigs can use larger hash algorithms, doesn't have to match exactly
  - Textual cleanup
  - Clarifications: primary key/subkey convention, CFB's not-quite-an-IV, Argon parameter encoding
  - Improve references (C, SHA-2, RFCs mentioned in intro)
  - "Packet Tag" is disambiguated into either "Packet Type ID" or "encoded Packet Type ID"
  - Codepoints are now explicitly called "IDs" (e.g. Public-Key Algorithm ID)
- Draft -12 (from more WGLC feedback and AD review):
  - Textual cleanup
  - IANA requirements clarifications
  - Upgrade steps

Rechartering status

- Interim discussion about rechartering happened
- New charter text is proposed (on gitlab)
- Topic Prioritization Poll suggested four initial candidate topics
- Four milestones proposed, all calls for adoption:
  - 2023-11: PQC draft(s)
  - 2024-01: Superseded Keys draft
  - 2024-01: Persistent Secret Keys draft
  - 2024-03: WKD (or HKP) draft(s)

PQC questions for the WG

Starting from draft-wussler-openpgp-pqc-03...

- Who has read the draft?
- Implementation status?
- Is algorithm selection what we want?
  - Are they parameterized reasonably?
  - Need for composite signature scheme?
  - Do we need six different ECDH schemes for each composite?
- All algorithms in a single draft, or broken out somehow?
- Are the wire formats sensible?
- Require v6 keys?

PQC sub-milestones

- Call for adoption on list
- Test vectors
- Interoperability testing

Any other business?