OpenPGP

IETF 119
Brisbane
2024-03-19

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”

OpenPGP

Agenda

- Crypto-Refresh + WG Status
- Post-Quantum Cryptography Algorithm Selection
  - KEM Algs
  - KEM Combiners
  - Signatures
  - Transition/Backward compatibility
- Drafts for possible adoption
  - Persistent Symmetric Keys
  - Replacement Key
  - *1PA3PC?*
  - *Hardware Secrets?*
  - *WKD?*
- AOB

Crypto-refresh since IETF 118

- Draft -13 (non-substantive)
  - Minor typo cleanup
  - IANA clarifications
  - Cleartext signing framework clarifications
  - Reference cleanup
- In RFC Editor's queue!

Successfully Rechartered!

https://datatracker.ietf.org/wg/openpgp/about/

- *The working group will produce a number of specifications that are adjacent to the OpenPGP specification and provide guidance to OpenPGP libraries and/or applications.*
- Milestones
  - PQC (adopted), Persistent Symmetric Keys, Superseded Keys

Any other business?