

# OpenPGP at IETF 117

San Francisco

2023-07-28

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**    **Remote 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
- 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 status
  - Summary since IETF 116 (pubreq!)
  - Open Editorial Merge Requests
- Rechartering?

# Crypto-refresh since IETF 116

- Draft -09:
  - Add fingerprint length octet in v6 PKESK for better parseability of unknown fingerprint versions
  - X25519 and X448: mix public key material into KDF as per RFC 7748
  - V3 PKESK for X25519 and X448: don't protect symmetric key algorithm choice, mandate AES
  - Remove “SaltedHash” armor header (no more one-pass verification of v6 CSF)
  - Test vectors: add locked secret key
  - Security considerations about session key reuse
  - New subsections: “Terminology Changes” and “Upgrade Guidance”
  - IANA considerations cleanup
- Draft -10:
  - Change IPR policy to pre5378Trust200902 since we can't contact all authors of RFC 4880
  - Fix erratum

# Crypto-refresh status

- Publication Requested!
- Shepherd writeup submitted
- AD review is in progress

# Outstanding editorial tuning

- Packet Tag vs. Type: (!324)
- Minor:
  - Clarify MTI markers in Upgrade Guidance (!321)
  - Clarify CFB description (!323)
  - Simplify description of reserved codepoints (!325)

# Should we recharter?

- Assuming we succeed in releasing the crypto-refresh...
  - Several presentations pending about possible rechartering topics
  - We could also close the WG
  - If we do recharter, we need text

# Possible Rechartering Topics

- Post-Quantum (Strenzke)
- Stateless OpenPGP API (SOP) (Gillmor)
- Automatic Forwarding (Wussler)
- Persistent Symmetric Keys (Huigens)
- Replacement for Designated Revoker, Attestation Signatures, User ID conventions, PGP/MIME guidance for v6 sigs (Gillmor)
- Fingerprint Human Interface (in-person verification, business cards, QR codes?)
- Superseded keys
- Domain separation for signing or encryption
- Web of Trust (regexes, trust signatures, validation constraints)
- Certification-capable subkeys
- Intended Recipients challenges
- Networked certificate discovery (HKP, WKD)
- Forward Secrecy
- PGP/MIME message construction
- Integration with KEYTRANS
- OpenPGP with non-OpenPGP Hardware tokens

# Rechartering process

- Please propose text for a new charter
- See **charter.md** in <https://gitlab.com/openpgp-wg/openpgp-wg-admin>
- Propose revised text by end of August
- Virtual interim in mid-September