IETF OpenPGP WG Interim Meeting 2021-02-26 15:00 UTC

IETF 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)

Administrivia

- Scribes and Note-takers?
- Agenda Bash
- Progress on `draft-ietf-openpgp-crypto-refresh`
- Developing the draft
- Next steps on `draft-ietf-openpgp-crypto-refresh`
- IETF 110 Agenda & next Interim

Progress on …`-crypto-refresh`

- Reset to RFC 4880, new draft name
- Restoring changes from …`-rfc4880bis-10` by topic:
  - -00: RFC 4880 + Minor formatting changes
  - -01: Errata + Camellia + Terminology
    - (+“whitespace” change, reverted)
  - …

Progress on `crypto-refresh-02`

- Codepoints reserved
- RFC 6637 (ECDSA + ECDH)
- Most registries now SPECIFICATION REQUIRED
- V3 signatures and malleable encryption deprecated
- SHA3
- Curve25519 for ECDH

Draft Development

https://gitlab.com/openpgp-wg/rfc4880bis

- Markdown
  - `rfc4880.md`, `rfc4880bis.md`, `crypto-refresh.md`
- Merge Requests
- Issue Tracker
- Mailing list <openpgp@ietf.org>

Next steps on `crypto-refresh`

Toward parity with `rfc4880bis-10`

Chartered Crypto

- v5 fingerprint
- EdDSA
- AEAD
  - S2K 253, AEAD prefs, V5 SKESK
- MTI update: cipher, hash, compression, AEAD, pubkey

Crypto-related

- v5 signature
  - Additional metadata
- Issuer Fingerprint
- Brainpool
- v5 keys
  - add'l count field

Not Crypto

- Attested Certifications
- Key Usages:
  - ADSK, Timestamping
- MIME Literal data (‘`m`’)
- Notations
- Intended Recipient Fingerprint
- Keyblock subpacket
- User ID Attribute

`crypto-refresh` beyond `rfc4880bis-10`

- Curve448?
- S2K update (argon2?)
- …?

IETF 110

- Meeting Thursday, 2021-03-11 “Session II”
  - (14:30-15:30 UTC)
  - https://meetings.conf.meetecho.com/ietf110/?group=openpgp&short=&item=1
- Register:
  - https://registration.ietf.org/110/
  - https://www.ietf.org/forms/110-registration-fee-waiver/

Next Interim

- IETF 111 is last week of July
- Early May?