OpenPGP IETF-95

2016-04-06
Buenos Aires,
Argentina

Chair:

- Daniel Kahn Gillmor

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Agenda Bashing
- **`draft-koch-openpgp-rfc4880bis-02`**
- Terminology review
- S2K
- fingerprint
- OAE

4880bis next steps

- Werner Koch has posted

  `draft-koch-openpgp-rfc4880bis-02`

- https://gitlab.com/openpgp-wg/rfc4880bis
- Please review and comment

Terminology review

- What kinds of cleanup are desired?
- Can we break with older OpenPGP terminology?

S2K

- Argon2i seems to have no objections
- **`draft-irtf-cfrg-argon2`**
- Argon2i has been recently revised to address Corrigan-Gibbs' attack, not yet covered in the IRTF draft

Fingerprint

- Include Creation timestamp?

Symmetric encryption

We need to replace CFB, but with what?

- AES-GCM
  - Built-in to browsers, known to be fragile
- AES-OCB
  - IP constraints? Rogaway is fine with a grant for any use with OpenPGP, unclear if there are other IP claims.
- ChaCha20-Poly1305
  - The popular new cipher (but: “Crypto Monoculture”)
- POET/AEZ/ELmD

AOB

- openpgp@ietf.org