OpenPGP WG @ IETF 114

July 29 2022 1400 UTC

Chairs: Daniel Kahn Gilmor, Stephen Farrell

Charter: https://datatracker.ietf.org/group/openpgp/about/
Mailing list: https://www.ietf.org/mailman/listinfo/openpgp
Jabber room: xmpp:openpgp@jabber.ietf.org?join
Meeting Materials:
https://datatracker.ietf.org/meeting/114/session/openpgp
Etherpad (notes): https://notes.ietf.org/notes-ietf-114-openpgp

Note Well

A reminder of IETF policies.

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)

Agenda

0. Chairs: Administrivia and agenda bash (5)
1. WGLC issues (as long as it takes)
2. Next steps
3. Daniel Huigens, Persistent Symmetric Keys (10)
4. Aron Wussler, Automatic Forwarding (10)
5. AOB

WGLC issues

- We had a WGLC (it won’t be the last;-)
- Issues in gitlab are labelled with “WGLC”
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/?sort=created_date&state=opened&label_name%5B%5D=WGLC&first_page_size=20
- Let’s go through ‘em and see what we can resolve
  - modulo confirmation on the list of course

Issue #132 - Padding

- Padding octets (zero/random/other)
- Issue
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/132
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/npCHOnOWEWVfvztmrkqs0w00NLk/

Issue #134 – AEAD Decryption Failures

- Suggests changing any "SHOULD fail" statements related to AEAD decryption errors to "MUST fail."
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/134
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/tN2jWx4hUtiMGSo8-ILRXYNumVY/

Issue #135 – GCM

- Should we include GCM or not?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/135
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/oevAcrfJSL_BuUoDq1wJ2QW2JX8/

Issue #136 – Binding Keys to Modes

- HKDF is specified (in 5.3.2 and 5.13.2) for use in key derivation to avoid pitfalls with different modes. Keep that?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/136
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/WMfDoKxSUo0-iRiX-wmRJ_hnl5Y/

Issue #137 – Direct Key Sigs

- Certificate-wide parameters live in a direct key sig for v5. Keep that?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/137
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/W52eXsqWOlinIlfx-eH7FRuXlSA/

Issue #138 –

- Revocation key subpacket is disallowed for v5 keys. Keep that?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/138
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/c45f-yCd2IfNOiuzsJS2KRXXfjM/

Issue #140 – IANA

- Check if we’re happy with the changes to IANA registration rules.
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/140
- Mail thread:
  - TBD

Issue #142 - Argon2

- Is the text sufficiently clear?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/142
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/wRlPUH6Fvo2BWY5mX-k4touABpM/

Issue #143 – Problematic keys

- Some problematic keys are known to exist in the wild. Should we add some text to describe how to handle that better?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/143
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/Zv8v1IwbbXYiDPKytfbUmtNdxak/

Issue #139 – Are we there yet?

- Do we want to “raise the bar” for changes to help get done? If so how/when?
- Issue:
  - https://gitlab.com/openpgp-wg/rfc4880bis/-/issues/139
- Mail thread:
  - https://mailarchive.ietf.org/arch/msg/openpgp/hlrPvBmO_AW9rsSh8KUhTtDU4CE/