OpenPGP @ IETF 115

London
2022-11-08

Co-chairs: Stephen Farrell (in person)
Daniel Kahn Gillmor (remote)

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
- Wear masks unless actively speaking at the microphone

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”

Agenda

WGLC Followup

- Avoiding conflicts with **`draft-koch`**
- Salt Length
- Aliased Signature Versions
- Contexts for Encryption and Sigs
- EC point wire formats
- IANA updates
- AOB

Future Work (if time)

- PQ next steps (Aron Wussler)
- Collecting possible re-charter items?

draft-ietf-openpgp-crypto-refresh WGLC

- Draft -07 is the basis for WG work going forward
  - Avoid conflicts with **`draft-koch`** where feasible
- **Please review!**
- We will not get to future work without getting the currently chartered work out the door

Avoiding Conflicts with `draft-koch`

Outstanding Conflicts

- Key version 5
- Signature version 5
  - If we change these, should we also sync versions of OPS and PKESK? SEIPD?

Already Deconflicted?

- Subpacket codepoints:
  - 39/Pref AEAD Ciphersuites ≠ **`d-k`**: 34/Pref AEAD
- AEAD:
  - SEIPDv2 ≠ **`d-k`**: packet tag 20
- Feature Flags:
  - 0x08/SEIPDv2 ≠ **`d-k`**: 0x02/packet tag 20
- One Pass Signature (OPS):
  - Added v5, **`d-k`** has only v3 unchanged
- PKESK:
  - Added v5 to match SEIPDv2, **`d-k`** has only v3 unchanged

Length of Salt

Aron Wussler recommends (see #150):

- V5 signatures use a 16-octet salt. Make larger in preparation for PQ signing schemes?
  - Static or vary on hash algo or pubkey algo?

Aliased Signature versions

Demi-Marie Obenour observes (#130):

- A v5 signature over a small message (<4GiB) can be rewritten into a v3 signature over subtly different data
  - Rewriting to v4 is sometimes also possible but much less likely
- Fix proposed: change trailer for hashed data in v5 sig
  - Or, rely on our ban of v3 verifications?

Context Parameter

Marcus Brinkmann recommends (see #145):

- Add Context Parameter for Encryption
  - Defense against several forms of EFail
- Daniel Huigens: Signatures too?
- Requires shared definition of context

EC Wire Format Simplification

Andrey Jivsov recommends (see #149):

- For v5 ECDH and ECDSA pubkeys, switch from SEC1 to compact x-only representation

IANA Updates

- All: SPECIFICATION REQUIRED (see #140)
  - Except: Version numbers, Packet types (both RFC REQUIRED)
- Designated Experts
  - Who?
  - What guidance? (model after TLS or COSE or ?, see #146)
- Registry review (e.g., #147)

Any other business?

- Send reviews to the list! <openpgp@ietf.org>
- Report issues at https://gitlab.com/openpgp-wg/rfc4880bis
- Read other reviews and issues and follow up