OpenPGP

IETF 96
Berlin, July 2016

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 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
- Any Birds of a Feather (BOF) session
- The IETF plenary session
- 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, Bluesheets
- Document Review
- Registry management
- 4880bis changes
- PGP/MIME vs. S/MIME
- AOB

Documents

draft-ietf-openpgp-rfc4880bis-00

Mailing list: openpgp@ietf.org

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

- Issues and pull requests tracked on gitlab
- Discussion on mailing list

Registry management

- Tight control over registry makes everyone unhappy
- Registries are small (7bit)
  - Expand to 14 bit
- Codepoint squatting/assignment
  - TLS WG is moving toward “Y” and “MTI” columns and FCFS assignment
  - Needs “designated expert”

Registry management (2)

(Example from TLS)

- For MTI and “Y” requests,
  - requester’s publish individual draft,
  - requester’s ask for WG adoption,
  - WG chairs do adoption call,
  - WG does its thing on WG draft,
  - IETF does its thing, and
  - IANA (assigns #s) & rfc editor (publishes) do their things.
- For all others:
  - request is submitted to IANA, WG, WG chair, AD,
  - request is redirected to designated expert,
  - designated expert reviews request:
    - if good-to-go designated expert tells IANA to assign code point (goto last step)
    - if not-good-to-go for an obvious reasons the designated expert rejects the request with some rationale (and probably lets the sec ADs know about it)
    - if not-good-to-go for all other reasons the designated expert asks (expert's choice depending on the situation) AD/WG chairs/community for guidance
  - IANA makes assignment and includes the cipher suite assignment specification reference in the registry (and possibly the rfc editor does their thing if an RFC is being published)

<over to Werner Koch for RFC4880bis>

PGP/MIME vs. S/MIME

- Message formats
  - Out of scope: we’re working on RFC 4880, not 3156
- Certificate formats
  - OpenPGP will not adopt X.509 directly
  - People who want to work on interop/translation mechanisms between cert formats can propose specific changes as long as they do not distract from chartered work

AOB

- Followup on list
  - openpgp@ietf.org
- Concrete proposals please!