OpenPGP WG Meeting

IETF-93
2015-07-24
Prague

Chairs:
Daniel Kahn Gillmor <dkg@fifthhorseman.net>
Christopher LILJENSTOLPE <ietf@cdl.asgaard.org>

Agenda

- Agenda Bashing, Blue Sheets, Scribe, etc. (10 min)
- Review of Working Group scope and timetable, Chairs (10 minutes)
- Discussion of suggested components of RFC4880bis
  - UDF a public-key fingerprint proposal (PHB) (10 minutes)
  - Fingerprint questions (10 minutes)
  - Potential inclusion of elliptic curves recommended by the Crypto Forum Research Group (CFRG) (10 minutes)
  - A symmetric encryption mechanism that offers modern message integrity protection (e.g. AEAD) (10 minutes)
  - Revision of mandatory-to-implement algorithm selection and deprecation of weak algorithms (10 minutes)
  - Certificate formats
  - Other cleanup
  - Revocation and expiry
  - Drafting plans
- Open Mic (30 min)

Charter

https://datatracker.ietf.org/doc/charter-ietf-openpgp/

This incarnation of the working group is chartered to primarily produce a revision of RFC4880 to address issues that have been identified by the community since the working group was originally closed.

These revisions will include, but are not limited to:

- Potential inclusion of elliptic curves recommended by the Crypto Forum Research Group (CFRG) (see note below)
- A symmetric encryption mechanism that offers modern message integrity protection (e.g. AEAD)
- Revision of mandatory-to-implement algorithm selection and deprecation of weak algorithms
- An updated public-key fingerprint mechanism

Charter scope

The Working Group will perform the following work:

- Revise RFC4880
- Other work related to OpenPGP may be entertained by the working group as long as it does not interfere with the completion of the RFC4880 revision.

As the revision of RFC4880 is the primary goal of the working group, other work may be undertaken, so long as:

1)The work will not unduly delay the closure of the working group after the revision is finished (unless the working group is rechartered).

2)The work has widespread support in the working group.

These additional work items may only be added with approval from the responsible Area Director or by re-chartering.

UDF

- PHB's slides

Fingerprint questions

- What material needs to be fingerprinted?
- How much entropy in the fingerprint?
- What representations?
  - UDF

    MB2GK-6DUF5-YGYYL-JNY5E-RWSHZ-SV75J
  - RFC 6920

    ni:///sha-256;UyaQV-Ev4rdLoHyJJWCi11OHfrYv9E1aGQAlMO2X_-Q
  - Others?
- Usability studies?

Elliptic Curves

- CFRG seems to have settled on 25519 and goldilocks
- Signature mechanism still undecided
- IUF streaming signing mechanism required
- Existing implementations
  - https://tools.ietf.org/html/draft-koch-eddsa-for-openpgp-01

Symmetric Crypto (AEAD)

- SEPID – replace or upgrade?
- AEAD mode – OCB/GCM/CCM?
- Any takers on drafting this?

Mandatory-to-Implement (MTI)

- Ciphers
- Asymmetric crypto
- Digests

Certificates

- v5 format needed?

Cleanup

- KeyID removal
- Terminology
- Compression
- S2K
- ??

Revocation and Expiry

- Do we need both?
- Should expiry be mandatory?
- Revocation reasons?

Drafting plans

- 4880bis early draft from Werner Koch:
  - git clone git://git.gnupg.org/gnupg-doc

    cd gnupg-doc/misc/id/rfc4880bis
- Other options?
- Section editors?

Open Mic

AOB