OpenPGP IETF-94

2015-11-03
Yokohama, Japan

Chairs:

- Daniel Kahn Gillmor
- Christopher LILJENSTOLPE

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
- 4880bis plans
- SEIPD→SED attack
- Algorithm deprecations
- Fingerprint
- CFB replacement (Bryan Ford)
- Metadata
- S2K
- Registry policies

4880bis plans

- Werner Koch is drafting a proposed 4880bis
- Will post pointers for workflow and patches
- Please review and comment

SEIPD → SED attack

- Jonas Magazinius pointed out you can convert symmetrically-encrypted integrity-protected data (SEIPD) packets to plain symmetrically-encrypted packets (SED) without decryption
- How do we deprecate SED effectively?

Algorithm Deprecation

How do we draft algorithm deprecation for stored data format? (MUST NOT what?)

- Digests:
  - MD5, SHA1?
- Symmetric:
  - IDEA, 3DES?, CAST5?, Blowfish?, Twofish?
- Asymmetric:
  - DSA? Size limits on RSA? NIST ECC? ElGamal?

Fingerprint

- One digest format or multiple?
- Choice of digest
- Truncation allowed?
- What is digested?
  - Creation time
  - Expiration time
- Distinguish v5 from v4?
- UI/UX guidance for implementors

Symmetric encryption

- Bryan Ford wrote:

https://datatracker.ietf.org/doc/draft-ford-openpgp-format/

- Modern modes
- Streaming/chunking
  - Asymmetric signature binding

Metadata protection

- Also in Bryan Ford's draft

https://datatracker.ietf.org/doc/draft-ford-openpgp-format/

How indistinguishable from noise do we want encrypted OpenPGP material to be?

S2K

- Secure Password Hashing competition has a winner:
- https://password-hashing.net/index.html
  - Argon2
    - Argon2i
    - Argon2d
- Parameterize for S2K
- Integration patch by Nils Durner
  - Sent to openpgp@ietf.org October 15
- Need IETF draft for Argon2i for normative reference?

Registry policies

- Crypto registries
  - Digest
  - Symmetric crypto
  - Asymmetric crypto
- S2K (key derivation)
- Compression
- Notations
- Packet Types

AOB

- openpgp@ietf.org