IETF-96 OpenPGP WG

Werner Koch

2016-07-18

MIME flag

- New Literal Data Packet tag 'm'
  - States that this contains a MIME part
  - Flexible way to encode properties of the content.
- Use 'u' instead of 't'
  - Do we need 't' and 'u' at all ?
- David Shaw suggested to explicitly state that the file name, file data, and the tag ('m') are not covered by the signature.
  - See also last topic.

Issuer fingerprint

- New subpacket.
- Makes it possible to find the key.
- Avoids "Bad signature" due to collissions in the 64 bit key ID.
- Fade out the use of the Issuer subpacket.
- Proposal has been sent and is in the issue tracker.

Encrypted-to

- New signature subpacket: encrypted-to
  - with a list of recipient keys
- Shows to whom a signed message was originally encrypted
- Proposal?

S2K

- Add a codepoint for argon2i
- Add a codepoint for "no S2K"
  - To be used with a high-entropy key
- Deprecate all others S2K modes
- Keep unprotected keys

Deprecation

- Deprecate 3DES
- Deprecate MD5
- Deprecate SHA1
- Deprecate SHA224
- Deprecate RM160
- Deprecate Twofish
- Deprecate Blowfish
- Deprecate Symmetrically Encrypted Data Packet (tag 9)
- Deprecate OpenPGP v3
- Deprecate all S2K but argon, cleartext, and "no S2K"
- Can we deprecate certain key sizes for algorithms with arbitrary length?

Deprecation strategy

Classes of deprecated algorithms and parameter values:

- MUST NOT implement (e.g. MD5)
- MUST NOT produce (maybe after a certain date?), but MAY consume
  - with a warning to the user where possible
- MAY implement for backward compatibility (e.g. SEIPD)

MTI profile

- STRONG proposal:
  - MUST implement AEAD
  - MUST implement AES256
  - MUST implement SHA512
  - MUST implement Ed25519
- COMPAT proposal:
  - MUST implement AEAD
  - MUST implement AES128
  - MUST implement SHA256
  - MUST implement RSA

v5 fingerprint

- Do we include the creation time?
- What is the transformation?
- Keys can't currently be longer than 64K.
  - Use a 4 octet length for future PQ crypto.

Proposal:

- No creation time.
- SHA-512 truncated to 200 bits.

Features subpacket

- We have "support MDC"
- Add "support AEAD" for v4 keys only
- v5 keys MUST NOT have a Features subpacket

Notations can be used for future work

AEAD

- AES-GCM?
- AES-OCB?
- Or both?
- Streamable?
  - POET/AEZ/ELmD

New signature class — literal data packet

- Signature class "Literal Data Packet" covering exactly the contents of the preceding literal data packet exactly.
  - Protects the file tag ('b' or 'm')
  - Protects the file meta data
  - Protects the packet header?
- Proposal?