Crypto-Refresh Outstanding MRs

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

IETF 116

OpenPGP session

2023-03-29

Subpacket Criticality (MR !268)

- Encourage marking specific subpackets as critical:
  - Sig Creation Time
  - Key Expiration Time
  - Sig Expiration Time
  - Exportable Certification (only when *not* exportable)
  - Regular Expression
  - Key Flags
  - Intended Recipient
- Does not say what receivers should do if they are not marked critical

Primary Keys MUST be able to sign (MR !269)

- Chooses between two variant interpretations of what we expect of primary keys:
  - Primary keys MUST be able to sign, instead of
  - ✘ Primary keys MUST be able to sign if they want to sign

SHOULD implement subpackets (MR !271)

- If an implementer can only prioritize interpretation of some subpackets, which should we encourage?
  - Preferred Ciphers
  - Preferred Hashes
  - Preferred Compression Algorithms
  - Preferred AEAD Ciphersuites
  - Reason for Revocation
  - (+) Features (SEIPDv1, SEIPDv2, etc)
- How should an implementer encrypt if they *don't* understand Features?

Clarify self-sig guidance (MR !272)

- Move from wishy-washy language to MUST, MAY, SHOULD:
  - Placement of self-sigs in certificates
  - Implementation guidance on importing a secret key with prefs/features that don't match the implementation capabilities

Clean up Notation registries (MR !273)

- Drop “Security Recommended” and “Interoperability Recommended” columns from Notation Flag registry
- Clarify that Notation Name/Data registry is initially empty

Others

- Comments on session key reuse (MR !228)
  - See Falko's presentation
- Test vectors
  - Locked secret key (MR !274)
  - Clearsigned message (MR !275)
  - Encrypted+signed message (??)
- Remove checksum+padding from v6 ECDH (MR !223)