OpenPGP Miscellany

The Internet
2023-09-27

Daniel Kahn Gillmor
OpenPGP Miscellany

• Several outstanding fixes needed
• This is a bit of a grab bag
• Most have a proposed draft as a starting point
• Please step up as author/editor!
OpenPGP Revocation

• Proposal: draft-dkg-openpgp-revocation

• Started as “Delegated Revoker” (see !18)

• But what is revocation, anyway? Why is it hard? (clearer problem statement)

• Focus on full-cert revocation (deprecate revocations of User IDs and Certifications)

• Describe workflows; include test vectors
First-Party Approval of Third Party Certifications (aka 1PA3PC)

- Proposal: draft-dkg-openpgp-1pa3pc  (started from 160)
- Certificates can grow without bound due to 3rd-party certifications.
- Ensure that the primary key agrees to each certification
- We probably want to change the name from “Attested” to “Approved”
- New Signature (type ID 0x16), new subpacket (type ID 37)
  - Self-signature made over primary key + user id
  - Most recent self-signature of this type overrules all others
  - Subpacket embeds list of digests of certifications
    - Which digest? (same digest as self-sig)
    - What to do when out of space in subpacket or hashed subpackets section?
- Known producers: Sequoia and PGPy
- Consumers: keys.openpgp.org
User ID conventions

- Proposal: draft-dkg-openpgp-userid-conventions (derived from !23)
- “By convention, UID is RFC 2822 mail name-addr”
- But it isn’t:
  - Encoding: UTF-8 vs. US-ASCII vs. RFC 1522 (“Jörg Schmidt <schmidt@example.de>”)
  - Raw mail-addr (“lucy@example.net”)
  - quoted-string (“Marc O’Brian <marc@example.com>”)
  - CFWS (and other whitespace)
  - Obsolete forms
  - etc.
- Document what the convention actually is.
PGP/MIME multipart/signed v6 (#116)

- Content-Type: multipart/signed; protocol="application/pgp-signature"; micalg=pgp-sha256
- One-pass processing of e-mail messages
- Broken by v6 signatures because of salt
- Analogous to HashedSalt in CSF?
- (no current proposed draft)
Stateless OpenPGP Interface

- Proposal: draft-dkg-openpgp-stateless-cli
- Command Line Interface
  - Key generation / revocation
  - signing/verification, encryption/decryption
  - Several solid implementations
- C Library API (new!)
  - Intended to be easy to build the CLI from, and as a basis for other language bindings
  - Incomplete (no encryption/decryption yet)
  - No implementations yet
- Basis of OpenPGP Interoperability Test Suite
- Several outstanding proposals for extending it