

OpenPGP Rechartering: Cleanup Work

San Francisco

2023-07-28

Daniel Kahn Gillmor

What does it mean to do cleanup?

- OpenPGP has historical mess
- Revising RFC 4880 added to this legacy
- Other existing implementation work that happened in parallel, outside of charter
- Can we clean up a spec that governs historical data?

Designated Revoker (!18)

- We deprecated “Revocation Key”:
 - Embeds (unversioned) fingerprint on the wire
 - Isn’t usable by a relying party that can’t find the key itself
 - Presumptively references external TPK, leaks social graph
- Delegated revocation for v6 keys can only be done now with escrowed revocation certs
 - Escrowed revocation certs are static, can’t reflect time of loss or reason.
- Proposal: “Designated Revoker” (subpacket type ID 36):
 - Contains full pubkey material (usable directly, no fingerprint wrangling)
 - Doesn’t need to be any particular Transferable Public Key (no social graph)
- No known current implementations

Attestation Signatures (!60) aka 1PA3PC

- Certificates can grow without bound due to 3rd-party certifications.
- Ensure that the primary key agrees to each certification
 - “First-party-attested third-party certifications” (1PA3PC)
- 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: GnuPG and PGPpy
- Consumers?

User ID conventions (!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.
- Proposal: 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?

Other cleanup?

- You know it's out there...
- Specific items in charter? Or general “cleanup”?