Replacement Key Mechanism

draft-gallagher-openpgp-replacementkey

Daphne Shaw, Andrew Gallagher

OpenPGP @ IETF 119

Current status

draft-gallagher-openpgp-replacementkey

- Based on draft-shaw-openpgp-replacementkey (2001)
- New signature subpacket for use in revocations
- Similar design to intended recipient subpacket:
  - Version of new key
  - Fingerprint of new key
- Provides a hint for how to find a new key
  - This must still be verified by the usual means

Usage scenario

draft-gallagher-openpgp-replacementkey

- Key owner wishes to roll their key (say to upgrade to PQC)
- Key owner creates a new key, and (preferably) certifies it with their old key
- Key owner soft-revokes the old key
  - …attaching a replacement key subpacket pointing to the new key
- Correspondent refreshes the old key and finds the revocation
  - They follow the reference to the new key and download it
  - Trust calculation should accept the new key as a usable key

Discourse

draft-gallagher-openpgp-replacementkey

- DKG:
  - this embeds another fingerprint in the wire format
  - hard-codes a particular hash algorithm
  - may not be safe long term
- ABG:
  - fingerprints are in widespread use already
  - should be safe for short/medium term indirections
  - replacing them is a long-term strategy

Further information

draft-gallagher-openpgp-replacementkey

- Draft: https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-replacementkey
- Repo: https://andrewgdotcom.gitlab.io/draft-gallagher-openpgp-replacementkey