OpenPGP Key Replacement

draft-ietf-openpgp-replacementkey

Daphne Shaw, Andrew Gallagher

OpenPGP @ Interim February 2025

Basic Design — Recap

draft-ietf-openpgp-replacementkey

- New signature subpacket for use in direct self-sigs and key revocations
- Contains a class (flags) octet, and one or more target records of the form:
  - ((Record length || Target version || Target fingerprint || Target imprint))
  - Imprint of the target key is similar to the fingerprint, but uses the sig's hash algo
- Can be used in normal or "inverse" directions, distinguished by a flag bit in the class
  - Paired normal and inverse subpackets form a key equivalence binding
- Provides a hint for how to find a new key, and a preferred ordering of equivalent keys

Recent Changes

draft-ietf-openpgp-replacementkey

- “No Replacement” now inferred from Reason for Revocation
- Removed references to Preferred Key Server subpacket
- Standardised treatment of undefined flag bits
- Target records have both fingerprint and imprint, and two-octet length
- Expanded UX guidance and clarifications

Major Outstanding Questions

draft-ietf-openpgp-replacementkey

- Make encryption fallback optional #30

Make Fallback Encryption Optional? (1/2)

draft-ietf-openpgp-replacementkey

- Equivalence binding has two meanings:
  - It allows upgrade from original to replacement key
  - It allows fallback encryption from replacement to original
- A keyholder might only want the first meaning:
  - “Trapdoor” upgrade without fallback
  - Could be configured using a class flag or a target flag
- https://gitlab.com/andrewgdotcom/openpgp-replacementkey/-/issues/30

Make Fallback Encryption Optional? (2/2)

draft-ietf-openpgp-replacementkey

- Pros:
  - Allows full control of semantics
  - Revoked original key(s) do not need to be fetched/refreshed
- Cons:
  - Might end up being rarely used (e.g. only if a keyholder loses both private key material of original and its revocation cert)
  - Target flags would require a wire format change
- We could allow target flags in principle, without specifying any now

Fallback Encryption (Decision)

draft-ietf-openpgp-replacementkey

- 0: Fallback always possible if equivalence binding exists (no change)
- 1: Per-target flags; fallback possible if 0x80.. set in target (MR17)
- 2: No per-target flags, fallback possible if 0x20.. set in class (for all targets)

- 3: (only if 1 not chosen) Allow per-target flags, but don’t specify any yet

Minor Outstanding Questions

draft-ietf-openpgp-replacementkey

- Is the draft terminology clear?

Timeline

draft-ietf-openpgp-replacementkey

- Feb 24 (2 weeks): new draft with outstanding questions addressed
- Mar/Apr: implementations?

Further Information

draft-ietf-openpgp-replacementkey

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