OpenPGP Key Replacement

draft-ietf-openpgp-replacementkey

Daphne Shaw, Andrew Gallagher

OpenPGP @ IETF 124 November 2025

Basic Design — Recap

draft-ietf-openpgp-replacementkey

- New signature subpacket for use in direct self-sigs and key revocations
- Provides a hint for how to find a new key, and a preferred ordering of equivalent keys
- 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 forward or reverse directions, distinguished by a flag bit in the class
  - Paired forward and reverse subpackets form an identity equivalence binding
  - Equivalence is transitive; identity claims are shared between all equivalent keys

Current Status

draft-ietf-openpgp-replacementkey

- Wire format is stable
- Draft text is mature and has numerous examples
- Lacks test vectors

Blocker: Interop and SOP

draft-ietf-openpgp-replacementkey

- Interop testing depends on SOP exposing an interface
- Final code point assignment depends on successful interop testing
- Multiple options proposed, limited discussion
  - https://gitlab.com/dkg/openpgp-stateless-cli/-/merge_requests/50
  - https://gitlab.com/dkg/openpgp-stateless-cli/-/merge_requests/52
  - https://gitlab.com/dkg/openpgp-stateless-cli/-/issues/124

Further Information

draft-ietf-openpgp-replacementkey

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