OpenPGP Key Replacement

draft-ietf-openpgp-replacementkey

Daphne Shaw, Andrew Gallagher

OpenPGP @ IETF 127 November 2026

Current Status

draft-ietf-openpgp-replacementkey

- Wire format is stable
- Draft text is mature, with examples and test vectors
- Two interoperating library implementations (go-crypto and rpgp)
- No application-level support yet

Optional Encryption Fallback (again)

draft-ietf-openpgp-replacementkey

- Old proposal: flags on each target record
  - Mark individual deprecated keys as “encrypt to” or “do not encrypt to”
  - Complex parsing, wire format change
- New proposal: zeroed-out “stop record”
  - Deprecated keys already an ordered list for encryption subkey selection
  - Subkey selection gives up at stop record, equivalence binding unaffected
  - Divides deprecated key list into two sub-lists

Outstanding decisions

draft-ietf-openpgp-replacementkey

- Generation of equivalence sets in SOP:
  - https://gitlab.com/dkg/openpgp-stateless-cli/-/merge_requests/50
- Encryption subkey selection in SOP:
  - https://gitlab.com/dkg/openpgp-stateless-cli/-/issues/124
- Stop record:
  - Defer to a future “encryption subkey selection” document?

Implementation

draft-ietf-openpgp-replacementkey

- Who is planning to implement?
  - Low level support in rPGP and go-crypto
  - No application implementations yet
- If not planning to implement, what is missing?

Further Information

draft-ietf-openpgp-replacementkey

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