OpenPGP New Proposals

Andrew Gallagher

OpenPGP @ IETF 124 November 2025

Media Types

draft-gallagher-openpgp-media-types

- RFC3156 specifies:
  - application/pgp-keys : ASCII-armored keyring (certificate bundle)
  - application/pgp-signature : ASCII-armored signature packet
  - application/pgp-encrypted : not an OpenPGP file type
    - Fixed string, only used as first part of multipart/encrypted
- RFC3156 pre-dates extension of “MIME Types” to “Media Types” in RFC4288
- No media types for messages, secret keys, non-armored formats…

Media Types

draft-gallagher-openpgp-media-types

- New media types for non-certificate content:
  - application/pgp-secret-keys
  - application/pgp-message
- New media type parameters for non-armored content:
  - application/pgp-keys;armor=true (default, for backwards compatibility)
  - application/pgp-keys;armor=false (RECOMMENDED)
- DRIVEBY: Permits prefixed v4 detached signatures in certificate bundles

Media Types

draft-gallagher-openpgp-media-types

- https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-media-types
- Repo: https://gitlab.com/andrewgdotcom/openpgp-media-types

PGP-GREASE

draft-gallagher-openpgp-grease

- 8 code points between 51 and 126, currently unallocated in any registry
- Reserves them for GREASE use in (almost!) all registries
- Implementations MAY generate (sub)packets with GREASE codepoints
  - Unknown code points SHOULD be gracefully ignored, but often aren’t
  - Errors can uncover interop failure in the wild
- Could be inserted by keyservers (carefully!)
- DRIVEBY: Aligns private/experimental area size to 16 (nybble)

PGP-GREASE

draft-gallagher-openpgp-grease

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

User Attributes

draft-gallagher-openpgp-user-attributes

- Third-party certifications cannot be reliably distributed
  - Cert owner may not permit distribution (via 1pa3pc or canonical bundle)
  - Cannot be appended to any other certificate, no other distribution channel
- Signature subpacket areas are not a solution
  - Newer signatures must duplicate the subpacket, leading to bloat
  - Unhashed subpacket areas are not bound, can be zeroed

User Attributes

draft-gallagher-openpgp-user-attributes

- Specifies Embedded Signature Attribute Subpacket
  - Same wire format etc. as Embedded Signature Subpacket
  - Allows revocation signatures to be distributed with issuer’s certificate
  - No duplication, only one User Attribute packet required
- Deprecates Image Attribute Subpacket

User Attributes

draft-gallagher-openpgp-user-attributes

- https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-user-attributes
- Repo: https://gitlab.com/andrewgdotcom/openpgp-user-attributes

Semantic Cleanup

draft-gallagher-openpgp-signatures

- Large parts of OpenPGP are loosely specified or undefined
- Holes at all layers in the stack:
  - Non-functional subpackets
  - Signature types with no (or contradictory) construction and/or semantics
  - Insufficient limits on recursion
  - Time evolution underspecified
  - “An implementation MAY use any reasonable method…”

Semantic Cleanup

draft-gallagher-openpgp-signatures

- Clarifies specification of 11 signature types and deprecates some usages
- Deprecates Signature Target subpacket
- Prevents recursive embedding of signatures within signatures
- Clarifies interpretation of conflicting subpackets
- Categorises subpackets and restricts subpackets to specific signature types
- Categorises signature types and links types to specific key flags
- …

Semantic Cleanup

draft-gallagher-openpgp-signatures

- Constrains message grammar
- Specifies deduplication of unhashed subpackets
- Radically simplifies calculation of certification and subkey validity
- Deprecates Revocable subpacket
- Expands upon revocation reasons and revocation workflows
- Specifies hard vs soft revocation
- …

Semantic Cleanup

draft-gallagher-openpgp-signatures

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