Proposed Topics for Rechartering

Daniel Huigens
Aron Wussler

IETF 116
2023-03-29

Automatic Forwarding

Transform a ciphertext to another recipient automatically on a server, preserving E2EE

- Useful for temporary automatic forwarding (e.g. when out of office) or distribution lists
- Based on Curve25519
- Requires changes for the forwarding final recipient when using ECDH, but not when using X25519 (or X448)

Draft: https://github.com/wussler/draft-forwarding

(Presented at IETF 114 and OpenPGP email summit)

Key Superseded

A mechanism to signal that a newer key is available/preferred, without necessarily revoking the current key

- Smooth the transition from v4 to v6, and to PQC
- Reference to the newer key such that an implementation can automatically detect or fetch it
- Legacy implementations can still use the old key

See: https://gitlab.com/openpgp-wg/rfc4880bis/-/merge_requests/222

Long-term Symmetric Keys

Allow encrypting messages with a managed symmetric key, stored in a keyring (as opposed to a password)

- Useful for encrypting drafts, sent messages, backup/archival, and other data that is only for the user themselves
- Can also re-encrypt the PKESKs of incoming messages, to allow key rotation, and improve performance of future decryption

Draft: https://gitlab.com/twisstle/openpgp-persistent-symmetric-keys

(Presented at IETF 114)

Forward Secrecy

Ensure that a future private key compromise does not affect past messages

- “Pretty Good Forward Secrecy”: short-lived keys + symmetric re-encryption + deleting old subkeys and PKESKs
- Perfect Forward Secrecy: e.g. double ratcheting

Domain Separation

Binds signatures and ciphertexts to a context on the application layer, preventing certain attacks such as decryption oracles.

Add an optional context parameter:

- For encryption/decryption (v2 SEIPD) in the AEAD data
- For signing/verification (v5 signatures) in the hashed data

See: https://gitlab.com/openpgp-wg/rfc4880bis/-/merge_requests/214

Key Verification

Verify keys distributed over insecure channels in an automated way, providing solid alternatives to manual fingerprint comparison

- QR codes
- OpenPGP-CA
- Key Transparency (presented at IETF 113, and BoF at IETF 116 this morning)

Questions?

Daniel Huigens
Aron Wussler

IETF 116
2023-03-29