HKP(S)

draft-gallagher-openpgp-hkp

Daphne Shaw, Andrew Gallagher

OpenPGP @ IETF 118

Current status

draft-gallagher-openpgp-hkp

- Based on draft-shaw-openpgp-hkp (2003)
- Added HTTPS/HKPS and hkp:/hkps: schemes
- Forbade short IDs, deprecated V3 keys
- Added op=stats, op=hget from SKS (but not other SKS paths)
- Mentioned CORS
- Updated HTTP status codes
- Cleaned up terminology, MUST and SHOULD
- Retconned options v modifiers

Future work

draft-gallagher-openpgp-hkp

- Key versions (keyver=3,4)
- Padding (option=pad)
- Role separation
  - Authority (SRV vs .well-known)
  - Recursive lookups
  - Relationship with WKD
- Authentication

Next Steps

draft-gallagher-openpgp-hkp

- Feedback from implementations, particularly clients
- Update for crypto-refresh
- Decide on scope of I-D
  - Fill out any remaining gaps
- Registry requirements
- … adoption?

Further information

draft-gallagher-openpgp-hkp

- Draft: https://datatracker.ietf.org/doc/html/draft-gallagher-openpgp-hkp
- Repo: https://andrewgdotcom.gitlab.io/draft-gallagher-openpgp-hkp
  - draft-gallagher-openpgp-hkp.md (Internet Draft)
  - openpgp-conformal-padding.md (discussion document)
    - Preserves anonymity class across (de)armoring roundtrip
  - openpgp-key-discovery.md (discussion document)
    - SRV vs .well-known, HKP vs WKD