Changes in `crypto-refresh`

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

IETF 116

OpenPGP session

2023-03-29

Since `crypto-refresh-07`

- v5 ⟶ v6 (Keys, Sigs, PKESK, SKESK)
- v6 signature trailer length field width
- v6 signature salt size bound to hash algo
- Forbid El Gamal with v2 SEIPD
- v6 cleartext secret key material has no checksum
- New pubkey algorithms: X25519 and X448 (see next slides)
- Novel v3 PKESK padding for X25519 and X448

Since `crypto-refresh-08`

(in git)

- v3 PKESK for X25519/X448: no padding, cleartext symmetric algorithms
- Guidance on Regex null termination