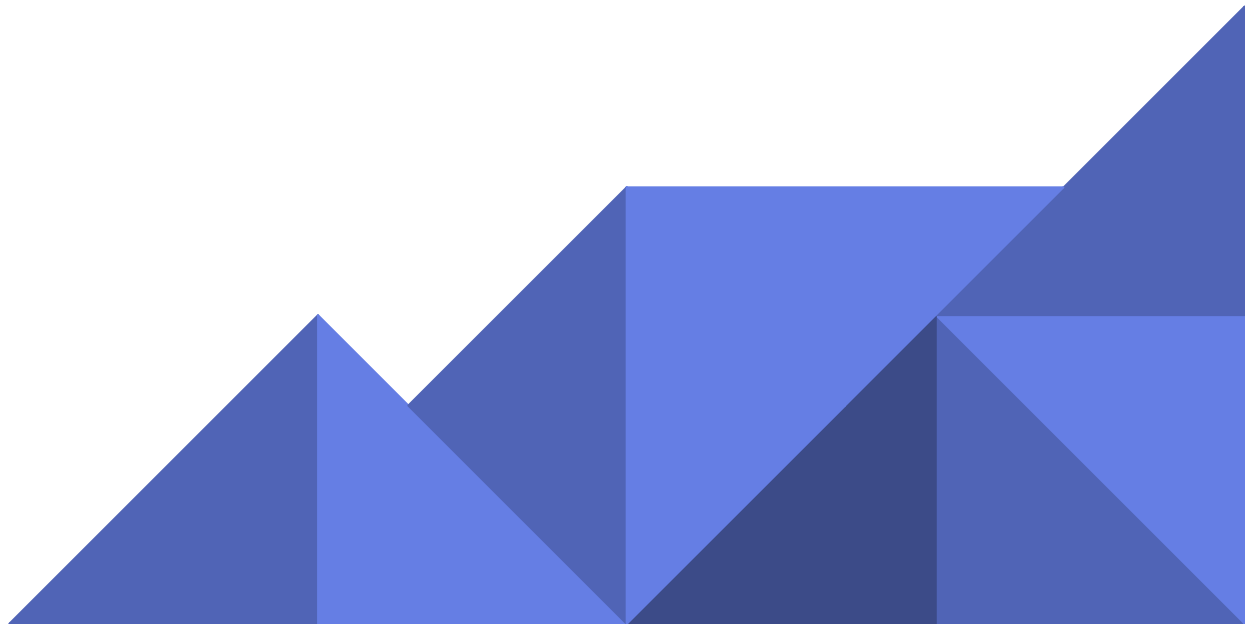
IETF 114

Persistent Symmetric Keys

Daniel Huigens



2022-07-29

Status Quo

Asymmetric Keys

- Stored in a keyring
- Long-term

Symmetric Keys

- Derived from a passphrase
- Single-use

Status Quo

Asymmetric Keys

- Stored in a keyring
- Long-term

Symmetric Keys

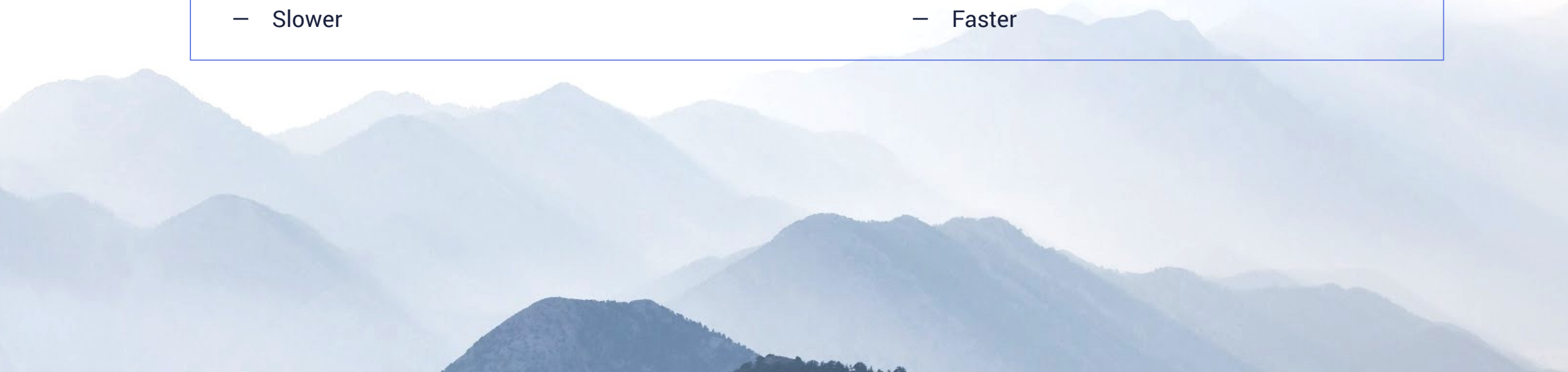
- Derived from a passphrase
- Single-use

Asymmetric Cryptography

- Vulnerable to quantum computers
- Slower

Symmetric Cryptography

- Less vulnerable (for larger key sizes)
- Faster



Our Goal

Persistent Keys

- Stored in a keyring
- Long-term

Symmetric Keys

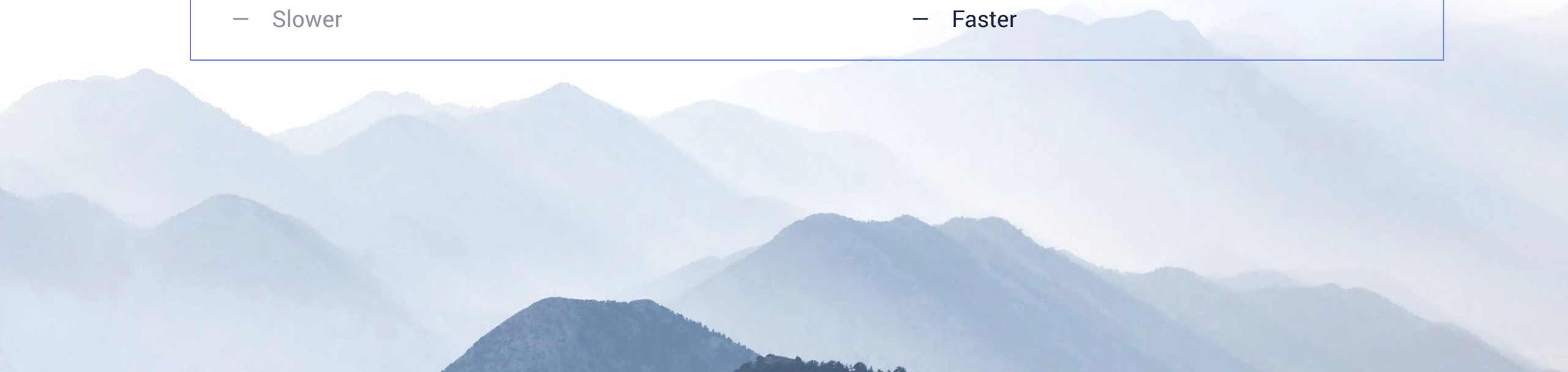
- Derived from a passphrase
- Single-use

Asymmetric Cryptography

- Vulnerable to quantum computers
- Slower

Symmetric Cryptography

- Less vulnerable (for larger key sizes)
- Faster



Use Cases: Symmetric Encryption

- Symmetric file / backup encryption
- Symmetrically re-encrypt incoming messages for archival
- Symmetrically encrypt drafts

Use Cases: “Symmetric Signatures” / MACs

- Symmetric key binding signatures
- Symmetric file signatures / tamper detection
- Storing signature verification results

Proposed Solution

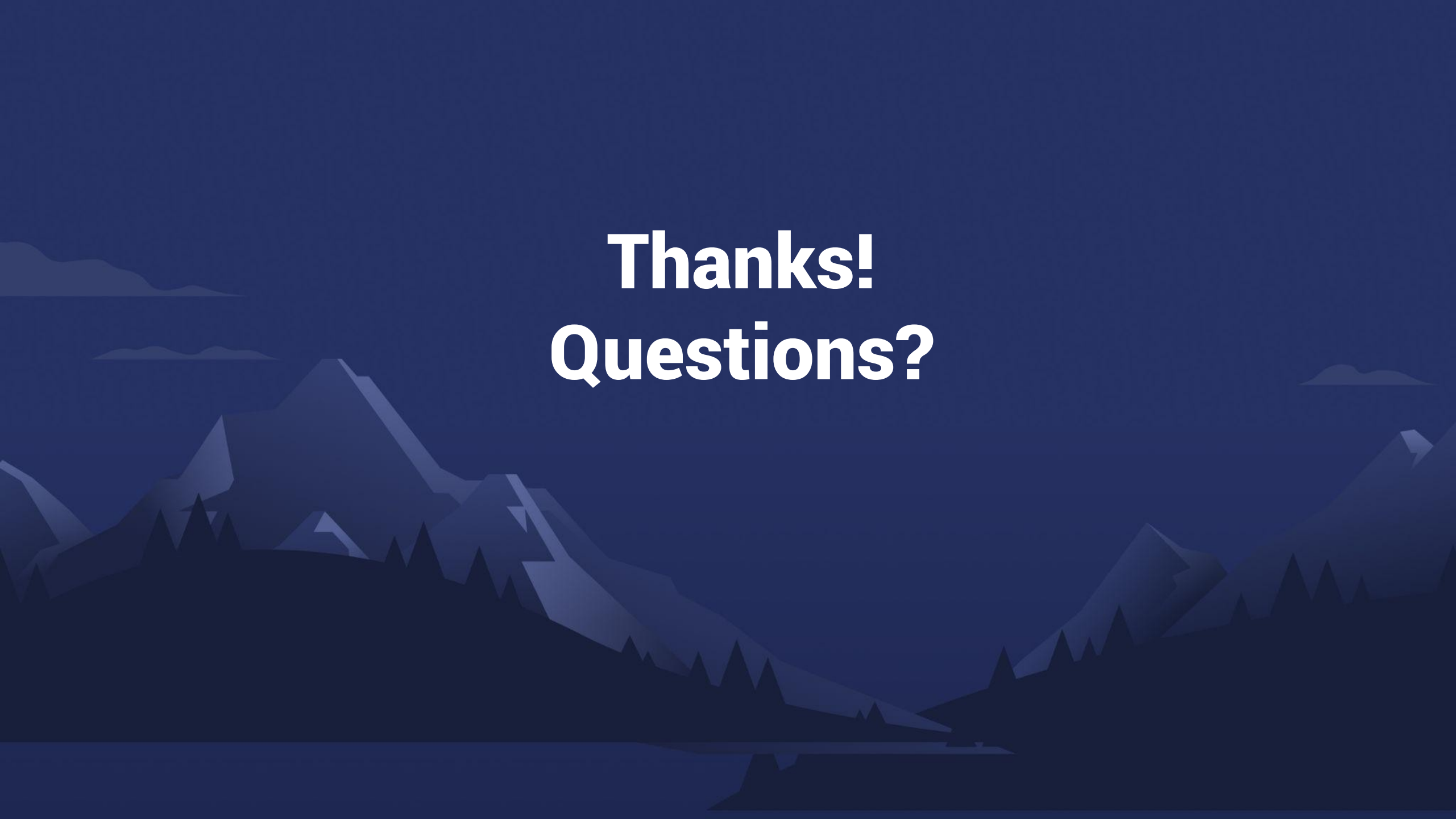
- Define two new “public key algorithms”: AEAD and HMAC
- These can go in a secret key packet, signature packet, or public-key encrypted session key packet
- Retcon PKESK and SKESK?
  - Persistent-Key Encrypted Session Key / Derived-Key Encrypted Session Key
  - Personal-Key Encrypted Session Key / Shared-Key Encrypted Session Key

Current Status

- Experimental implementations in forks/branches of OpenPGP.js and go-crypto
- https://gitlab.com/twiss1/openpgp-persistent-symmetric-keys
- https://twiss1.gitlab.io/openpgp-persistent-symmetric-keys/

Questions for the WG

- Interest in this?
- Next charter?
- Reasonable solution?
- Please read the draft :)


Thanks!
Questions?