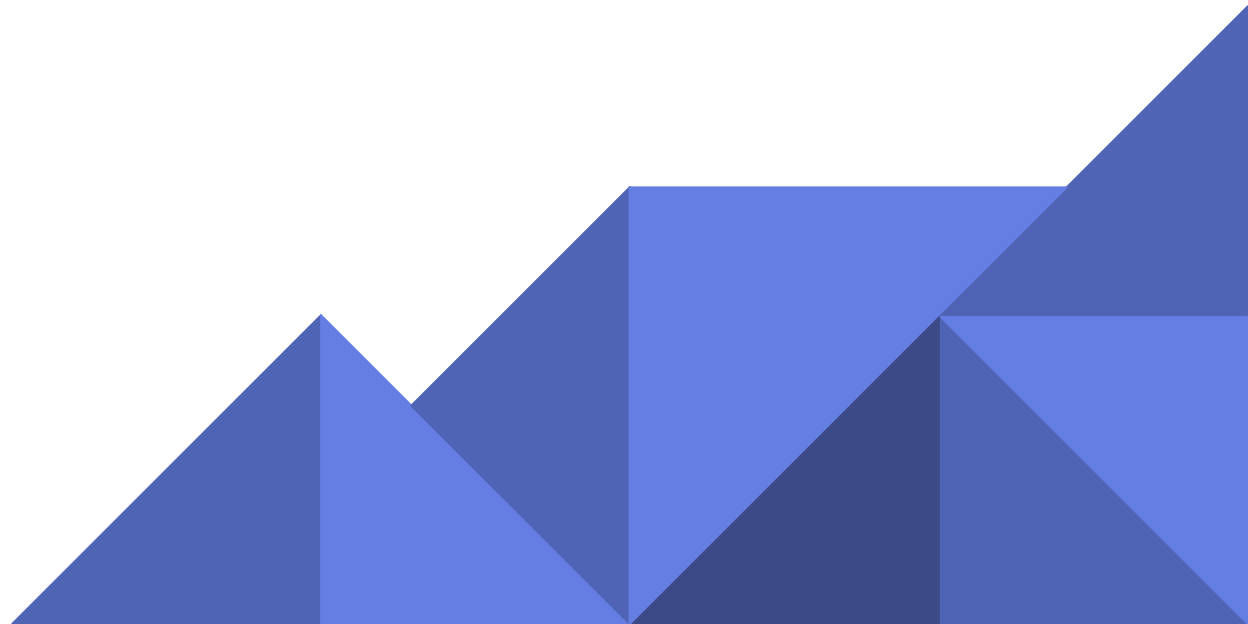
IETF 119

Persistent Symmetric Keys

Daniel Huigens



2024-03-20

What & Why?

- Encrypt messages using long-term symmetric keys, e.g. for archival
- Create attestations using long-term symmetric keys, e.g. to record signature verifications
- Faster & smaller than asymmetric crypto, & post-quantum secure

How?

- The semantics we need are those of PKESK and signature packets
- So: retcon “Public Key Algorithms” to “Persistent Key Algorithms”
- Define two new Persistent Key Algorithms: AEAD and HMAC

New ~~Public~~ Persistent Key Algorithms

ID	Alg.	Public Key	Secret Key	Signature	PKESK
128?	AEAD	sym. algo, hash(seed)	seed, key material	N/A	AEAD algo, IV, length, ciphertext
129?	HMAC	hash algo, hash(seed)	seed, key material	authentication tag	N/A

New ~~Public~~ Persistent Key Algorithms

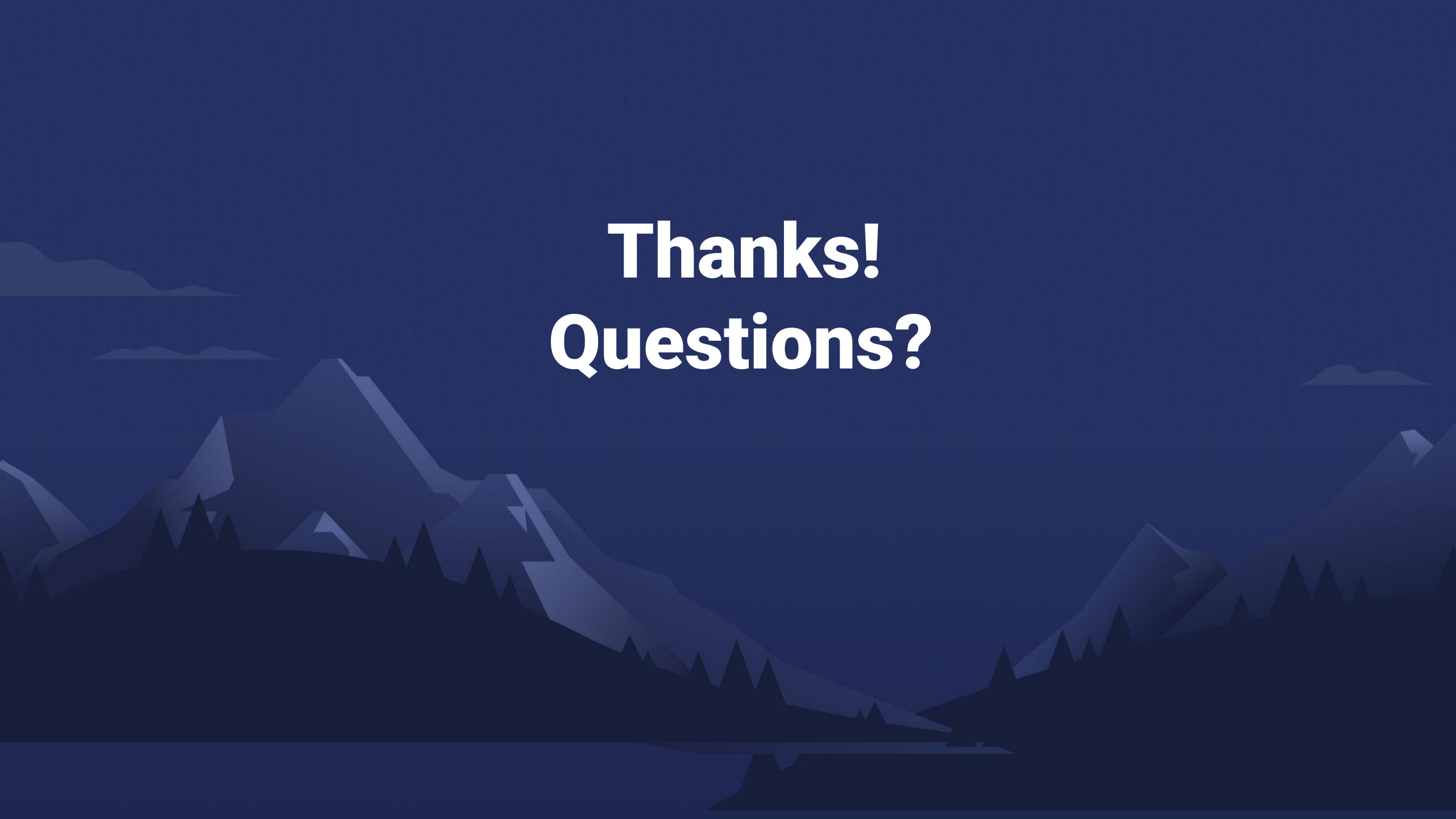
ID	Alg.	Public Key	Secret Key	Signature	PKESK
128?	AEAD	sym. algo, hash(seed)	seed, key material	N/A	AEAD algo, IV, length, ciphertext
129?	HMAC	hash algo, hash(seed)	seed, key material	authentication tag	N/A

Current Status

- Personal draft: draft-huigens-openpgp-persistent-symmetric-keys
- https://twisstle.gitlab.io/openpgp-persistent-symmetric-keys/
- Experimental implementations in forks/branches of OpenPGP.js and go-crypto

Questions for the WG

- Feedback?
- Call for adoption soon?


Thanks!
Questions?