Persistent Symmetric Keys

Changes

- Reduced number of reserved algorithm IDs for future symmetric algorithms
- Tied persistent symmetric keys to v≥6 (on GitLab, not yet in latest draft)

Proposed algorithms

ID	Algorithm	Public Key Format	Secret Key Format	Signature Format	PKESK Format
128	AEAD	sym. algo, AEAD algo, fingerprint seed [Section 5.1]	key material	N/A	IV, ciphertext [Section 5.3]
129	HMAC [RFC2104]	hash algo, fingerprint seed [Section 5.2]	key material	authentication tag [Section 5.4]	N/A
130 to 140	Reserved for Future Persistent Symmetric Key Algorithms				
200 to 210	Private or Experimental Persistent Symmetric Key Algorithms				

Table 1: Persistent Symmetric Key Algorithm registrations

Not addressed

- Not possible to derive public key material from private key material

Deployment thoughts

- Thinking about whether to add a subkey or a separate key

Questions for the WG

- Are we approaching readiness?
- More implementations?

Thoughts? Questions?