draft-kampanakis-ml-kem-ikev2-03

Summary

- Introduces soon to be standardized, quantum-resistant ML-KEM to IKEv2 for PQ-hybrid and potentially PQ-pure key exchanges.
- Uses RFC9370. Does not define any new mechanisms.
- Requests “Transform Type 4 - Key Exchange Method Transform IDs” IANA codepoints
  - TBD36 for ML-KEM-768
  - TBD37 for ML-KEM-1024

Some details

- ML-KEM can be used in
  - IKE_INTERMEDIATE (RFC9242)
  - IKE_FOLLOWUP_KE (RFC9370)
  - IKE_SA_INIT
    - ML-KEM-512 would fit in one 1460B UDP packet.
    - ML-KEM-768, barely...
    - ML-KEM-768 is a SHOULD NOT.
- Keying material is derived as per RFC9370
  - SK_d, SK_a[i/r], and SK_e[i/r]
  - SKEYSEED and KEYMAT

Open questions

- Should we get a codepoint for ML-KEM-512?
  - It would fit in a IKE_SA_INIT
  - It could be used in a PQ-pure key exchange.
  - ML-KEM-512 has lower security level (close or slightly less than 128-bits depending on analysis). TLS converged towards using ML-KEM-768 to be more conservative regarding security level.

Path Forward?

- IPSECME WG draft or
- I-D to get codepoints from Expert Review as per IANA “Transform Type 4 - Key Exchange Method Transform IDs” ’s Registration Procedure.

Thank you