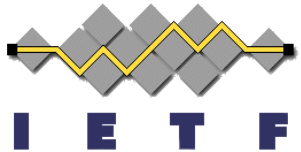
PQ/T Hybrid Composite Key Exchange & Reliable Transport for IKEv2

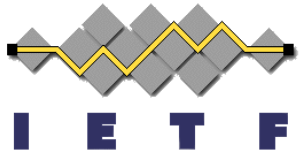
draft-reddy-ipsecme-ikev2-hybrid-reliable

Tirumaleswar Reddy, Valery Smyslov

IETF 125, Shenzhen

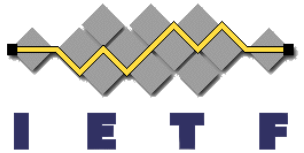


Background



- Large PQC KEMs may not fit in IKE_SA_INIT, forcing a fallback to traditional key exchange before PQC payloads can be exchanged.
  - PQC KEM public keys and ciphertexts are significantly larger than traditional DH values.
- The IKE_INTERMEDIATE exchange with IKE_FOLLOWUP_KE is then required to complete the PQ/T Hybrid Key Exchange.
- With IKE fragmentation, loss of a single fragment causes the entire set of fragments to be retransmitted.

Background

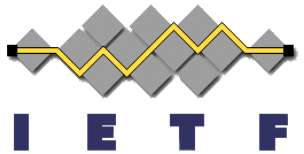


- These additional exchanges introduce multiple round trips and increase handshake latency.
- Current IKEv2 negotiation allows independent DH and ML-KEM selection, potentially creating **untested hybrid constructions**.
  - draft-ietf-pquip-pqc-engineers recommends a small number of well-defined hybrid configurations

Solution overview

- ietf-ipsecme-ikev2-reliable-transport allows separate Transports for IKE and ESP
  - Enables large PQC KEM payloads to be exchanged in IKE_SA_INIT
  - Avoids IKE fragmentation and retransmission of large PQC payloads

Solution overview

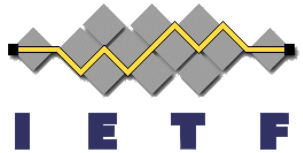


- IKE SA is initiated over TCP from the beginning
- Hybrid PQC + traditional key exchange performed during IKE_SA_INIT
- A combined KE payload format that carries both traditional and PQC components within a single payload
- PQ/T hybrid composite key exchange algorithms for IKEv2, representing single, fixed, known good combinations of traditional and PQC KEM algorithms.

Combined Key Exchange Payload

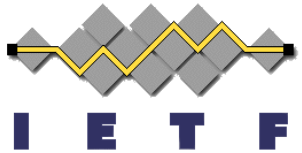
- Initiator sends: KEi = DH_public_i || PQC_public_i
- Responder returns: KEr = DH_public_r || PQC_ciphertext
- Hybrid key exchange completes during IKE_SA_INIT without additional key exchange

Hybrid Secret Construction



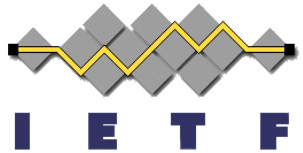
- Two shared secrets are produced
  - Tradiational ECDH shared secret
  - PQC KEM shared secret
- These are combined using the CFRG Universal Combiner (irtf-cfrg-hybrid-kems) defined for hybrid KEMs
  - Security holds if either the traditional or PQ component remains secure.

Integration with IKEv2 Key Schedule



- Combined hybrid secret feeds into the standard IKEv2 key schedule
- SKEYSEED = prf(Ni | Nr, K_combined)
  - K_combined replaces the traditional g^ir shared secret input to the IKEv2 key schedule.

PQ/T hybrid composite key exchange algorithms



- Each composite algorithm defines a fixed pairing of a traditional DH group and a PQC KEM.
  - ecp256-mlkem768
  - ecp384-mlkem1024
  - curve25519-mlkem768

draft-reddy-ipsecme-ikev2-hybrid-reliable

- Comments and suggestions are welcome
- Consider for WG adoption