Post-Quantum Traditional (PQ/T) Hybrid PKI Authentication in IKEv2

IETF 123 Madrid

`draft-hu-ipsecme-pqt-hybrid-auth-02`

Hu Jun — Nokia

Yasufumi Morioka — NTT DOCOMO

Wang Guilin — Huawei

Recap: Problem Statement

- The newly published PQC algorithms need time to be field proven
- IKEv2 PQ/T hybrid PKI authentication uses one traditional key (e.g. RSA) + one PQC key (e.g. ML-DSA) for PKI authentication
- Hybrid authentication is secure as long as at least one component authentication is secure

Recap: Design Choices

1. Hybrid AUTH payload format is SAME as digital signature auth(RFC7427), but with a new IANA assigned auth method
2. For reason of efficiency, instead of multiple exchanges(RFC4739), using single exchange for auth; specially considering hybrid auth is likely to be used along with hybrid key exchange.
3. Given #1, always use a composite signature for both type-1 and type-2; to avoid reinventing wheel, and also consistent with cert verification, follow composite signature scheme specified in draft-ietf-lamps-pq-composite-sigs
4. Use SUPPORTED_AUTH_METHODS (RFC9593) for hybrid auth algorithm combination announcement

What IKEv2 payload are changed by the draft

- A new SUPPORTED_AUTH_METHODS format
- A new AUTH method value

There is no changes to AUTH or CERT payload, the draft reuse digital-signature AUTH payload format and specifies how to compute it with type-1 or type-2 setup

CA Setup type-1 and type-2

- Type-1: a single pair of composite cert/key, specified by ietf-lamps-pq-composite-sigs
- Type-2: two pairs of non-composite cert/key, specified by RFC9763

Both are valid options for hybrid PKI setup that we need to support, and a single solution is preferred.

Why not do multiple AUTH exchanges (RFC4739) for type-2?

1. Prefer a single solution
2. To minimize number of exchange given it is already much bigger with hybrid KE
   - But it will increase the packet size
     - Sure, but the packet size is already big even with single traditional or PQC AUTH/Cert, we will NOT avoid fragmentation by doing multiple AUTH exchanges
     - Also single AUTH exchange with 2x fragments is simpler and more effiecent than two AUTH exchanges with 1x fragments each

Why use ietf-lamps-pq-composite-sigs method to generate/verify signature in AUTH

ietf-lamps-pq-composite-sigs is needed to verify certificate chain after AUTH payload verification, so don’t see a point of having a different way for AUTH payload processing

Key reuse

The use of ietf-lamps-pq-composite-sigs means component keys are not supposed to used for any other purposes for security reason, however as point out in 10.3 of draft-ietf-lamps-pq-composite-sigs-07, having an IKEv2 hybrid auth specific ctx (“IKEv2-PQT-Hybrid-Auth“) helps to mitigate key reuse issue

Key changes in -02

- dropping support for PreHash ML-DSA, change example to Pure Signature ML-DSA
  - 02 was updated at time with ietf-lamps-pq-composite-sigs-04, however since ietf-lamps-pq-composite-sigs-05 changes to use ML-DSA pure mode with an explicit hash, so this part need to be updated to align with it

Question?