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

IETF 121 Dublin

`draft-hu-ipsecme-pqt-hybrid-auth-01`

Hu Jun
Nokia

Yasufumi Morioka
NTT DOCOMO

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

Two PKI Setups

- Type-1: single cert with composite key (e.g. draft-ietf-lamps-pq-composite-sigs)
- Type-2: two certs, a traditional key cert + a PQC key cert

To simplify solution, hybrid auth does not support other combinations (e.g. 1 PQC + 2 traditional)

Design Choices

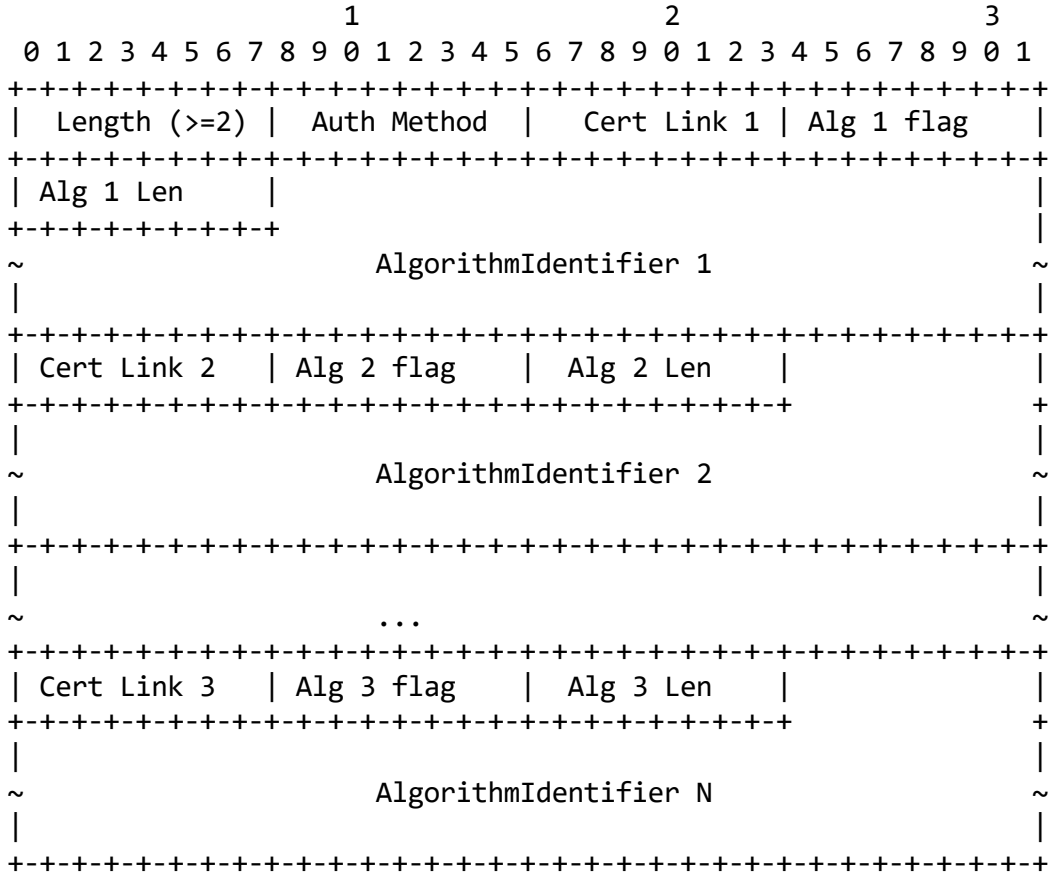
1. For reason of efficiency, instead of multiple exchanges(RFC4739), using single exchange for auth; specially considering hybrid auth is likely to be used along with hybrid key exchange.
   - This draft could be used along with RFC4739 if deemed necessary
2. Hybrid AUTH payload format is same as digital signature auth(RFC7427), but with a new IANA assigned auth method
3. Given #1, always use a composite signature for both type-1 and type-2; to avoid reinventing wheel, follow11 composite signature scheme specified in draft-ietf-lamps-pq-composite-sigs
4. Use SUPPORTED_AUTH_METHODS (RFC9593) for hybrid auth algorithm combination announcement

Example Call Flow with PPK

```
Initiator                          Responder
-------------------------------------------------------------------
HDR, SAi1, KEi, Ni,
          N(USE_PPK) -->
                  <--  HDR, SAr1, KEr, Nr, [CERTREQ,] N(USE_PPK),
                                        N(SUPPORTED_AUTH_METHODS)

HDR, SK {IDi, CERT+, [CERTREQ,]
        [IDr,] AUTH, SAi2,
        TSi, TSr, N(PPK_IDENTITY, PPK_ID),
        N(SUPPORTED_AUTH_METHODS)} -->
                             <--  HDR, SK {IDr, CERT+, [CERTREQ,]
                                        AUTH, [N(PPK_IDENTITY)]}
```

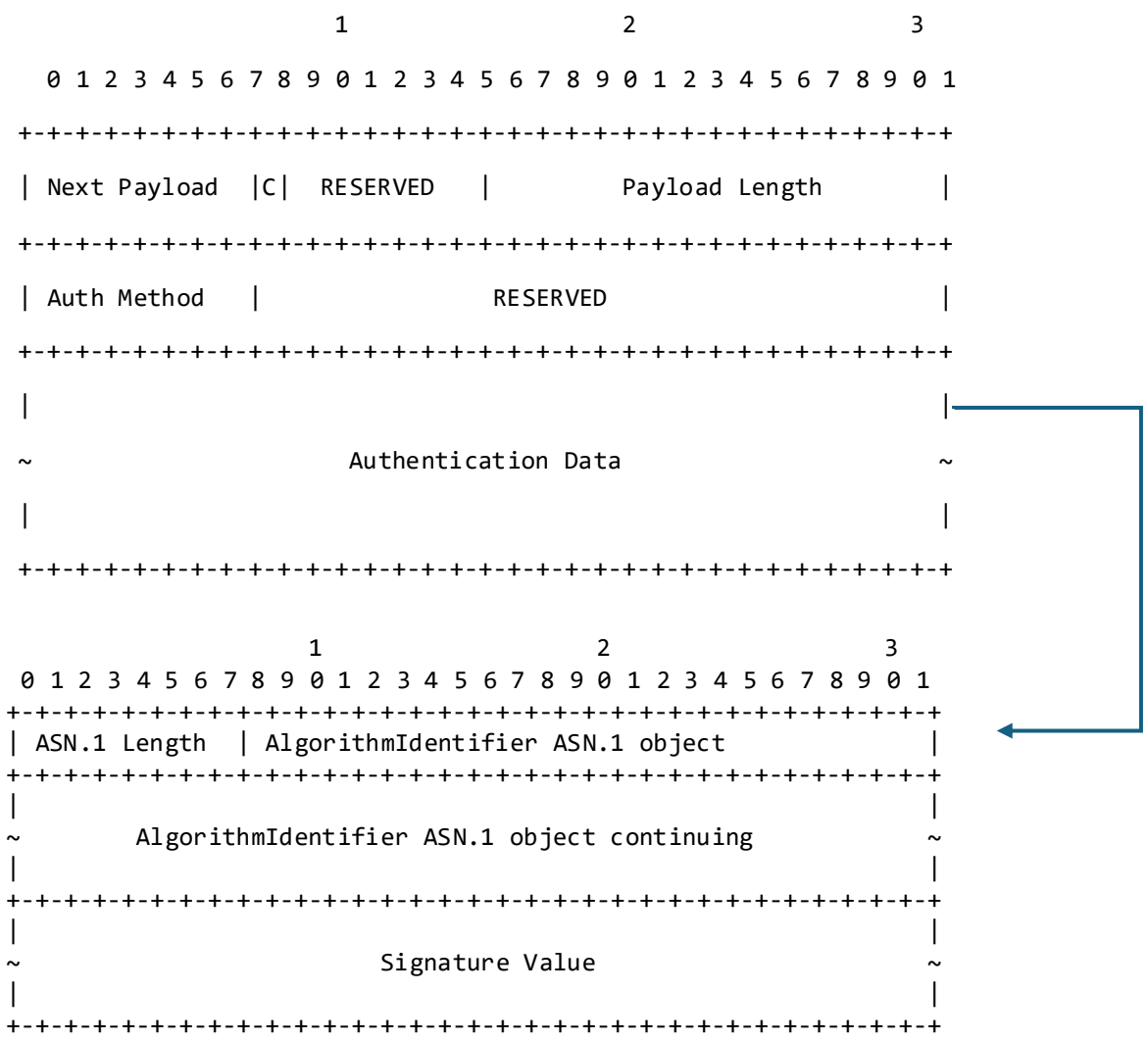
Announcement: SUPPORTED_AUTH_METHODS (RFC9593)



New Announcement Format

- Auth Method: A new value to be allocated by IANA
- Cert Link N: Links corresponding signature algorithm N with a particular CA. as defined in {{Section 3.2.2 of RFC9593}}
- Alg N Flag:
  - C: set to 1 if the algorithm could be used in type-1 setup
  - S: set to 1 if the algorithm could be used in type-2 setup
- AlgorithmIdentifier N: The variable-length ASN.1 object that is encoded using Distinguished Encoding Rules (DER) {{X.690}} and identifies the algorithm of a composite signature as defined in {{Section 7 of I-D.ietf-lamps-pq-composite-sigs}}.
- Announcement without any AlgorithmIdentifiers signals that there is no particular restrictions on algorithm.

Auth & Cert Payload



Type-1 initiator Example

1. selected combination: id-HashMLDSA44-RSA2048-PSS-SHA256, which uses Hash ML-DSA-44

2. Follow {{Section 4.3.1 of I-D.ietf-lamps-pq-composite-sigs}} with following input:

    - sk is the private key of the signing composite key certificate

    - M is InitiatorSignedOctets

    - ctx is "IKEv2-PQT-Hybrid-Auth"

    - PH is SHA256

Type-2 Example

almost same as type-1, just use component key directly, with same example:

  - mldsaSK is the private key of ML-DSA certificate, tradSK is the private key of the RSA certificate

  - M is InitiatorSignedOctets

  - ctx is "IKEv2-PQT-Hybrid-Auth"

  - PH is SHA256

The signing PQC certificate MUST be the first CERT payload in the IKEv2 message, while traditional certificate MUST be the second CERT payload.

Question?