Multi-Authentication in IKEv2

draft-wang-ipsecme-multi-auth-ikev2-pq-00

IPSECME, IETF 125 @ Shenzhen

19/3/2026

Guilin Wang and Wei Pan

Multi-Authentication in IKEv2

❑ Information of our draft

- **Title**: **Multi-Authentication in IKEv2 with Post-quantum Security**
- draft-wang-ipsecme-multi-auth-ikev2-pq-00
- https://datatracker.ietf.org/doc/draft-wang-ipsecme-multi-auth-ikev2-pq/

❑ PQ Authentication in IKEv2

- **RFC 9593 (Announcing Supported Authentication Methods in IKEv2).**
  - One peer indicates the list of supported authentication methods to the other while establishing IKEv2 SAs
  - SUPPORTED_AUTH_METHODS Notification to improve interoperability for authentication method negotiating
  - 3 types of announcements specified: for MAC, for a specific signature auth. & for a general signature auth.
- ML-DSA, SLH-DSA or any PQ signature authentication: Signature Authentication in IKEv2 using PQC (draft-ietf-ipsecme-ikev2-pqc-auth-06)
- Composite Signature Authentication: PQ/T Hybrid PKI Authentication in IKEv2 (draft-hu-ipsecme-pqt-hybrid-auth-04)

❑ Motivations

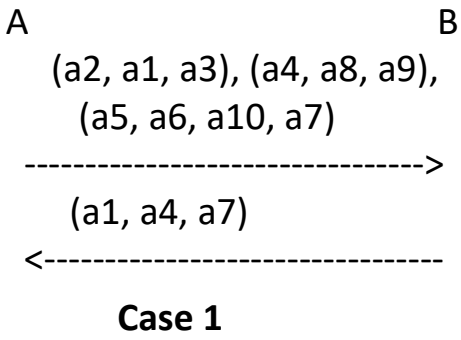
- **IKEv2 may need a flexible multiple authentication, where**

  - both peers are able to negotiate multi-authentication methods in IKEv2 according to their local policies; and
  - authentication methods selected do not necessarily belong to the same category.
  - **Examples:** MAC + PQ signature, PSK + PQ signature, T signature + PQ signature, MAC + T signature + PQ signature, …

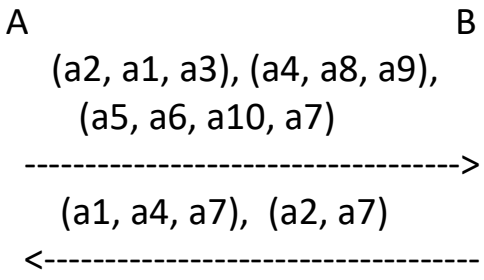
Multi-Authentication in IKEv2

- **The proposed solution**
  - **Basic idea: Mimic the means of negotiating ADDKE in RFC 9370**
    1) A sends multiple authentication method sets to B.
    2) B selects one authentication method in each set and sends the answer to A.
    3) These authentication methods selected will be used by B to authenticate itself to A.
  - Similar procedures can be done to negotiate the multi-authentication methods for A to authenticate itself to B.
  - **This draft specifies how to extend the Authentication Methods Announcements (RFC 9593) to achieve the above.**
- **Compact answers to save communications**
  - **1 authentication method set:** Both A and B will use the same methods to authenticate each other.
  - **2 authentication method sets:** the 1st set for A to authenticate B, and the 2nd set for B to authenticate A.
  - **3 authentication method sets:** the 1st set for A to authenticate B, and other sets for expressing B's authentication policy.

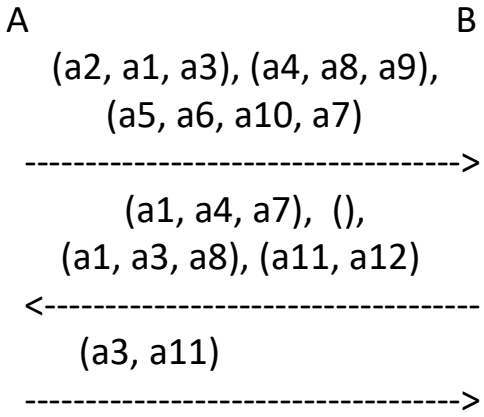
Examples: A and B negotiate multi-authentication with 12 algorithms



Case 1



Case 2



Case 3

Multi-Authentication in IKEv2

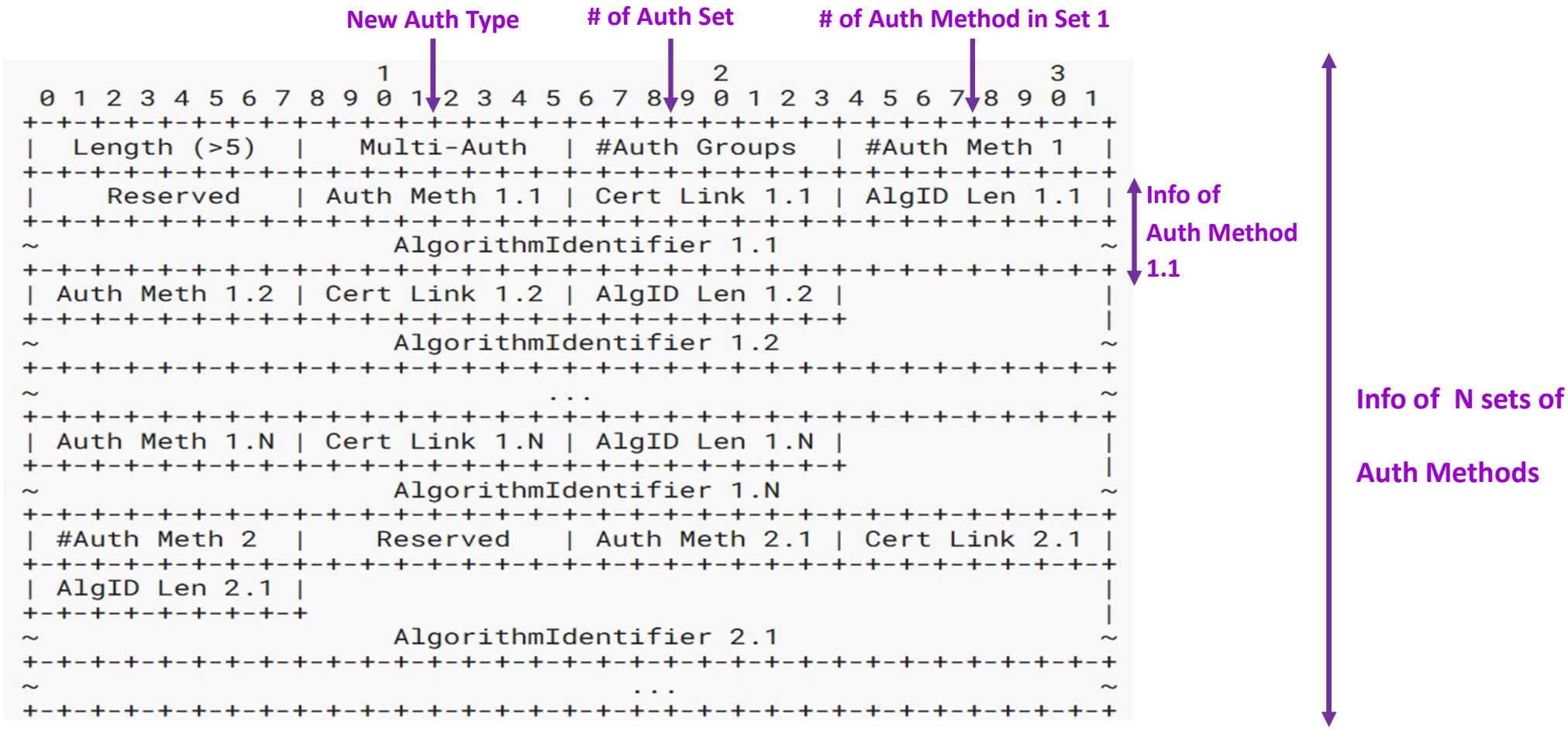


Fig. 3 Payload Format for Multi-Authentication Announcement

Multi-Authentication in IKEv2

```
Initiator                                                    Responder
-----------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*..), --->
KEi, Ni, N(INTERMEDIATE_EXCHANGE_SUPPORTED), ..
                    <--- HDR(IKE_SA_INIT), SAr1(.. ADDKE*..), [CERTRQ,]
                         KEr, Nr, N(INTERMEDIATE_EXCHANGE_SUPPORTED), ..
                         N(SUPPORTED_AUTH_METHODS(17((a2a1a3),(a4a8a9),(a5a6a10a7))))

                     ... (IKE_INTERMEDIATE for ADDKE) ...

HDR(IKE_AUTH), SK{IDi, [CERT,] [CERTRQ,]
[IDr,] AUTH, SAi2, TSi, TSr,
N(SUPPORTED_AUTH_METHODS(17(TBD)(a1a4a7),(a2a7)))} --->
                     ... (IKE_INTERMEDIATE for [CERT,]) ...
                    <--- HDR(IKE_AUTH), SK{IDr, [CERT,] AUTH, SAr2, TSi, TSr}
                                    ... (IKE_INTERMEDIATE for [CERT,]) ...
```

Fig. 1 An Example of Multi-Authentication between Two Peers

Multi-Authentication in IKEv2

Appreciate your you comments and reviews!

Thanks!