Multi-Authentication in IKEv2

draft-wang-ipsecme-multi-auth-ikev2-pq-01

IPsec Workshop @ Vienna

17/7/2026

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-01
- 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-05)

Multi-Authentication in IKEv2

❑ **Intuitive Motivations**

- Similar thing for ID verification when opening a bank account
- **(A or B) and (C or D) and E**

https://www.thebalancemoney.com/how-can-i-easily-open-bank-accounts-315723

❑ **Technical 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.
    (More complex than Key Exchange!)
  - **Examples:** MAC + PQ signature, PSK + PQ signature, T signature + PQ signature, MAC + T signature + PQ signature, …
- **Offer better backward compatibility.**

Multi-Authentication in IKEv2

❑ Comparison with RFC 4739 – Multiple Authentication

Section 1 in [RFC4739]:
"*For instance, it may be necessary to authenticate both the host (machine) requesting access, and the user currently using the host.* "

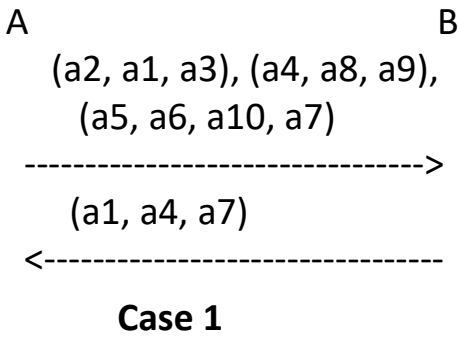
	Our Mult-Authentication	**Multiple Authentication [RFC 4739]**
Purposes	to enhance cryptographic resilience against quantum attacks.	mainly to facilitate verification at different domains in IKEv2.
	to run multiple authentications in IKEv2	mainly considers how to run Extensible Authentication Protocol (EAP) methods with Authentication Methods in IKEv2
Mechanisms	**extending the authentication announcement [RFC9593]:** • the two peers can negotiate two or more authentication methods in IKEv2.	**realized via two types of notification**: • indicate their willingness: to run further authentication: first run MULTIPLE_AUTH_SUPPORTED notification in the IKE_SA_INIT response and the first IKE_AUTH request. • complete the second authentication: they exchange ANOTHER_AUTH_FOLLOWS notification in any IKE_AUTH message. • More further authentication if necessary ...
	Running PQ algorithms (large sizes, fragmentation,..) Published in 2006 • Based on RFC 7383, RFC 9242, a& RFC 9593.	• Published in 2006 • No PQ consideration at all

Section 2.1 in [RFC4739]:
"*it is assumed that both peers know what credentials they want to present; there is no negotiation about, for instance, what type of authentication is to be done.*" "

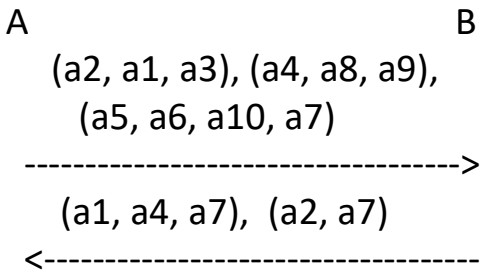
Multi-Authentication in IKEv2

- **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.

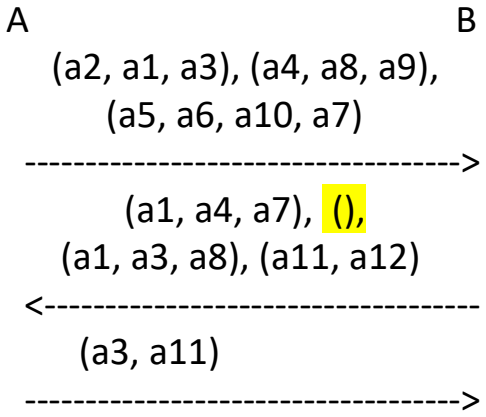
Examples: A and B negotiate multi-authentication with 12 algorithms



Case 1



Case 2



Case 3

Multi-Authentication in IKEv2

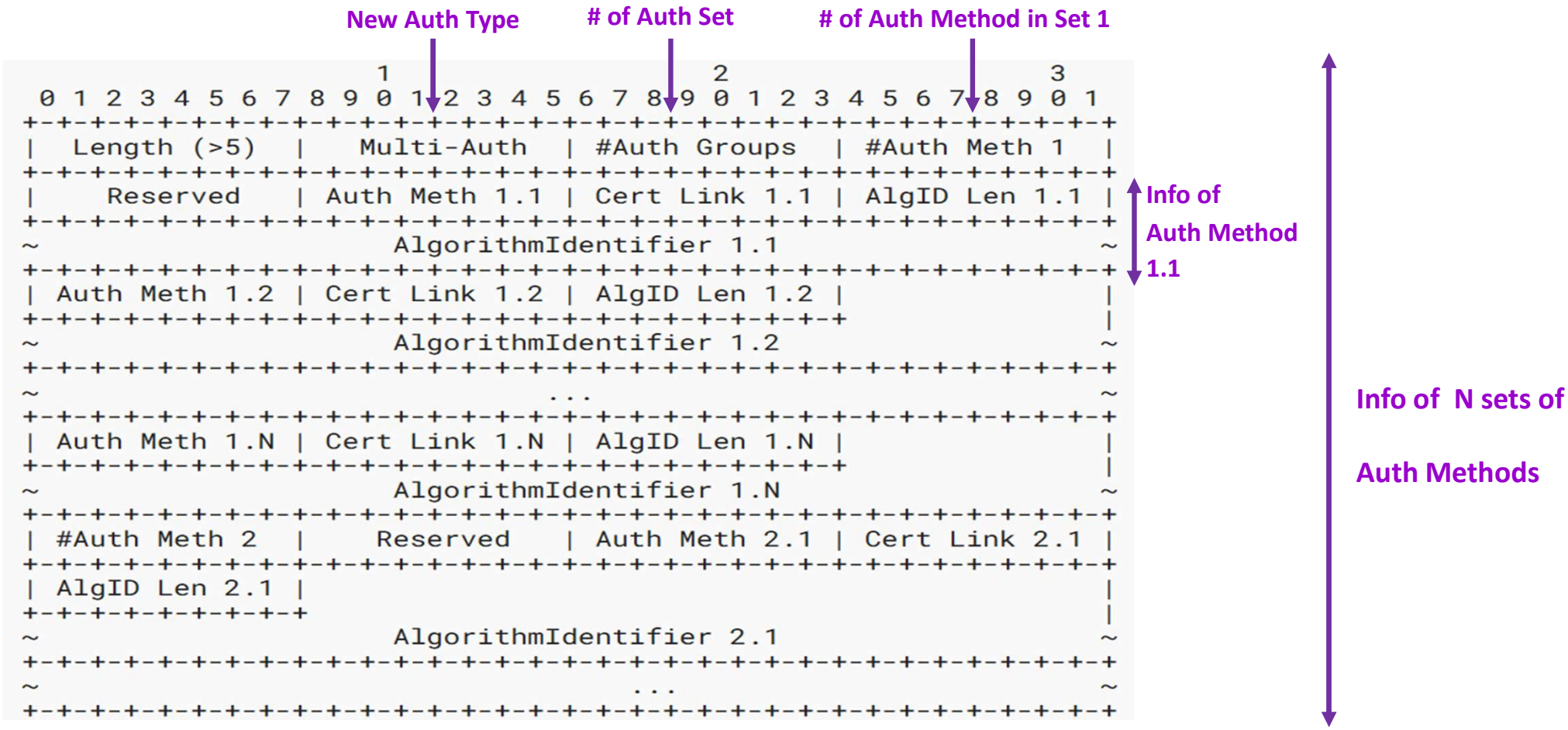


Fig. 3 Payload Format for Multi-Authentication Announcement

Multi-Authentication in IKEv2

❑ Notation

- **Length**: Length of the whole blob of the announcement in octets; must be greater than 5.
- **Multi-Auth**: The value of "Multi-Authentication", which is supposed to be 17 (TBD).
- **#Auth Group**: The number of Authentication Groups listed in this announcement.
- **#Auth Meth**: The number of Authentication Methods in a given authentication group.
- **Reserved**: One byte reserved for future use.
- **Auth Method**: The value of one announced authentication method in a given authentication group.
- **Cert Link**: Links this announcement with a particular CA, which issued the public certificate for the Auth Method identified in AlgorithmIdentifiers below; see Section 3.2.2 of [RFC9593] for detail. If this Auth Method is not related to the certificate, this information MUST be ignored.
- **AlgID Len**: Length of each authentication method algorithm ID, that is identified in AlgorithmIdentifier below, in octets.
- **AlgorithmIdentifier**: One or more variable-length ASN.1 objects that are encoded using Distinguished Encoding Rules (DER) [X.690] to identify one specific Authentication Method algorithm.

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: Issues for AUTH

- To complete each Authentication Method separately or in a combined way?
- Special considerations for KEM-based authentication, PAKE?
- Good for some applications of IPsec?
- Other issues, improvements, …?

Multi-Authentication in IKEv2

Appreciate your you comments and reviews!

Thanks!