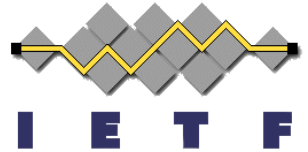


Hybrid Post-Quantum and Traditional Authentication for IKEv2

[draft-reddy-ipsecme-pqt-hybrid-auth](#)

Tirumaleswar Reddy, Scott Fluhrer

IETF 126, Vienna

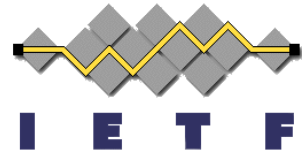


Composite Signatures



- Combines PQC and traditional signatures/public keys
- Verification succeeds only if both signatures verify
- One AlgorithmIdentifier identifies the composite scheme, including the full parameter set of each constituent algorithm
- Composite ML-DSA for use in X.509 PKI
<https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/> is submitted to IESG

Motivation for PQ/T Hybrid Authentication



- A CRQC can break the traditional public-key algorithms (RSA, ECDSA) typically used for IKEv2 authentication
- Uncertainty remains for both traditional and PQC algorithms during the migration
- Composite signatures provide defence-in-depth
 - Authentication remains secure as long as at least one component algorithm remains unbroken
 - Risk of bugs or vulnerabilities in ML-DSA implementations

IKEv2 Integration: No On-Wire Protocol Changes



- Reuses the "Digital Signature" authentication method (RFC 7427)
 - Composite signature carried in the AUTH payload "Signature Algorithm" field as a single AlgorithmIdentifier
- Standard AUTH payload format (RFC 7296)
- Composite algorithms advertised via SUPPORTED_AUTH_METHODS (RFC 9593)
- No new payloads, exchanges, notifications, or message formats

Exchanges: Standard IKEv2 Flow



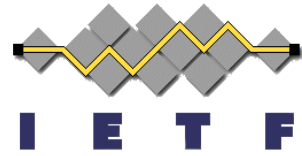
Initiator

Responder

```
-----
HDR, SAi1, KEi, Ni -->
    <-- HDR, SAR1, KEr, Nr, [CERTREQ,]
        N(SUPPORTED_AUTH_METHODS)
HDR, SK {KEi(1)} --> (IKE_INTERMEDIATE)
    <-- HDR, SK {KEr(1)}
HDR, SK {IDi, CERT+, [CERTREQ,] [IDr,] AUTH,
    SAi2, TSi, TSr,
    N(SUPPORTED_AUTH_METHODS)} --> (IKE_AUTH)
    <-- HDR, SK {IDr, CERT+, AUTH, SAR2, TSi, TSr}
```

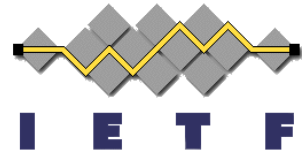
- ML-KEM key exchange via IKE_INTERMEDIATE (RFC 9242 / RFC 9370); key exchange is independent of the authentication mechanism
- Same exchanges as any certificate-based IKEv2 deployment

Composite Certificate Processing



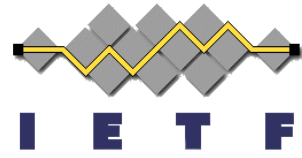
- End-entity certificate MUST contain a composite public key (ietf-lamps-pq-composite-sigs)
- Composite signature algorithm in AUTH MUST match the end-entity certificate public key algorithm; mismatch fails the IKE_SA negotiation
- Signing and verification per the composite scheme; internal hashing and preprocessing are opaque to IKEv2
- One certificate chain and one AUTH payload provide hybrid assurance

Key Exchange and Message Size



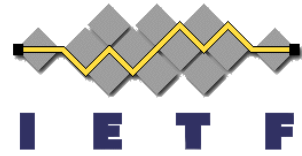
- Hybrid authentication paired with a PQ/T hybrid or a post-quantum key exchange; otherwise a CRQC attacker can recover the SA keying material
- PQC signatures and certificate chains increase IKE_AUTH message size
- Implementations MUST support IKEv2 Fragmentation (RFC 7383)

Negotiation and Downgrade Protection



- Brownfield upgrades: a peer can offer traditional-only, composite-only, or both; existing IKEv2 mechanism selects cleanly
- If hybrid authentication is required by policy, a non-composite certificate or signature **MUST** fail the IKE_SA negotiation

EUFCMA is Sufficient for IKEv2



- **Composite gives EUFCMA:** forging needs breaking both components; survives a break of one algorithm
- **What SUFCMA adds:** only prevents a *different* valid signature on an *already-signed* message.
- Fresh nonces and SPIs make the signed octets unique per IKE SA; impersonation requires a valid signature on a new IKE SA's signed octets, which composite prevents

Peer identity can't be spoofed even if one of the two algorithms breaks

Next Steps

- Complements draft-ietf-ipsecme-ikev2-pqc-auth: same framework (RFC 7427 + RFC 9593); PQC-only there, PQ/T hybrid here
- Comments and suggestions are welcome
- Consider for WG adoption