KEM-based Authentication for EDHOC

(draft-pocero-lake-authkem-edhoc-00)

Authors: L. Pocero Fraile, C. Koulamas, A. P. Fournaris, E. Haleplidis

Affiliations: ISI, R.C. ATHENA

Presenter: Lidia Pocero Fraile

May 26th, 2026

IETF

Motivation

- Provide a **KEM-KEM-based, signature-free authentication method** for **EDHOC** that:
  - Reduces memory overhead and processing time to support **more constrained devices**.
  - It's the method presented throughout Objective 1 as **KEM,** and when using ML-KEM-512 it shows:
    - **Class C1** support without out-of-band PSK provisioning
      - **<2.3 KiB RAM, <16 KiB Flash** PQC Memory footprint
    - **Faster than signature-based** authentication in some conditions
      - For **B2** PHY rates (>10^5 bit/s) under **S1/S2** or larger MTUs Classes
      - Example results for 20 MHz CPUs under lossless link-to-link conditions
        - For BLE network (S1/B2)→ ~0,34 s
        - For IEEE 802.15.4 (S1/B2) → ~0,45 s
        - For NB-IoT (S4/B2) →~0,58 s

EDHOC RF9528
Method 3

PQ

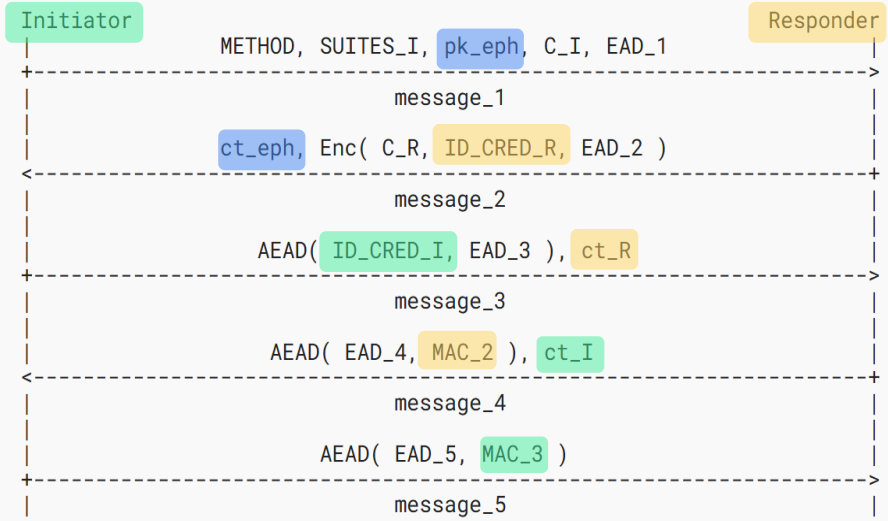
Method Type Value	Initiator Authentication Key	Responder Authentication Key
5 (suggested)	Static KEM Key	Static KEM Key

Signature free

draft-pocero-lake-authkem-edhoc-00

Proposed Mutual KEM-Based Authentication Method for EDHOC

EDHOC Message Flow for Method 5:
Signature-free KEM-based auth for both I and R



- Single-KEM design for both key exchange and mutual authentication

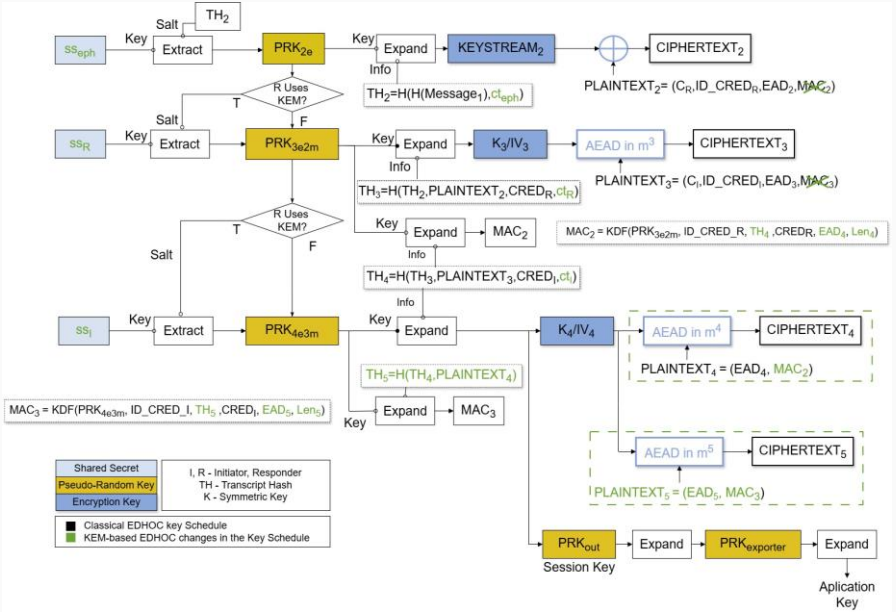
INITIATOR	RESPONDER
Static-KEM pair	Static-KEM pair
⬇	⬇
ID_CRED_I	ID_CRED_R
⬇	⬇
Ct_I	Ct_R
⬇	⬇
MAC_3	MAC_2

Proposed Mutual KEM-Based Authentication Method for EDHOC

- Maintains **EDHOC message formats, key schedules, and security mechanisms,** aiming to preserve equivalent security properties
- **TH chaining** based on accumulated previous TH values and the current plaintext message
- **MACs** are computed over Message data (credentials), and THs → verify handshake integrity and authenticity, while also providing credential binding.
- Following the Noise Framework/EDHOC key schedule, each new shared secret is immediately mixed into the session state
  - message_3 encryption key derived from **ss_R** and **ss_eph**
  - only the Responder owning **sk_R** can decrypt message_3,

→ Aims to provide **Initiator Identity Protection** against **active attacks**

EDHOC Key Schedule for Method 5:
Signature-free KEM-based auth for both I and R



Ongoing Formal Verification of Method 5

- **Completed** formal verification in **Tamarin** for the proposed KEM/KEM-based EDHOC authentication method ***(with Vaishnavi Sundararajan, IIT Delhi)***
  - **Verified**:
    - Secrecy of the established session key *(prk_out)*
    - Injective agreement for the *Initiator*
    - Injective agreement for the *Responder*
  - **Verified** additional properties:
    - Secrecy of intermediate key material → *(prk_2e, prk_3e2m, prk_4e3m)*
    - Perfect Forward Secrecy (PFS) of *prk_out*
    - Weak post-compromise security of *prk_out*
- **Ongoing** verification work in **ProVerify**
  - Equivalence-based proofs for formal verification of **ID_CRED protection**

Looking for adoption from the WG !

Funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.