KEM-based Authentication for EDHOC

draft-pocero-authkem-edhoc-00

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

Affiliations: ISI, R.C. ATHENA

Presenter: Lidia Pocero Fraile

IETF 123, Madrid
July 23rd, 2025

Motivation

- The urgency of the post-quantum transition makes it critical to adapt EDHOC for quantum resistance
- The PQC signature-base EDHOC, using NIST standardized signature schemes, introduces significant overhead
  - Long key sizes and signatures
  - High processing times
  - High memory overhead
- A KEM-based authentication method for EDHOC enables signature-free authentication

Theoretical Foundation - PQNoise

XX:

$-> e$

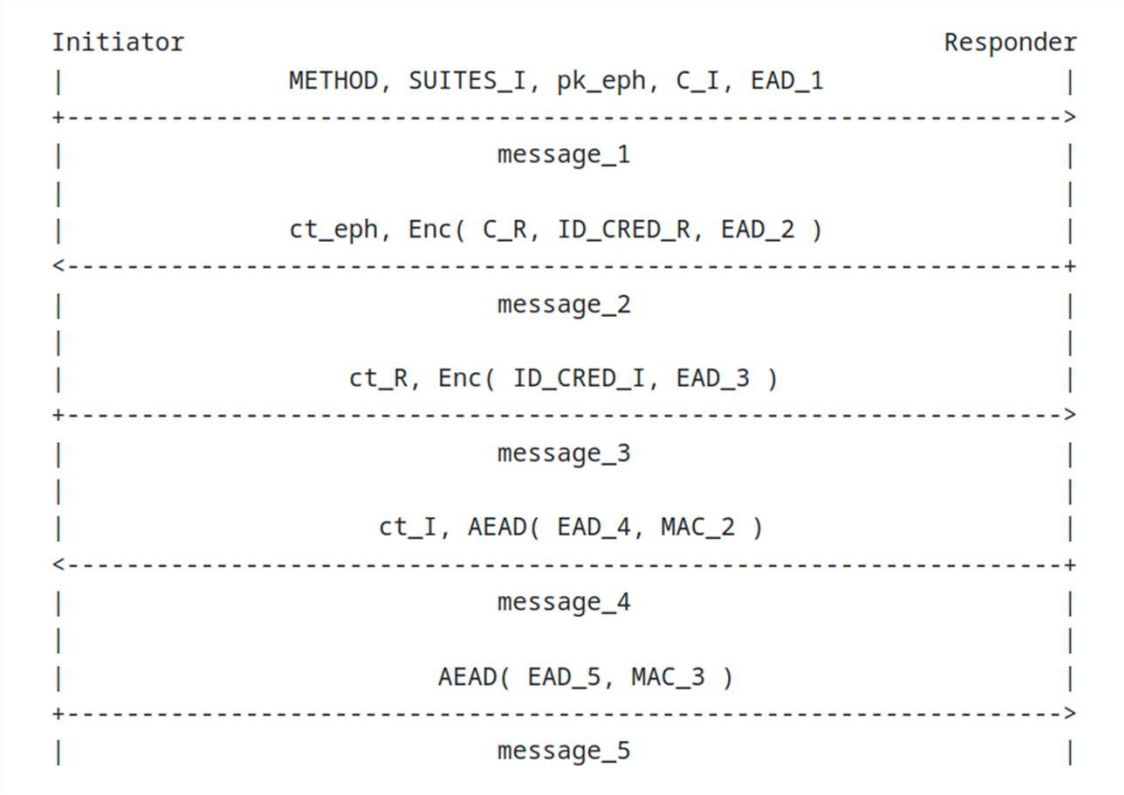
$<- e, ee, s, es$

$-> s, se$

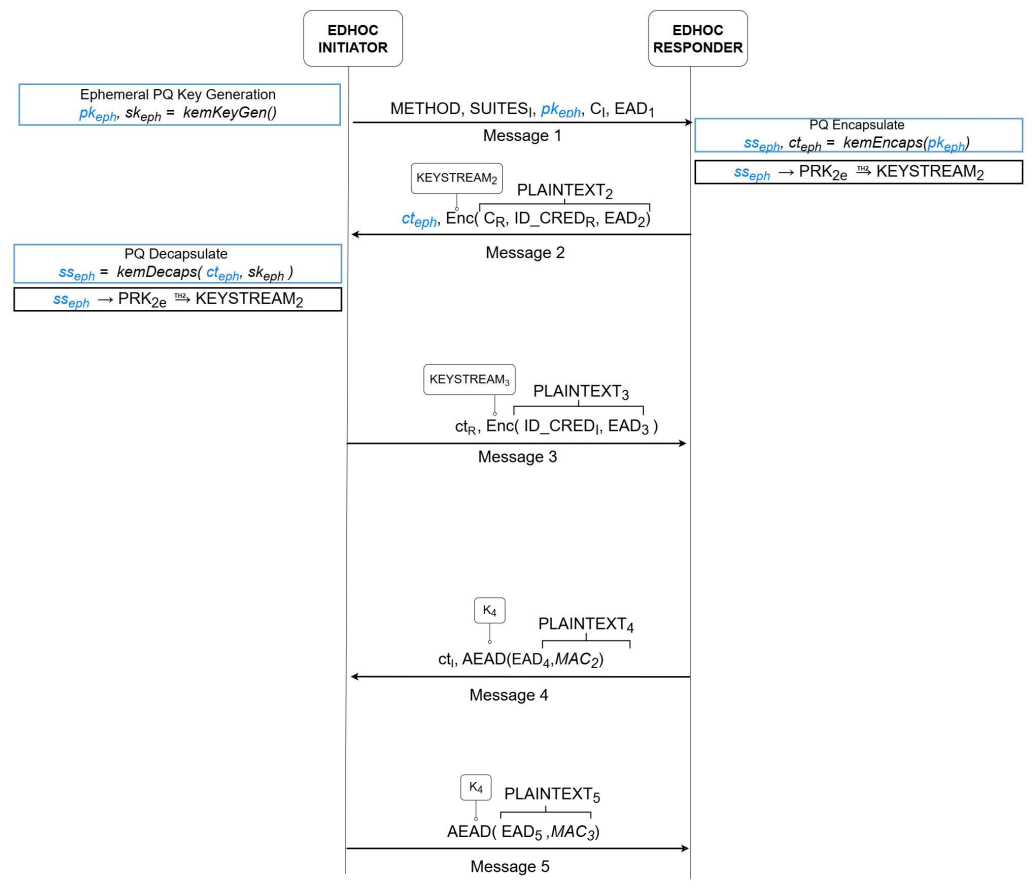

```
pqXX:
-> e
<- ekem, s
-> skem, s
<- skem
```

- Static-DH method of EDHOC: based on Noise XX pattern:
  - Supports mutual authentication without pre-shared knowledge.
  - Static public keys can be transmitted during the handshake
  - Incremental channel security guarantees
- The PQ translations of noise pattern from [PQNoise-CCS2]
  - Add up to one round trip

Overview

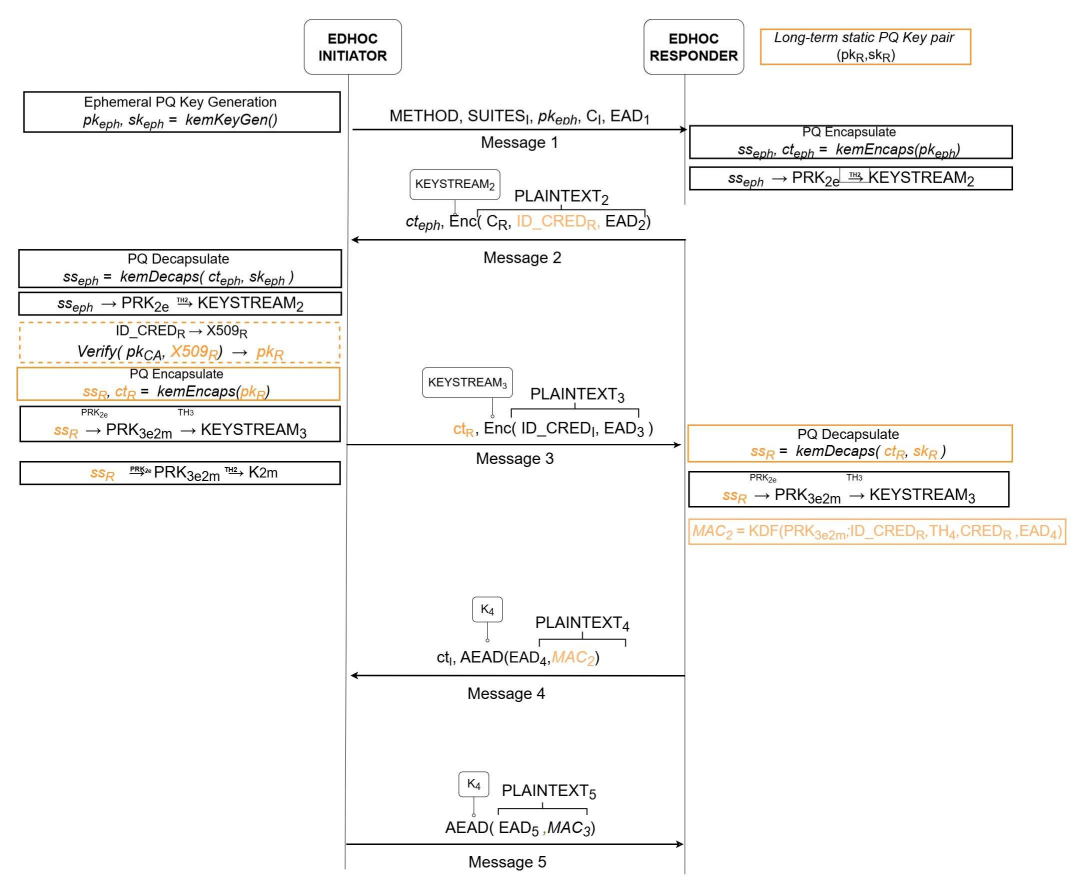

Initiator
Responder
METHOD, SUITES_I, pk_eph, C_I, EAD_1
message_1
ct_eph, Enc(C_R, ID_CRED_R, EAD_2)
message_2
ct_R, Enc(ID_CRED_I, EAD_3)
message_3
ct_I, AEAD(EAD_4, MAC_2)
message_4
AEAD(EAD_5, MAC_3)
message_5

Overview - Ephemeral KEM



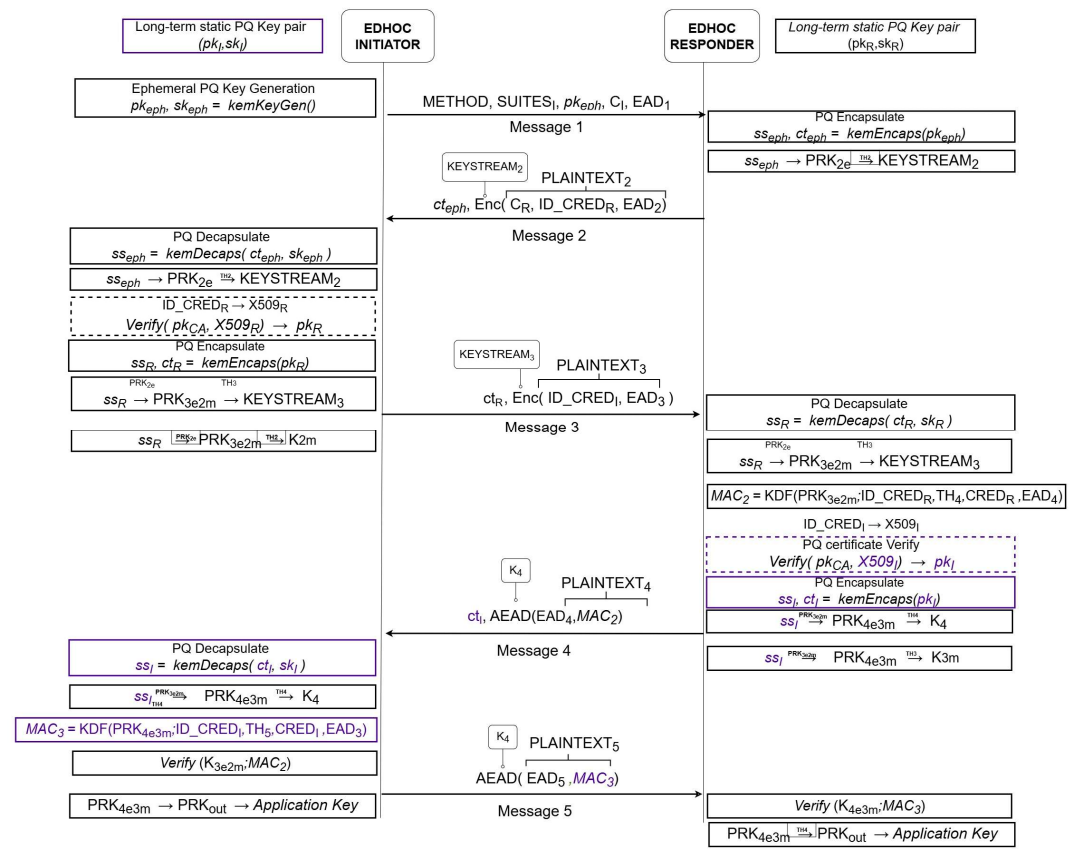
draft-pocero-authkem-edhoc-00

Overview – KEM-based authentication for the Responder



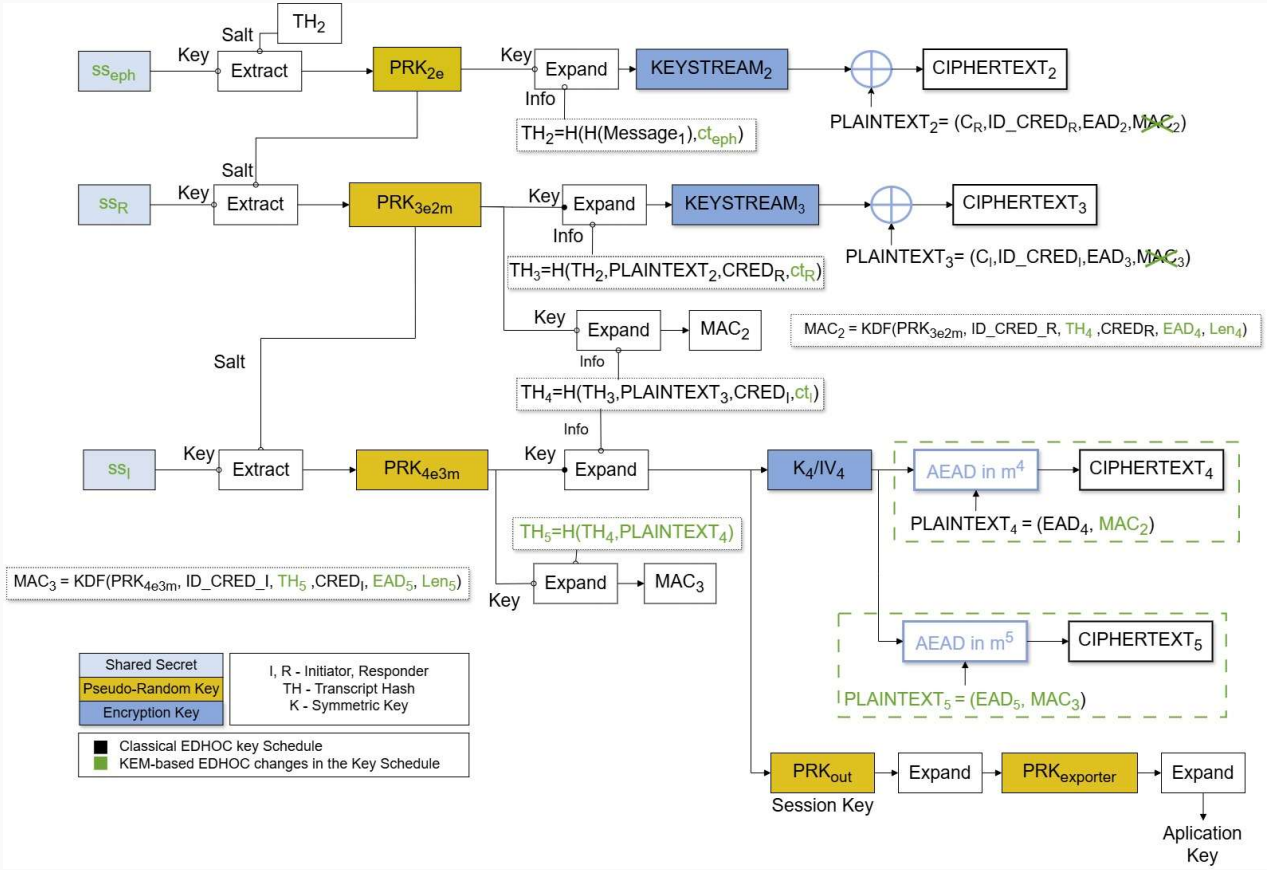
draft-pocero-authkem-edhoc-00

Overview – KEM-based authentication for the Initiator



draft-pocero-authkem-edhoc-00

KEM-based authentication method – Key schedule



draft-pocero-authkem-edhoc-00

Security Considerations

- The additional message_4 and message_5
  - Prove possession of the final session key
  - Ensure mutual authentication by using the final key derived from the three shared secrets
  - Include MAC_2 and MAC_3 to:
    - Provide credential binding: MAC's contexts contain the credentials sent in message_2 and message_3, respectively
    - Ensure all handshake integrity and authenticity: MAC's contexts contain the latest TH4 and TH5

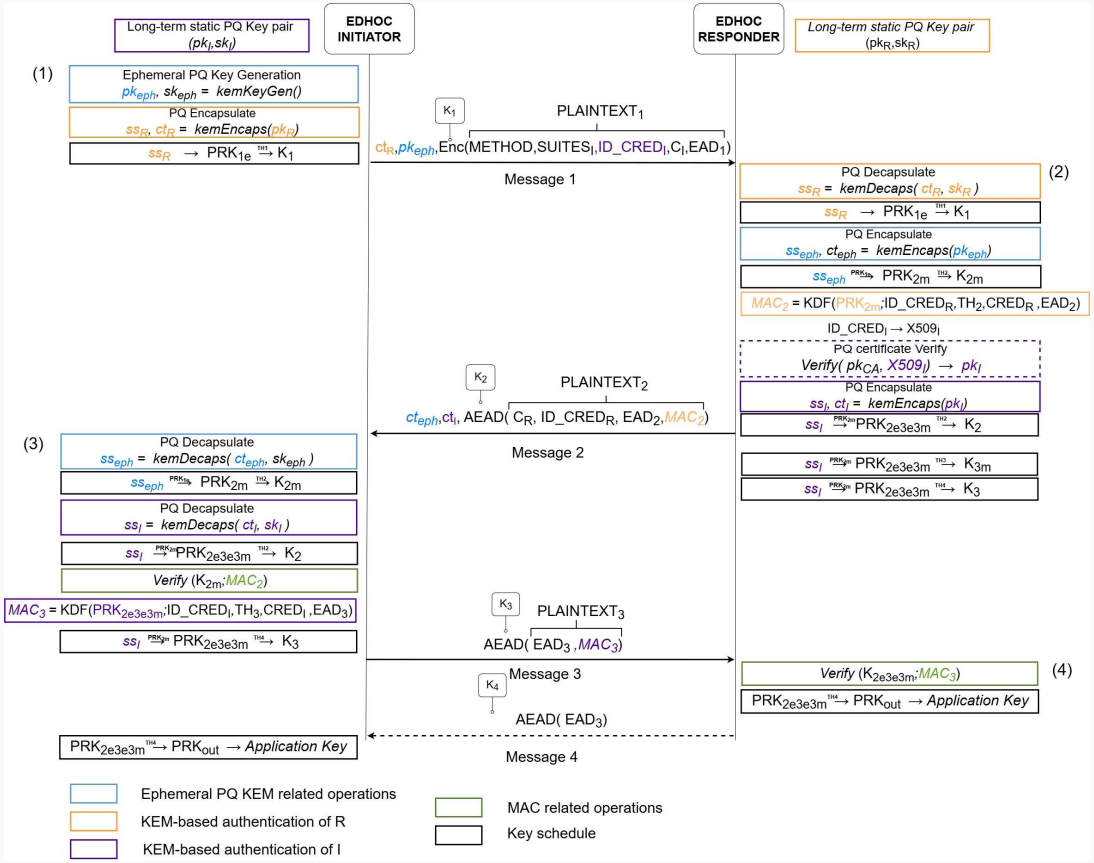
Security Considerations

- Security Achieved Upon Handshake Completion
  - Full forward secrecy
  - Explicit mutual authentication.
  - Integrity and Authenticity of the Handshake
  - Credential binding (A potential misbinding attack will not be detected until the handshake concludes)
- Security Precautions Until Handshake Completion
  - EAD data should be treated as unprotected
  - Keying materials should not be persistently stored

Security Considerations – Details to discuss

- Identity protection
  - Against passive attacks for the Responder
  - Against active attacks for the Initiator:
    - Credentials encrypted with a key combining both Responder's static shared secret and ephemeral shared secret → Only the Responder can decrypt (weaker forward secrecy)
- PRK_out and K_4 are expanded from the same PRK_4e3m and TH4
  - Drawback: Key confirmation implies the authentication of the handshake only until message 3
  - Advantage: MACs and encryption keys are exported from different THs

KEM-based Authentication for EDHOC in: Initiator-Known Responder (IKR) Scenarios



KEM-based Authentication for EDHOC in: Initiator-Known Responder (IKR) Scenarios

- Identity protection
  - Against active attacks for the Initiator: Credentials encrypted with a key that only the Responder can compute → no forward secrecy
  - Against active attacks for the Responder: Credentials encrypted with a key derived from the three shared secrets → perfect forward secrecy
- Pseudorandom Key confirmation via messages 2 and 3
- Reevaluate the need for message 4
  - K_4 and PRK_OUT are derived from (PRK_2e3e2m, TH4)
    - TH4 input contains ID_CRED_R and PLAINTXT_3
    - The confirmation of key possession → proves all handshakes' authenticity

Looking for feedback/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.

IETF®