Updates on KEM-based Authentication for EDHOC (draft-pocero-authkem-edhoc-01)

Authors: L. Pocero Fraile, C. Koulamas, A. P. Fournaris, E. Haleplidis
Affiliations: ISI, R.C. ATHENA
Presenter: Lidia Pocero Fraile

IETF 124, Montreal
November 6th, 2025

IETF

Feedback and Issues from IETF 123

1. IANA-related issues.
2. Identity Hiding Attack for Multiple Public Keys Exploitable via XOR-encryption in Message 3.
3. Confusingly expressed paragraph about repudiation in the Security Considerations section.
4. Need support for PQ combined authentication variants (KEM-based and Signature-based).

Updates and Solutions in the New Draft Version (-01)

- **ISSUE #1**: IANA-related issues
- **SOLUTION #1:** Update the IANA Considerations section in draft-01

Section	Issue (from IANA Review)	Update (in draft -01)
Sec. 5.1 **Sec. 5.2** **Sec. 5.3**	- Duplicate change controller/reference fields - Fixed values - Extra “unassigned” row.	- Moved note above table - Values update to (suggested) - removed extra row

Updates and Solutions in the New Draft Version (-01)

- **ISSUE #2**: Identity Hiding Attack for Multiple Public Keys Exploitable via XOR-encryption in Message 3.
- **SOLUTION #2**: Replaced XOR encryption with AEAD encryption for Message 3 and updated the corresponding text.
  - AEAED used only for Integrity protection of Message 3.
  - The derived key until this point does not yet authenticate the Initiator identity.

Updates and Solutions in the New Draft Version (-01)

- **SOLUTION #2**: Replaced XOR encryption with AEAD encryption for Message 3 and updated the corresponding text.

Section	Update (in draft -01)
Sec 1.2 / Fig.1	Update **message flow diagram**: replaced XOR with AEAD in message_3
Sec 3. / Fig.2	Modified **key derivation scheme**: replaced block XOR → AEAD
Sec 3.1.2 Fig.3	Updated **key derivations**: renamed KEYSTREAM_3 → K_3/IV_3
Sec 4.3.2	Update **the Initiator composition of message 3** to use COSE_Encrypt0 with AEAD and K3/IV3 instead of XOR-based encryption

Updates and Solutions in the New Draft Version (-01)

- **ISSUE #3**: Confusingly expressed paragraph about repudiation in the Security Considerations section
- **SOLUTION #3:** Reworded the paragraph in the Security Considerations section

Section	Update (in draft -01)
Sec. 6	“The KEM-based authentication method does not provide non-repudiation, but only implicit proof of participation, similar to EDHOC with static DH keys”

Updates and Solutions in the New Draft Version (-01)

- **COMMENT #4**: Need support for PQ combined authentication variants (KEM-based and Signature-based).
- **UPDATE #4**: Extend the protocol with two additional authentication methods providing combination variants.

Two possible approaches:

1. **Message-flow-preserving approach:** adopted as the main design.
2. **Early authentication approach:** presented in Appendix A as an alternative for discussion

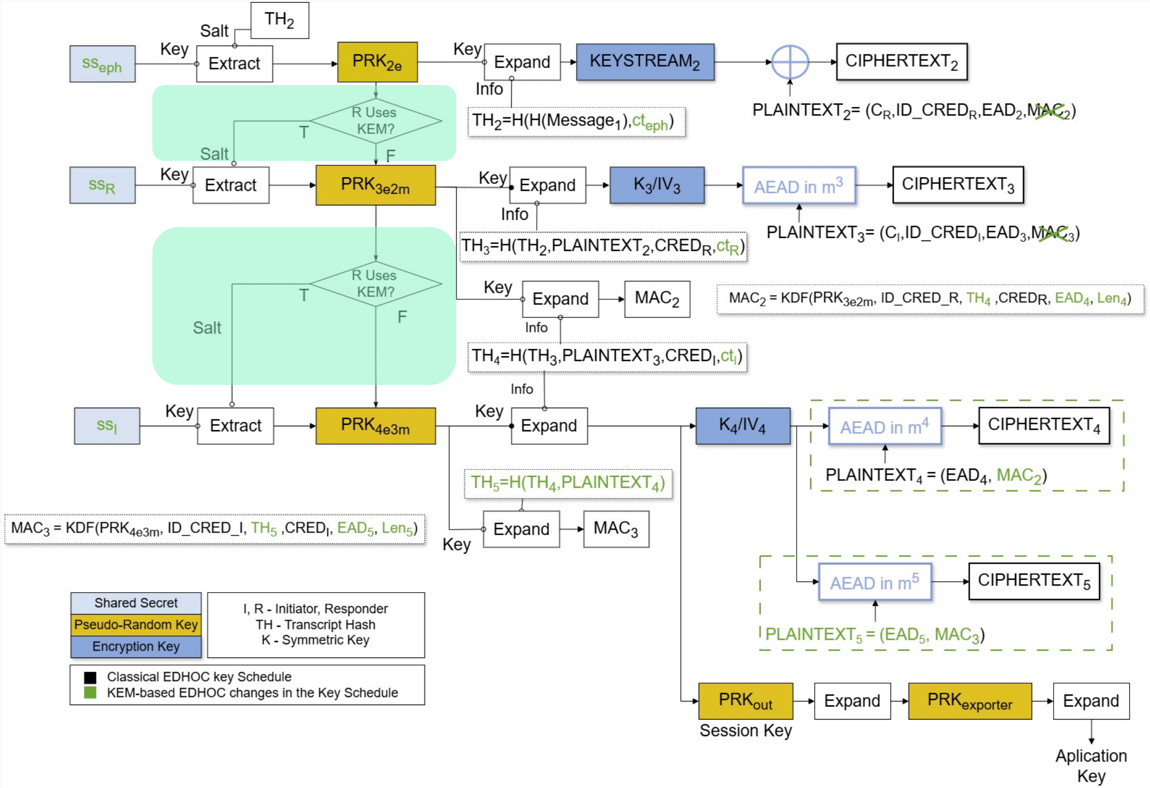
EDHOC KEM/Signature-Based Combined Authentication
Message-flow-preserving approach

- Extension to three authentication methods: KEM-based and combined KEM/signature variants for PQ authentication

Method Type Value	Initiator Authentication Key	Responder Authentication Key
4	Static KEM Key	Static KEM Key
5	Static KEM Key	PQC Signature
6	PQC Signature	Static KEM Key

EDHOC KEM/Signature-Based Combined Authentication
Key Schedule (Common to Both Approaches)

1. **Key derivation adjustments:** The PRK chaining structure is extended to handle both KEM and signature variants, combining multiple KEM shared secrets for KEM-based methods, or simplifying to reuse previous PRKs for signature-based authentication.



EDHOC KEM/Signature-Based Combined Authentication
Message-flow-preserving approach – Message Flow Updates

2. Message Format Updates

- Introduces Sig_R_or_MAC_2 and Sig_I_or_MAC_3 to cover all methods
  - Method 4 → MAC_2, MAC_3
  - Method 5 → Sig_R, MAC_3
  - Method 6 → MAC_2, Sig_I
- KEM ciphertext become optional trailing fields (omitted when unused)
  - Ct_R → methods 4 and 6
  - Ct_I → methods 4 and 5

```
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                                |
|                                                                    |
|                 AEAD( ID_CRED_I, EAD_3 ), ct_R?                    |
+------------------------------------------------------------------->
|                           message_3                                |
|                                                                    |
|               AEAD( EAD_4, Sig_R_or_MAC_2 ), ct_I?                 |
<-------------------------------------------------------------------+
|                           message_4                                |
|                                                                    |
|                  AEAD( EAD_5, Sig_I_or_MAC_3 )                     |
+------------------------------------------------------------------->
|                           message_5                                |
```

EDHOC KEM/Signature-Based Combined Authentication
Message-flow-preserving approach – Main document updates

- **Key derivation adjustments and message formats refined:** Update the document to reflect the previously described technical changes
- **Method-aware message formatting and processing:** Message formatting and processing rules in **Section 4** are extended to explicitly depend on the selected authentication method, by adding conditional steps for KEM- or signature-based variants in:
  - Message composition and processing flows.
  - Key derivation
  - Inclusion or omission of KEM ciphertexts (ct_R, ct_I)
  - Signature or Signature over MAC
  - Transcript adjustments: Transcript hashes (TH_i) to reflect optional KEM inputs and the chosen auth method.
- **Consistency & cleanup:** Aligns terminology and processing with RFC 9528 where applicable; fixes typos, normalizes lengths/rules, and clarifies processing steps.

EDHOC KEM/Signature-Based Combined Authentication
Early authentication approach – Message Flow Updates

Method 4: KEM-based/KEM-based

```
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, AEAD( ID_CRED_I, EAD_3 )                         |
+-------------------------------------------------------------------------->
|                              message_3                                    |
|                                                                           |
|                      ct_I, AEAD( EAD_4, MAC_2 )                           |
<--------------------------------------------------------------------------+
|                              message_4                                    |
|                                                                           |
|                         AEAD( EAD_5, MAC_3 )                              |
+-------------------------------------------------------------------------->
|                              message_5                                    |
```

EDHOC KEM/Signature-Based Combined Authentication
Early authentication approach – Message Flow Updates

Method 5: KEM-based/PQC sig-based

```
Initiator                                                    Responder
|              METHOD, SUITES_I, pk_eph, C_I, EAD_1                 |
+------------------------------------------------------------------>
|                          message_1                                |
|                                                                   |
|              ct_eph, Enc( C_R, ID_CRED_R, sig, EAD_2 )            |
<------------------------------------------------------------------+
|                          message_2                                |
|                                                                   |
|                    AEAD( ID_CRED_I, EAD_3 )                       |
+------------------------------------------------------------------>
|                          message_3                                |
|                                                                   |
|                       ct_I, AEAD( EAD_4)                          |
<------------------------------------------------------------------+
|                          message_4                                |
|                                                                   |
|                      AEAD( EAD_5, MAC_3 )                         |
+------------------------------------------------------------------>
|                          message_5                                |
```

Method 6: PQC sig-based/KEM-based

```
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, AEAD( ID_CRED_I, sig, EAD_3 )                 |
+------------------------------------------------------------------>
|                          message_3                                |
|                                                                   |
|                      AEAD( EAD_4, MAC_2 )                         |
<------------------------------------------------------------------+
|                          message_4                                |
```

EDHOC KEM/Signature-Based Combined Authentication

Comparison of Message-Flow-Preserving and Early Authentication Approaches

Aspect	Message-Flow-Preserving Approach	Early Authentication Approach
Objective	Maintain consistent message structure and number across all authentication methods.	Prioritize early authentication as soon as each party can authenticate.
Authentication Timing	Parties authenticate later (Responder in message_4, Initiator in message_5).	Each party authenticates in the first message where possible.
Message Count	Fixed five-message flow for all methods.	Reduce to four messages for method 6
Complexity	Lower: same format and flow across all methods.	Higher: requires different message formats and flows depending on method.
Resilience to Attacks	Authentication assurance achieved later and misbinding detected only after full exchange.	Enables earlier detection of misbinding and failed authentication.
Interoperability & Implementation	Easier to specify and implement due to unified message structure.	Harder to specify and implement due to variant message flows.

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.