EDHOC PSK-based authentication method
draft-lopez-lake-edhoc-psk-01

Elsa Lopez-Perez, Inria
Göran Selander, Ericsson
John Preuβ Mattsson, Ericsson
Rafael Marin-Lopez, University of Murcia
Status

• Published -01 on 4 July 2024

• Goal of the presentation
  • Present the current status and the two proposed variants for PSK-based authentication in EDHOC
Motivation

• Working Group Charter alignment:
  • PSK authentication is a key objective in the IETF LAKE WG Charter

• Leveraging existing infrastructure:
  • Billions of SIM cards deployed worldwide.
  • Cost-effective: update software rather than replace hardware.
  • Preserves the investments in current technology.

• Gradual transition:
  • EDHOC + PSK supports adoption by older devices.
  • Bridges the gap between current and future security protocols.
  • Ensures backward compatibility while moving forward.

EDHOC with PSK offers a practical, cost-effective path to enhance IoT security while utilizing existing infrastructure
Proposed solutions

VARIANT 1

METHOD, SUITES_I, G_X, C_I, ID_CRED_PSK, EAD_1
message_1

G_Y, Enc(KEystream_2; C_R, MAC_2, EAD_2 )
message_2

AEAD(K_3; EAD_3 )
message_3

AEAD(K_4; EAD_4 )
message_4

VARIANT 2

METHOD, SUITES_I, G_X, C_I, EAD_1
message_1

G_Y, Enc(KEystream_2; C_R, EAD_2 )
message_2

Enc(KEystream_3; ID_CRED_PSK) AEAD(K_3; EAD_3)
message_3

AEAD(K_4; EAD_4 )
message_4
Variant 1: message flow

- Include ID_CRED_PSK in message_1 in cleartext.
- message_2 remains the same.
- Remove MAC_3 in message_3
- message_4 remains the same

EDHOC message flow, as in RFC 9528

EDHOC PSK-authentication Variant 1 message flow
Variant 1: key schedule

- \( \text{PRK}_3e2m = \text{EDHOC\_Extract} (\text{salt}3e_2m, \text{CRED\_PSK}) \)
- \( \text{PRK}_4e3m = \text{PRK}_3e2m \)
- \( \text{MAC}_2 = \text{EDHOC\_KDF} (\text{PRK}_3e2m, 2, \text{context}_2, \text{mac\_length}_2) \)
- \( \text{K}_3 = \text{EDHOC\_KDF} (\text{PRK}_4e3m, \text{TBD}, \text{TH}_3, \text{key\_length}) \)
- \( \text{IV}_3 = \text{EDHOC\_KDF} (\text{PRK}_4e3m, \text{TBD}, \text{TH}_3, \text{iv\_length}) \)
- \( \text{context}_2 = \ll \text{C\_R}, \text{ID\_CRED\_PSK}, \text{TH}_2, \text{CRED\_PSK}, ? \text{EAD}_2 \gg \)
- \( \text{TH}_3 = H(\text{TH}_2, \text{PLAINTEXT}_2, \text{CRED\_PSK}) \)
- \( \text{TH}_4 = H(\text{TH}_3, \text{PLAINTEXT}_3, \text{CRED\_PSK}) \)
Variant 2: message flow

- Include ID_CRED_PSK in message_3 encrypted.
- Remove MAC_2.
- Message 3 consists of two ciphertexts concatenated:
  - Ciphertext_3a containing ID_CRED_PSK encrypted with keystream_3.
  - Ciphertext_3b containing AEAD with EAD_3.
- Remove MAC_3 in message_3
- External_aad in AEAD in message_3 includes the ID_CRED_PSK
- message_4 remains the same. It is needed for Responder’s authentication (it can be replaced by an OSCORE message)

EDHOC message flow, as in RFC 9528

EDHOC PSK-authentication Variant 2 message flow
Variant 2: key schedule

- \( \text{PRK}_3e2m \) = \( \text{PRK}_2e \)
- \( \text{PRK}_4e3m \) = EDHOC_Extract( SALT_4e3m, CRED_PSK )
- \( \text{KEYSTREAM}_3 \) = EDHOC_KDF( \( \text{PRK}_3e2m \), TBD, TH_3, key_length )
- \( \text{K}_3 \) = EDHOC_KDF( \( \text{PRK}_4e3m \), TBD, TH_3, key_length )
- \( \text{IV}_3 \) = EDHOC_KDF( \( \text{PRK}_4e3m \), TBD, TH_3, iv_length )
- \( \text{TH}_3 \) = H(TH_2, PLAINTEXT_2, CRED_PSK)
- \( \text{TH}_4 \) = H(TH_3, ID_CRED_PSK, ? EAD_3, CRED_PSK )

\[ \begin{align*}
\text{TH}_2 &= \text{H}(\text{TH}_1, \text{SESSION}) \\
\text{TH}_3 &= \text{H}(\text{TH}_2, \text{PLAINTEXT}_2, \text{CRED}_\text{PSK}) \\
\text{TH}_4 &= \text{H}(\text{TH}_3, \text{ID}_\text{CRED}_\text{PSK}, \text{EAD}_3, \text{CRED}_\text{PSK})
\end{align*} \]
## Comparison of Variant 1 and Variant 2

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Variant 1</th>
<th>Variant 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Lower: ID_CRED_PSK sent in the clear</td>
<td>Higher: ID_CRED_PSK encrypted in message_3</td>
</tr>
<tr>
<td>Identity Protection</td>
<td>Initiator exposed from message_1. Both I and R are vulnerable against passive and active attackers</td>
<td>Initiator protected until message_3. I and R’s identities are protected against passive attackers.</td>
</tr>
<tr>
<td>Authentication Timing</td>
<td>Message_1</td>
<td>Message_3</td>
</tr>
<tr>
<td>Computational Efficiency</td>
<td>Slightly higher (no encryption of ID_CRED_PSK)</td>
<td>Slightly lower (Encryption of ID_CRED_PSK)</td>
</tr>
<tr>
<td>Early access control</td>
<td>Possible from message_1</td>
<td>Possible from message_3</td>
</tr>
<tr>
<td>DoS Attack Vulnerability</td>
<td>Lower due to earlier authentication</td>
<td>Potentially higher</td>
</tr>
<tr>
<td>Resource allocation</td>
<td>Fewer resources allocated before authentication</td>
<td>More resources allocated before authentication</td>
</tr>
<tr>
<td>Key derivation timing</td>
<td>Earlier</td>
<td>Later</td>
</tr>
<tr>
<td>Completeness</td>
<td>Complete: achieves mutual authentication + implicit key authentication without message_4</td>
<td>A fourth message is needed for mutual authentication and key confirmation</td>
</tr>
<tr>
<td>Number of messages</td>
<td>Message_4 is only used for key confirmation (explicit key authentication) 3 + optional</td>
<td>A fourth message is needed for R’s authentication and key confirmation 4</td>
</tr>
<tr>
<td>Num. of operations</td>
<td>2 Asym. 4 Sym.</td>
<td>2 Asym. 4Sym.</td>
</tr>
</tbody>
</table>
Next Steps

• Implementation of EDHOC_PSK in lakers
  • [https://github.com/openwsn-berkeley/lakers](https://github.com/openwsn-berkeley/lakers)
  • Merge PSK with the already supported StatStat method

• Evaluation and comparison of Variant 1 and Variant 2
  • Security
  • Privacy
  • Number of operations
  • Energy consumption
  • Latency
  • Memory consumption
Thank you!