Using the Extensible Authentication Protocol with Ephemeral Diffie-Hellman over COSE (EDHOC)

Advances and Changes for draft-ietf-emu-eap-edhoc-01

Dan García-Carrillo, University of Oviedo
Rafael Marín-López, University of Murcia
Göran Selander, Ericsson
John Preuß Mattsson, Ericsson

IETF 120
Summary of main items

• Quick recap

• Changes in the Flag Field
  • Variable length EDHOC Message Length

• Advances in implementation
  • Paris Hackathon participation

• Next steps
Quick recap

Context
EDHOC [RFC 9528] provides a compact and lightweight authenticated Diffie-Hellman key exchange

Use of CBOR and COSE

Credentials
Certificates and RPK
Changes in Flag Field

**Context**

- With the goal of saving bytes we implement the following changes in the flag field

**Approach**

<table>
<thead>
<tr>
<th>Request</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8</td>
<td>0 1 2 3 4 5 6 7 8</td>
</tr>
<tr>
<td>+----------------</td>
<td>+----------------</td>
</tr>
<tr>
<td></td>
<td>R R R S M L L L</td>
</tr>
<tr>
<td>+----------------</td>
<td>+----------------</td>
</tr>
</tbody>
</table>

R = Reserved
S = EAP-EDHOC start
M = More fragments
L = Nº of bytes of EDHOC Message Length

R = Reserved
M = More fragments
L = Nº of bytes of EDHOC Message Length
Changes in Flag Field

Variable length EDHOC Message Length
Advances in implementation
Paris Hackathon (INRIA)

Context
• Currently, we have two implementations: University of Murcia’s (UMU) and University of Uniovi’s (UNIVOVI) of EAP-EDHOC peer and EAP-EDHOC server.

EAP peer
• OpenPANA 0.2.4 (UNIOVI) and hostapd - WPA-Supplicant v2.11-dev (UMU)

EAP server
• freeRADIUS 3.2.3 with uOSCORE-uEDHOC v3.0.4 (UMU)
• freeRADIUS 3.2.1 with uOSCORE-uEDHOC v1.0.5 (Uniovi)

Advances
• UMU has tested the method using a real access point.
• We have just finished fragmentation support (UMU)

Acknowledgments
• We appreciate Francisco López Gómez effort on developing EAP-EDHOC for hostapd - WPA-Supplicant v2.11-dev and freeRADIUS 3.2.3
Next steps

• We would appreciate reviewers for the document
• Adapt implementation to I-D v01
THANK YOU