Ephemeral Diffie-Hellman Over COSE (EDHOC)

draft-selander-ace-cose-ecdhe-05
SELANDER, MATTSSON, PALOMBINI
IETF98 ACE, MAR 27 2017
DESIGN GOALS

- Use strong existing design – SIGMA-I
- Small code and message size
- Reuse existing primitives
  - CBOR
  - COSE
- Minimize choices
- Stay in one UDP packet
- End-to-End not Hop-by-Hop Security
- Counter proposal – carry DTLS inside of CoAP
EDHOC with Asymmetric Keys

- The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.

```
Party U
| S_U, N_U, E_U, ALG_1, EXT_1 |
+-------------------------------+
| message #1                    |
| S_U, S_V, N_V, E_V, ALG_2, Enc(K_2; EXT_2, ID_V, Sig(V, aad_2); aad_2) |
+-------------------------------+
| message #2                    |
| S_V, Enc(K_3; EXT_3, ID_U, Sig(U; aad_3); aad_3) |
+-------------------------------+
| message #3                    |

Party V

```
EDHOC with Symmetric Keys

- Similar to the asymmetric case but without COSE_Sign0 with an COSE_Encrypt0 in message_1 to encrypt EXT_1 and get PSK proof-of-possession already in message_1 (may be used for DoS protection).

```
<table>
<thead>
<tr>
<th>Party U</th>
<th>Party V</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S_U, N_U, E_U, ALG_1, EXT_1</td>
</tr>
</tbody>
</table>
| +-------------------------------+-------------------------------+
| message #1                      |
| | S_U, S_V, N_V, E_V, ALG_2, Enc(K_2; EXT_2, ID_V, Sig(V, aad_2); aad_2) |
| +-------------------------------+-------------------------------+
| message #2                      |
| | S_V, Enc(K_3; EXT_3, ID_U, Sig(U; aad_3); aad_3) |
| +-------------------------------+-------------------------------+
| message #3                      |
```
EDHOC Key Schedule

• Use HKDF for as the primitive
• \( K_i = HKDF( PSK, \text{Ephemeral Secret}, \text{info structure}) \)
• Info structure = [
  * Algorithm Identifier or IV identifier
  * aad information
    * aad information = [
      * Message i data
      * Hash of all previous messages
      * certificate if one is used.\]
EXAMPLE

- Sending EDHOC embedded in OSCOAP has been removed. EDHOC is now sent as payload.

- OSCOAP Master Secret, Master Salt, and identities can be obtained from EDHOC.

Figure 5: Transferring EDHOC in CoAP
NEXT STEPS

• One existing implementation of -05 by Jim Schaad. One more implementation ongoing by SICS

• Look for better review of cryptographic properties

• Test vectors, error messages.