OSCOAP Profile for ACE

draft-seitz-ace-oscoap-profile-01

Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 97, CORE WG, Seoul, Nov 17, 2016
OSCOAP

› OSCOAP defines a method for in-layer security of CoAP message exchanges using the COSE format.

› OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations

› Independent of how CoAP is transported (UDP, TCP, Bluetooth, 802.15.4, foo...)

› Requirements: draft-hartke-core-e2e-security-reqs
Related Work

- **DTLS Profile**
- **OSCOAP Profile**
- **6tisch Minimal Security**
- **Multicast OSCOAP**

- **ACE Framework**
- **EDHOC**
- **OSCOAP**

- **DTLS**
- **OAuth 2.0**
- **COSE**
- **CoAP**

- **Group Communication CoAP**

- **JOSE**
- **CBOR**

Colors:
- Red = ACE WG
- Blue = CoRE WG
- Green = 6tisch WG
- Gray = Individual submission
- Orange = Adopted by WG
- Light Blue = IESG review
- Green = RFC
Related Work

- **ACE Framework**
- **EDHOC**
- **OSCOAP**

Diagram:
- DTLS Profile
- OSCOAP Profile

Legend:
- = ACE WG
- = CoRE WG
- = 6tisch WG
- = Individual submission
- = Adopted by WG
- = IESG review
- = RFC
Ace Framework
(draft-ietf-ace-oauth-authz-04)

Figure 1: Basic Protocol Flow.

Draft Status

- [https://github.com/LudwigSeitz/OSCOAP-ace-profile](https://github.com/LudwigSeitz/OSCOAP-ace-profile)

- Updated according to OSCOAP and EDHOC updates

- EDHOC is a 3-pass protocol, but EDHOC + OSCOAP is still 2 round trips

```
+------------------------+------------------------|
<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDHOC message_1</td>
<td>-----------------------</td>
</tr>
<tr>
<td>EDHOC message_2</td>
<td>-----------------------</td>
</tr>
<tr>
<td>OSCOAP Request + EDHOC message_3</td>
<td>----&gt;</td>
</tr>
<tr>
<td>OSCOAP Response</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
```

Figure 12 from EDHOC draft
Profile Description

Access Token contains:

› OSCOAP only:
  - Symmetric key (Base Key)
  - Context identifier (Cid)
  - AEAD algorithm (Algorithm)
  - Client identifier (Sender ID)
  - Server identifier (Recipient ID)

› OSCOAP + EDHOC (sym):
  - Symmetric key
  - Key identifier

› OSCOAP + EDHOC (asym):
  - Asymmetric key

Client

AS

Access Token request

Access Token + RS Information "profile":"coap_oscoap"

(EDHOC +) OSCOAP

POST auth-info Access Token (+ EDHOC message1)

2.04 (+ EDHOC message2)

OSCOAP request (+ EDHOC message 3)

OSCOAP response

RS
EDHOC + OSCOAP

Figure 6: Key establishment with EDHOC via the authz-info endpoint
## OSCOAP

<table>
<thead>
<tr>
<th>Resource</th>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+--------</td>
<td>Header: POST (Code=0.02)</td>
<td></td>
</tr>
<tr>
<td>POST</td>
<td>Uri-Path:&quot;authz-info&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/cbor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Payload: EDHOC message_1 + access token</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-------+ Header: 2.04 Changed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/cose+cbor</td>
<td></td>
</tr>
<tr>
<td>2.04</td>
<td>Payload: EDHOC message_2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+--------</td>
<td>CoAP request +</td>
<td></td>
</tr>
<tr>
<td>OSCOAP</td>
<td>Object-Security option</td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>COSE_Encrypt0:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unprotected Header: EDHOC message_3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-------+ CoAP response +</td>
<td></td>
</tr>
<tr>
<td>OSCOAP</td>
<td>Object-Security option</td>
<td></td>
</tr>
<tr>
<td>response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key establishment without EDHOC via the authz-info endpoint
OSCOAP or EDHOC + OSCOAP

EDHOC + OSCOAP
› Smaller Access Token + RS Info
› Perfect Forward Secrecy

OSCOAP
› Smaller messages
› Can fit into 1 round trip (for further study)

<table>
<thead>
<tr>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
</tr>
<tr>
<td>+--------------+--------------</td>
</tr>
<tr>
<td>CoAP request +</td>
</tr>
<tr>
<td>OSCOAP</td>
</tr>
<tr>
<td>request</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>&lt;--------------</td>
</tr>
<tr>
<td>OSCOAP</td>
</tr>
<tr>
<td>response</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Planned Next Steps

› Get feedback

› SICS Implementation
Thank you! Comments/questions?