OSCOAP Profile of ACE

draft-seitz-ace-oscoap-profile

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG meeting, IETF 96
Overview

• ACE Profiles in general:
  – Communication protocol
  – Communication security
  – Mutual authentication
  – Proof-of-Possession method for access tokens (could coincide with client authentication)

• This profile:
  – Use of OSCOAP and EDHOC for C – RS
    • Optionally also for C – AS and RS – AS
OSCOAP and EDHOC

• OSCOAP
  – Defines how to use COSE to provide object security for CoAP messages
  – Defines a challenge-response protocol to link requests to responses

• EDHOC
  – Diffie-Hellman over COSE
  – Establishes a shared secret key with PFS
Basic protocol

1. Step: Combined authentication, key establishment & access token transfer

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>C: +--------&gt;</td>
<td>Header: POST (Code=0.02)</td>
</tr>
<tr>
<td>POST</td>
<td>Uri-Path:&quot;authz-info&quot;</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/cose+cbor</td>
</tr>
<tr>
<td></td>
<td>Payload: EDHOC message_1 + access token</td>
</tr>
<tr>
<td>&lt;--------+</td>
<td>Header: 2.04 Changed</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/cose+cbor</td>
</tr>
<tr>
<td>2.05</td>
<td>Payload: EDHOC message_2</td>
</tr>
</tbody>
</table>
Basic protocol ctd.

2. Step: Use OSCOAP

Client

| request: |
| GET example.com |
| [Header, Token, Options:{..., Object-Security:COSE object}] |

Response: 2.05 (Content)

[Header, Token, Options:{..., Object-Security:-}, Payload:COSE object]
Communication Security with AS

• Can use any communication security protocol between C – AS and RS – AS
• In particular EDHOC + OSCOAP can be used here as well
Thank you!

Questions/comments?