OSCOAP Profile of ACE

draft-seitz-ace-oscoap-profile

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG meeting, IETF 96
20. July, 2016

Overview

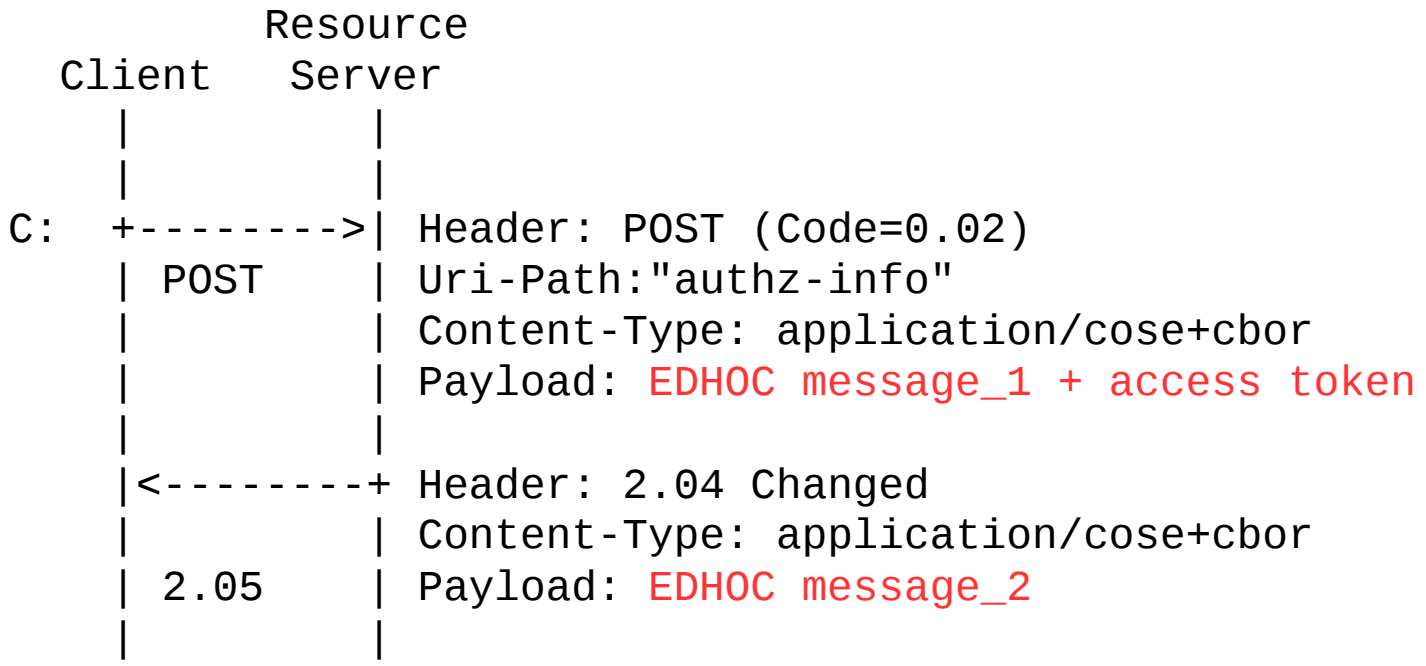
- ACE Profiles in general:
  - Communication protocol
  - Communication security
  - Mutual authentication
  - Proof-of-Possession method for access tokens (could coincide with client authentication)
- This profile:
  - Use of OSCOAP and EDHOC for C – RS
    - Optionally also for C – AS and RS – AS

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



Basic protocol ctd.

2. Step: Use OSCOAP

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?