OSCOAP Profile for ACE

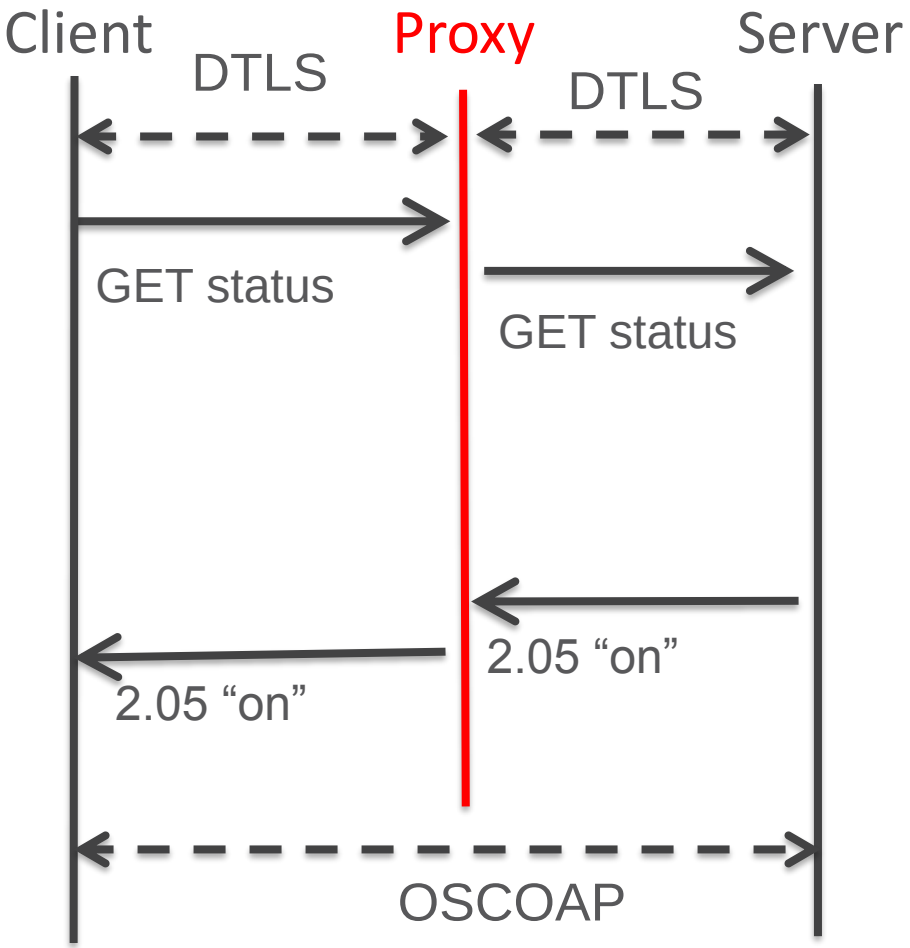
draft-seitz-ace-oscoap-profile-01

Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

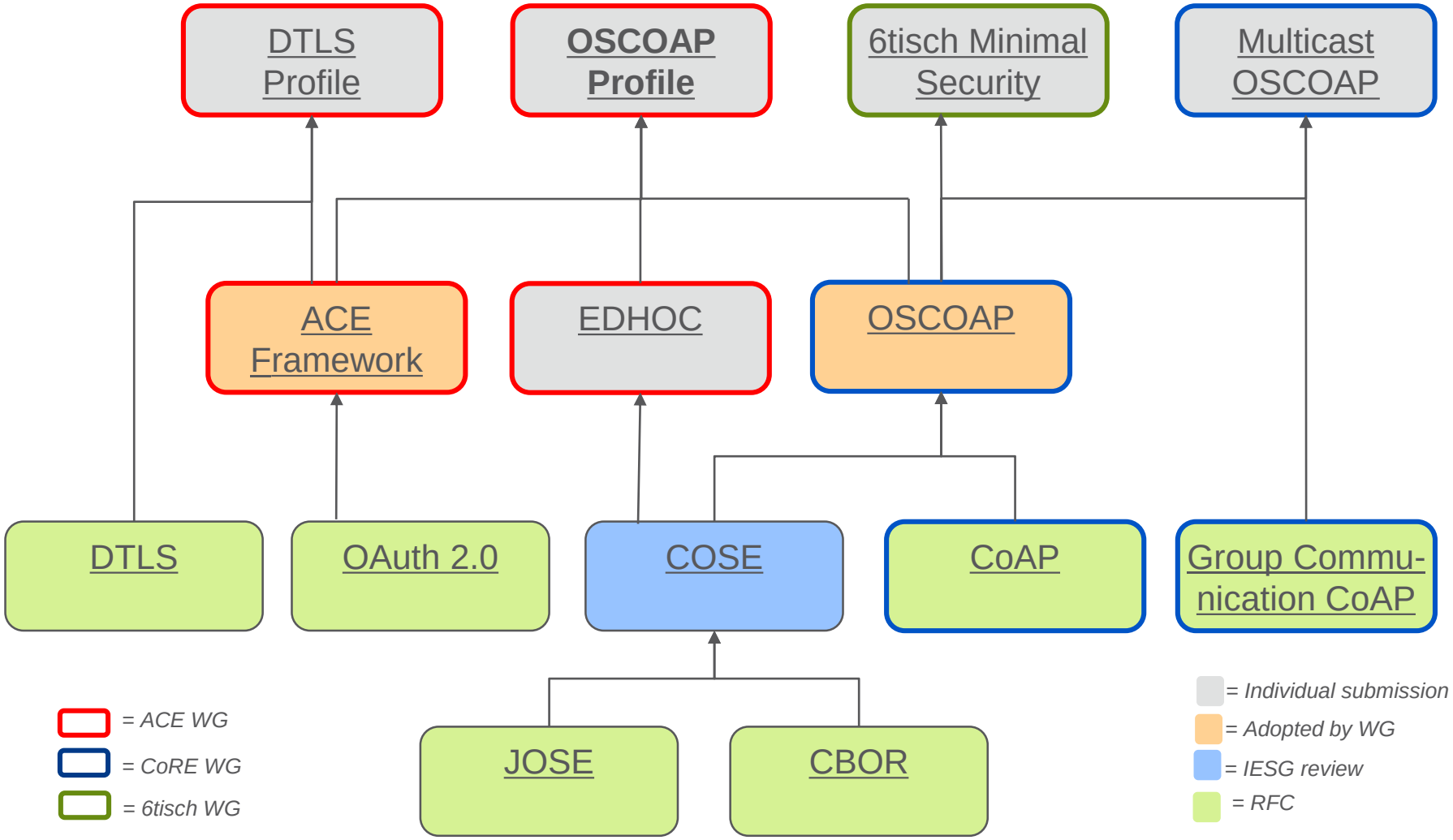
IETF 97, CORE WG, Seoul, Nov 17, 2016

OSCOAP

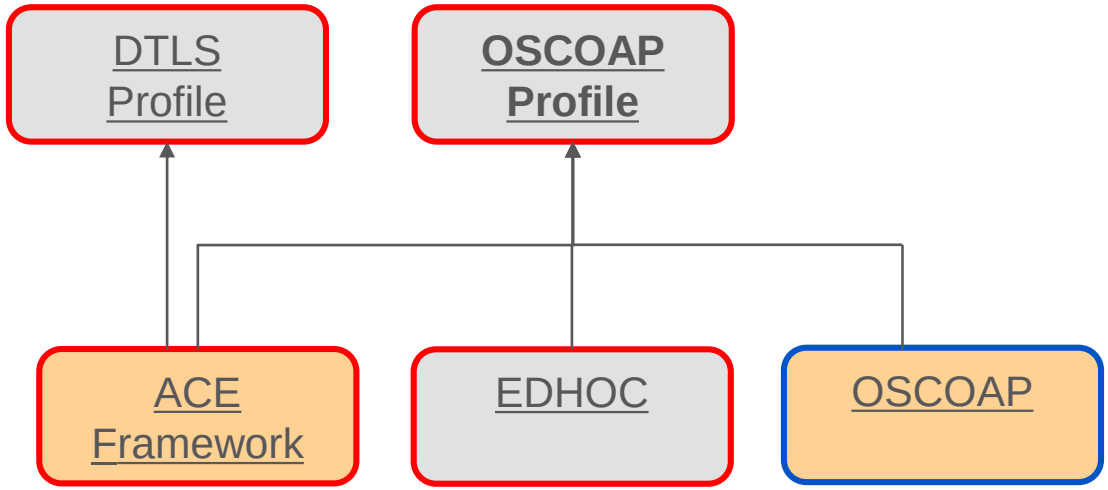
- OSCOAP defines a method for in-layer security of CoAP message exchanges using the COSE format.
- OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations
- Independent of how CoAP is transported (UDP, TCP, Bluetooth, 802.15.4, foo…)
- Requirements: draft-hartke-core-e2e-security-reqs



Related Work



Related Work



= *ACE WG*

= *CoRE WG*

= *6tisch WG*

= *Individual submission*

= *Adopted by WG*

= *IESG review*

= *RFC*

Ace Framework
(draft-ietf-ace-oauth-authz-04)

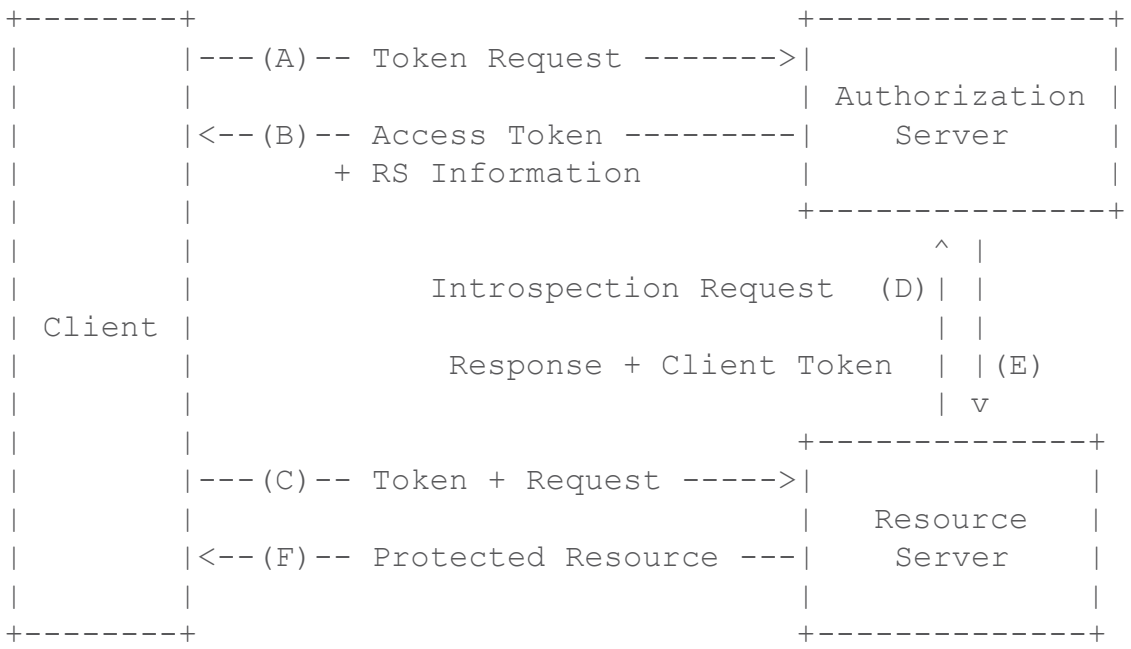


Figure 1: Basic Protocol Flow.

› https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-04

Draft Status

- 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

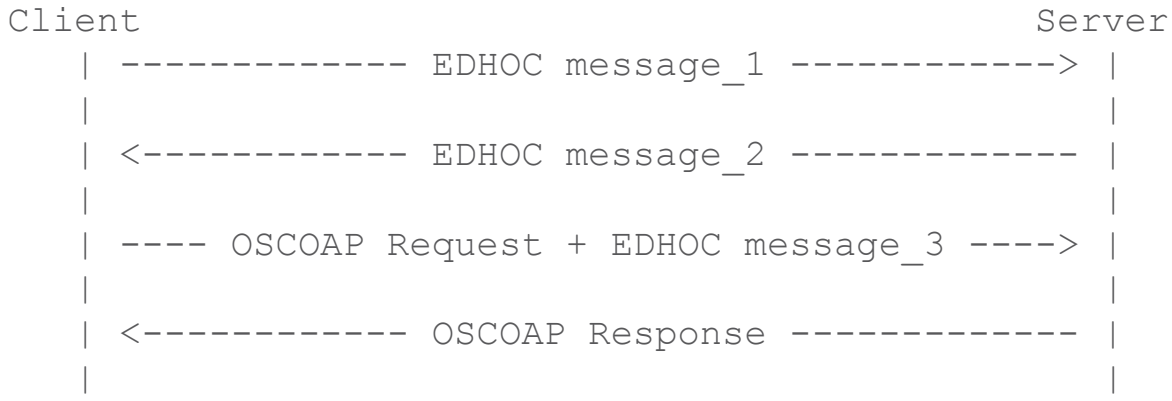
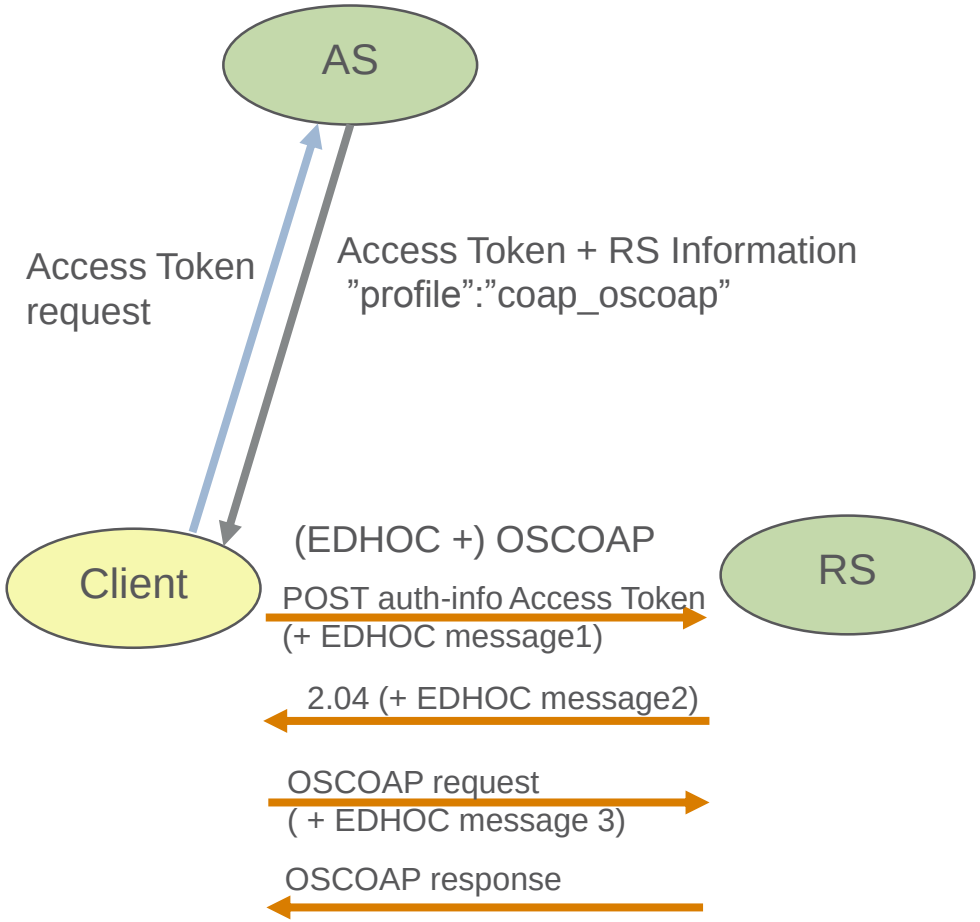


Figure 12 from EDHOC draft

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

EDHOC + OSCOAP

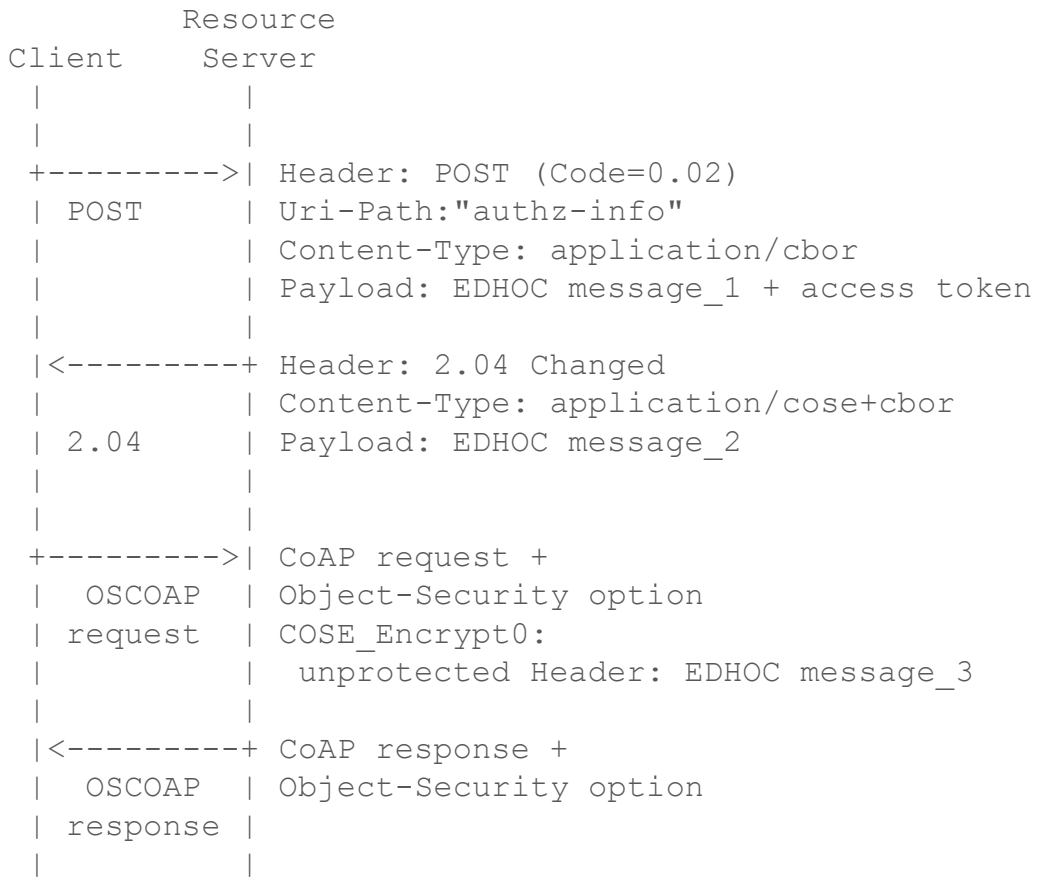
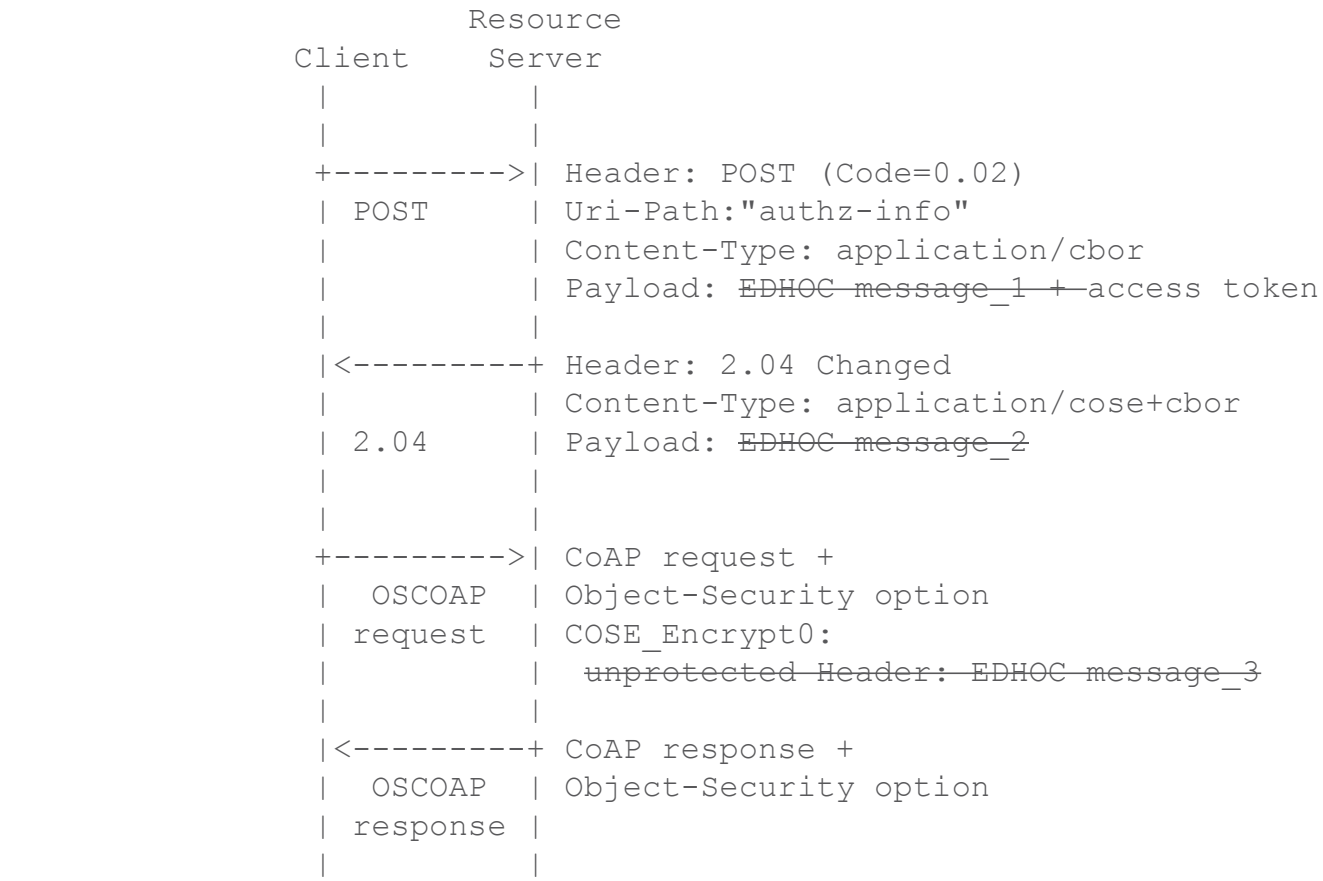


Figure 6: Key establishment with EDHOC via the authz-info endpoint

OSCOAP



Key establishment without EDHOC via the authz-info endpoint

OSCOAP or EDHOC+OSCOAP

EDHOC + OSCOAP

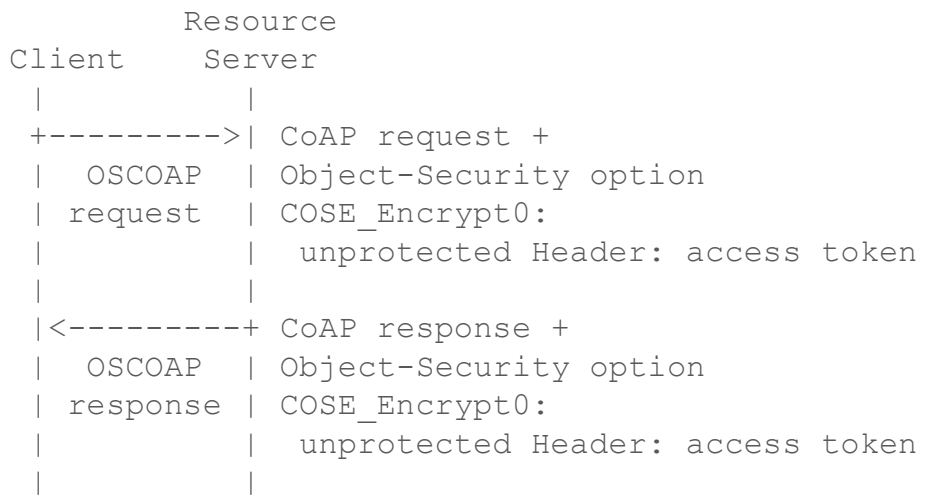
› Smaller Access Token + RS Info

› Perfect Forward Secrecy

OSCOAP

› Smaller messages

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



Planned Next Steps

- Get feedback
- SICS Implementation

Thank you!

Comments/questions?