



EDHOC-OSCORE profile of ACE
draft-ietf-ace-edhoc-oscore-profile-08

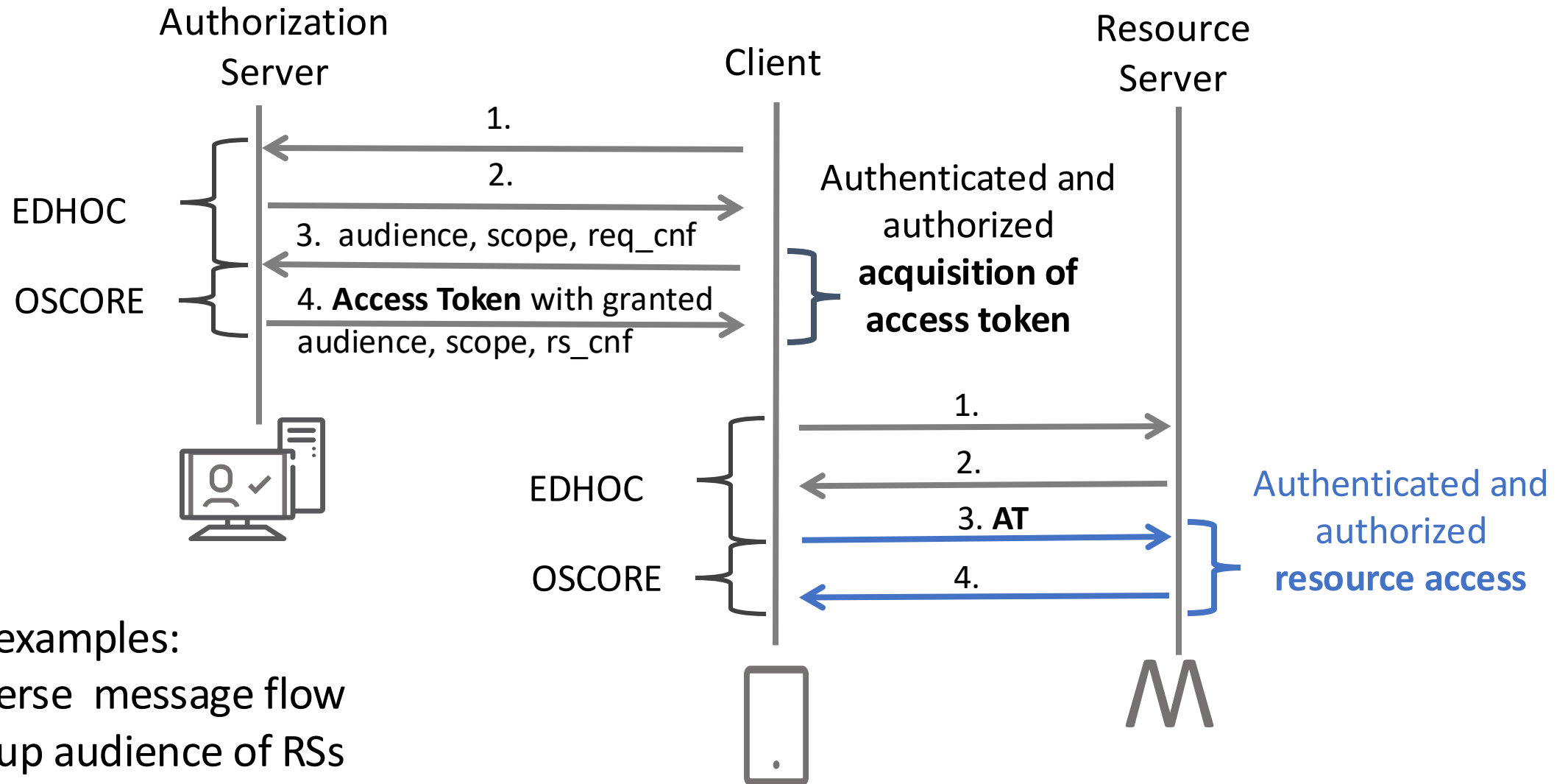
Göran Selander, John Preuß Mattsson, Ericsson AB
Marco Tiloca, Rikard Höglund, RISE AB

IETF 123, ACE WG, July 24, 2024

EDHOC-OSCORE profile of ACE

- Examples of using EDHOC-OSCORE profile
- Main changes in -08
- Next steps

Example (Optimized forward message flow A.2)



- Other examples:
 - Reverse message flow
 - Group audience of RSs
 - Multicast trigger

Main changes in -08:

- New EAD items for improving information flow
- Revision of EDHOC information
- Clarifications and editorials

EAD item A: Retrieve Request Creation Hints

- ead_value = AS_request_creation_hints or empty
 - Empty item asks for AS_request_creation_hints
- Forward message flow: EAD_1 (empty) and EAD_2
- Reverse message flow: EAD_2 (empty) and EAD_3
- non-critical – can be ignored by the receiving peer
- OPTIONAL to implement
- AS_request_creation_hints SHOULD NOT include "audience" and "scope" when present in the EAD item conveyed in the EAD_2 field.

EAD item B: Request Authentication Credential By Value

- ead_value is empty
- When present in EAD_1
 - it requests the AUTH_CRED_R by value in ID_CRED_R (message_2)
- When present in EAD_2
 - it requests AUTH_CRED_I by value in ID_CRED_I (message_3)
- non-critical – can be ignored by the receiving peer
- OPTIONAL to implement
- Main use in forward message flow, but can also be used in reverse flow

Revision of EDHOC Information

- OSCORE specific EDHOC information removed
 - osc_version, osc_ms_len, osc_salt_len
- Labelling of EDHOC information as
 - Prescriptive (need to comply with)
 - Non-Prescriptive (informational)
 - e.g., mandatory use of message_4 (P)
 - e.g., methods supported (NP)
 - helps out when using EDHOC application profiles

Next steps

- Needs another iteration
 - Review reverse message flow
 - Implications of access token in respective messages
- More text on choice of forward / reverse flow and the choice of message for carrying access token
- Discuss RS belonging to multiple audiences
- Discuss control of AUTH_CRED_C used by AS
 - and thereby control of Public key of C