Ephemeral Diffie-Hellman Over COSE (EDHOC) and Object Security for Constrained Environments (OSCORE) Profile for Authentication and Authorization for Constrained Environments (ACE)

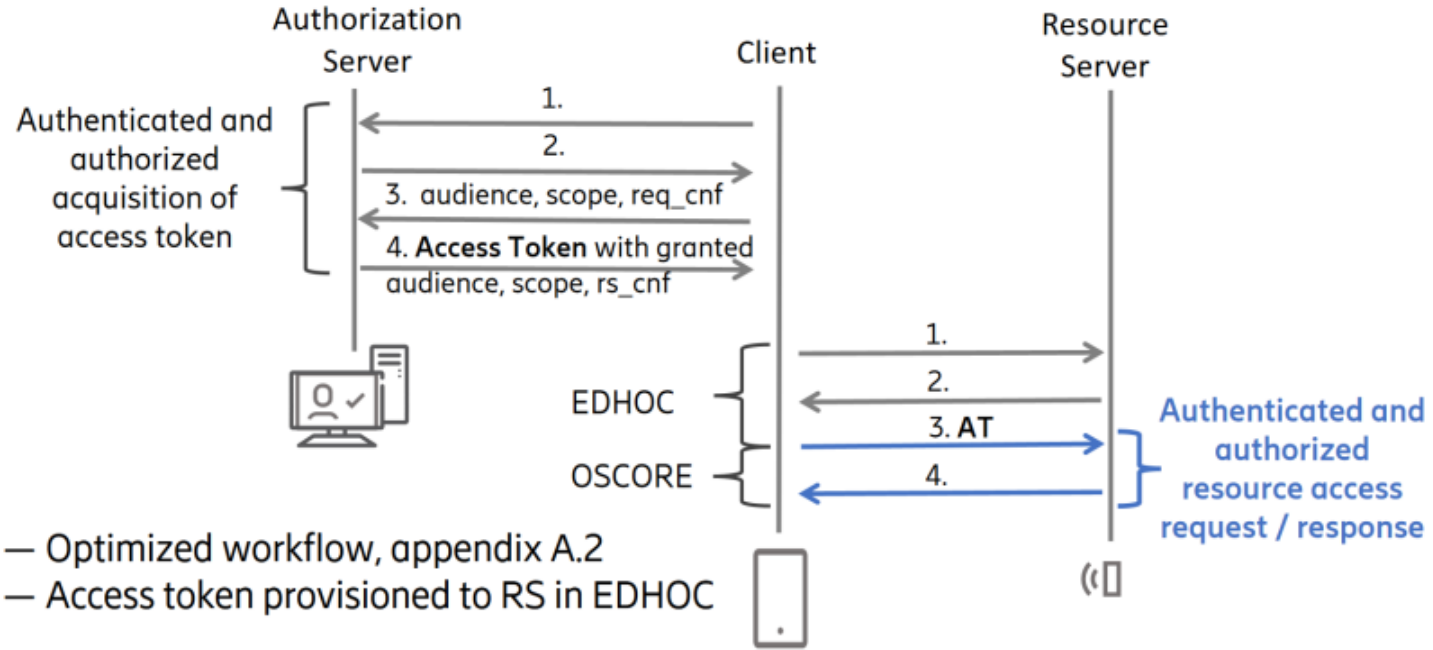
draft-ietf-ace-edhoc-oscore-profile-06

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

IETF 121 meeting – Dublin – November 8th, 2024

Overview

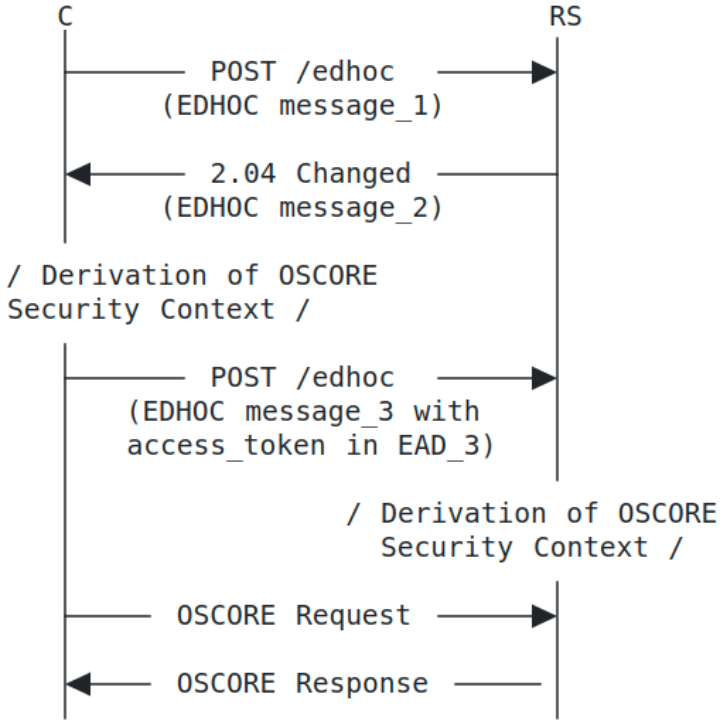
- **New profile of the ACE framework**
  1. Uses EDHOC for key establishment (and optionally Access Token uploading in an EAD item)
  2. Uses OSCORE for secure communication (based on keying material from EDHOC)



Main Updates in v -06 (1/3)

- **The access token can be uploaded in EDHOC in EAD_3, EAD_2, or EAD_4**
  - Previously only EAD_3 was mentioned
  - Reverse message flow: EAD_2 or EAD_4
  - Forward message flow: EAD_3
  - Goal: Enable both EDHOC message flows
    - Identity of Initiator protected against active attacks
    - Identity of Responder protected against passive attacks

- **Disallow upload of the access token to the /authz-info endpoint over an unprotected channel**
  - Results in a simplification of the profile
  - Ensures the Access Token content is always protected, also for non-encrypted Access Tokens



(*) Proposed in *draft-ietf-cbor-edn-e-ref*

Main Updates in v -06 (2/3)

- **Included EDHOC EAD item for transporting a Session ID**
  - Used if the Access Token has been provisioned to the RS and is valid, but there is a need to establish a (new) OSCORE Security Context with EDHOC between C and RS
  - Serves as a binding to identify which Access Token to supersede

- **Provided more details and added example of dynamic update of access rights**
  - Clearer information on how update of access rights is performed
  - New Access Token is uploaded protected using the existing OSCORE Security Context
  - The session_id parameter indicates to the RS which token to update

Main Updates in v -06 (3/3)

- **Editorial improvements and revised examples**
- **Defined in detail the use of the EDHOC reverse message flow**
  - Aligned with the normal execution of EDHOC
  - C makes an empty POST request to the EDHOC resource at RS (trigger request)
  - If EAD_2 or EAD_4 includes the EAD item EAD_ACCESS_TOKEN
    - … the RS MUST ensure that the included access token is valid
  - If EAD_2 or EAD_4 includes the EAD item EAD_SESSION_ID
    - ... the RS MUST ensure that the access token associated with that session_id and with the AUTH_CRED_C used in the EDHOC session is valid
- **Provided details on access token invalidity**
  - An access token becomes invalid, e.g., due to its expiration or revocation:
  - … then the RS MUST delete the Access Token and associated OSCORE Security Context
  - ... and the RS MUST notify C with an error response with code 4.01 (Unauthorized) for any long running request (e.g. observation)

Select Next Steps

- **Mandate Access Token Request/Response to be encoded in CBOR**
  - In the interest of simplification
  - Already stating that the EDHOC_Information object must be encoded as CBOR
- **Proof-of-possession of the Client's private key at the AS**
  - When receiving the Client's authentication credential in the 'req_cnf' parameter of the Access Token Request
  - Ongoing discussions on different approaches for accomplishing this
- **Discussion and guidelines on Access Tokens issued to a group-audience**
- **Comparison of privacy and security properties of including the Access Token in EAD_2 or EAD_4**

Thank you!

Comments/questions?

https://github.com/ace-wg/ace-edhoc-oscore-profile