EDHOC-OSCORE profile of ACE

draft-ietf-ace-edhoc-oscore-profile-04

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

IETF 119, ACE WG, March 19, 2024
EDHOC-OSCORE profile of ACE

— Quick recap

— Main changes in -04

— Selected open issues:
  — $\text{ID}_{\text{CRED}}$ size optimization considerations
  — Use of EDHOC reverse message flow
Recap EDHOC-OSCORE profile

Authenticated and authorized acquisition of access token

1. Access
2.
3. audience, scope, req_cnf
4. Access Token with granted audience, scope, rs_cnf

Authenticated and authorized resource access request / response

— Optimized workflow, appendix A.2
— Access token provisioned to RS in EDHOC
Main changes in -04:

— Removed option to transport access token in EAD_1
  — Remaining options: POST/authz-info and EAD_3

— Updated EAD item (ead_label, ead_value)
  — ead_value = { 0 : access_token }
  — ead_value = { 1 : session_id }

— Additional EDHOC_INFORMATION parameters
  — supported types of authentication credentials, -identifiers, EAD items, Initiator/Responder role

— Clarifications of session_id, token_series, and association between session_id, access token, and security context
Optimization considerations  1(3)

Simplified example with RPK, i.e., CWT Claims Set (CCS)

1. Learn \((PK_C, \text{kid}_C)\)
2. Verify PoP
3. Include \((PK_C, \text{kid}_C)\) in Access Token

Assume RS has multiple Clients - how different will the \text{kid}_C be?

RS uses \text{kid}_C to look up \(PK_C\) and authenticate C
Optimization considerations 2(3)

Learn \((PK_{RS}, kid_{RS})\)  
Verify PoP

Include \((PK_{RS}, kid_{RS})\) in response

Assume a Client have multiple RSs, either single-RS or group audience, - how different will the kid_{RS} be?

---

Resource Server

Authorization Server

1. 
2. 
3. 
4. \(AT, (PK_{RS}, kid_{RS})\)

Client

1. 
2. \(ID_{CRED} = kid_{RS}\)
3. \(AT, ID_{CRED} = kid_{C}\)

C uses kid_{RS} to look up PK_{RS} and authenticate RS
Optimization considerations

— Use of kids allow for very short credential identifiers

— But many-to-one settings can result in much lookups in the RPK/CCS case

— Proposal to define new CBOR headers / conf claims
  — for hash of CCS/CWT
    — not as short as kid but stochastically unique
  — for URI to CCS/CWT

— Analog to x5t/x5u

— Comments?
Reverse flow

— Proposal to support the EDHOC reverse message flow
— AT in EAD_2 can be read by an active attacker
— Compare forward flow
  — AT in EAD_3: not read by intermediary
  — POST /authz-info: read by passive attacker
— Comments?