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-05

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

IETF 120 meeting – Vancouver – July 22nd, 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-05 (1/3)

CBOR diagnostic notation in examples

› Revised to use the construct e" (*) for importing values from a CDDL model
  - e'SOME_NAME' is replaced by the value assigned to SOME_NAME in the CDDL model in Appendix C
  - For example, \{e'session_id' : h'01', e'cipher_suites': 3\} stands for \{0 : h'01', 2 : 3\}.

› Use registered CBOR abbreviations
  - Together with comments
  - "scope" : "write" / scope / 9 : "write"
Main Updates in v-05 (2/3)

› Editorial improvements

› IANA considerations
  – Fixed name of registry columns
  – Change controller: s/IESG/IETF
  – Revised, detailed registration policies for the new registry "EDHOC Information"

› Simplification: only CWTs are supported as Access Tokens
  – That is, rule out JWTs otherwise admitted by ACE
  – CWTs are anyway RECOMMENDED in RFC 9200

› Made [1] an informative reference
  – The ACE alternative workflow is just considered as an example
  – The concept of "token series" taken from there is expanded and customized here

Main Updates in v-05 (3/3)

› Clarification: EDHOC can be used in the forward or reverse message flow
  – I.e., the EDHOC Initiator can be (i) the ACE Client or (ii) the ACE Resource Server (RS)
    I. The Client starts EDHOC by sending EDHOC message_1 to RS
    II. The Client sends a “trigger request” to RS, which replies with EDHOC message_1
  – What to use depends on the deployment setting, and mostly on which identity to protect the most (the Initiator’s identity is protected against active attackers)

› Allow transporting the Access Token in the EAD item of any EDHOC message
  – EDHOC forward message flow: EAD1 or EAD3
  – EDHOC reverse message flow: EAD2 or EAD4
  – What to use depends on
    › The used EDHOC message (see above)
    › The security/privacy properties to achieve (still to be discussed, see also issue #8)

Issue #8: https://github.com/ace-wg/ace-edhoc-oscore-profile/issues/8
Next Steps

› Consistency-checking authentication credentials from different EDHOC fields
  – E.g., if an EAD item transports the CWT including C's authentication credential, …
  – … the authentication credential from ID_CRED_X and the EAD item have to be the same

› IANA review feedback on Section 10.3
  – Add column in the “OAuth Parameters CBOR Mappings” registry called "Original Specification"

› Describe actions to take after invalidation/deletion of authentication credentials
  – Building on and expanding the high-level guidelines from draft-ietf-lake-edhoc-impl-cons

› Cover the usage of the EDHOC reverse message flow in more detail

› 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

› Discussion and guidelines on Access Tokens issued to a group-audience
Thank you!

Comments/questions?

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