EDHOC-OSCORE profile of ACE-OAuth

draft-selander-ace-edhoc-oscore-profile-00

G. Selander, J. Preuß Mattsson, Ericsson
M. Tiloca, R. Höglund, RISE

ACE Interim, 12 September 2022
Motivation

— `coap-oscore` profile of ACE–OAuth (RFC 9203)
  — defines authorization and access control Client for access to resources at a Resource Server
  — provisioning of access rights and associated secret symmetric key
  — uses OSCORE (RFC 8613)

— This profile (`coap-edhoc-oscore`)
  — provisioning of access rights and associated asymmetric key (authentication credential)
  — uses EDHOC (draft-ietf-lake-edhoc)
    — and then OSCORE with the shared secret

— More strict trust model than RFC 9203
— Lower overhead than RFC 9202
Compare RFC 9202 / RFC 9203

Compared to RFC 9202 (coap-dtls)

- Identical token provisioning
- EDHOC instead of DTLS handshake
- OSCORE instead of record layer

Compared to RFC 9203 (coap-oscore)

- Nonce/ID exchange in RFC 9203
- No EDHOC exchange in RFC 9203
- OSCORE security context derivation in both

Figure 1: Protocol Overview

The following subsections describe the details of the POST request and response to the /token endpoint between C and AS. In this exchange, AS provides C with the access token, together with a set of parameters that enable C to run EDHOC with RS. In particular, these include information about the authorization credential of RS, AUTH_CRED_RS, transported by value or uniquely referred to.
Other properties of coap-edhoc-oscore

- Supports update of access rights
  - Introduces the term “token series”
  - Highlight existing access tokens between same C and RS (same series)

- Supports update of security context without updating access rights
  - EDHOC-KeyUpdate (see EDHOC)
  - Key Update for OSCORE (draft-ietf-core-oscore-key-update)

- Supports the use of authentication credential by reference and by value (like EDHOC)

- Specifies EDHOC Information for use by C or RS when determining application profile of EDHOC
  - May be included in message exchange before running EDHOC
  - Registers parameters and claims used by EDHOC
Examples in Appendix A

Optimizations
— Access Token may be carried in the EAD_1 field of EDHOC message_1
  — instead of a separate POST /authz-info exchange

— EDHOC and OSCORE can be combined in two round trips
  — draft-ietf-core-oscore-edhoc
  — (optionally with Access Token in message_1)

Alternate flow
— AS, instead of C, may POST /authz-info to RS
  — Generalize to framework?
Next steps

— Already very detailed

— Minor update: Parameter informing C that RS supports KUDOS

— Ready for WG review