

EDHOC-OSCORE profile of ACE

draft-ietf-ace-edhoc-oscore-profile-02

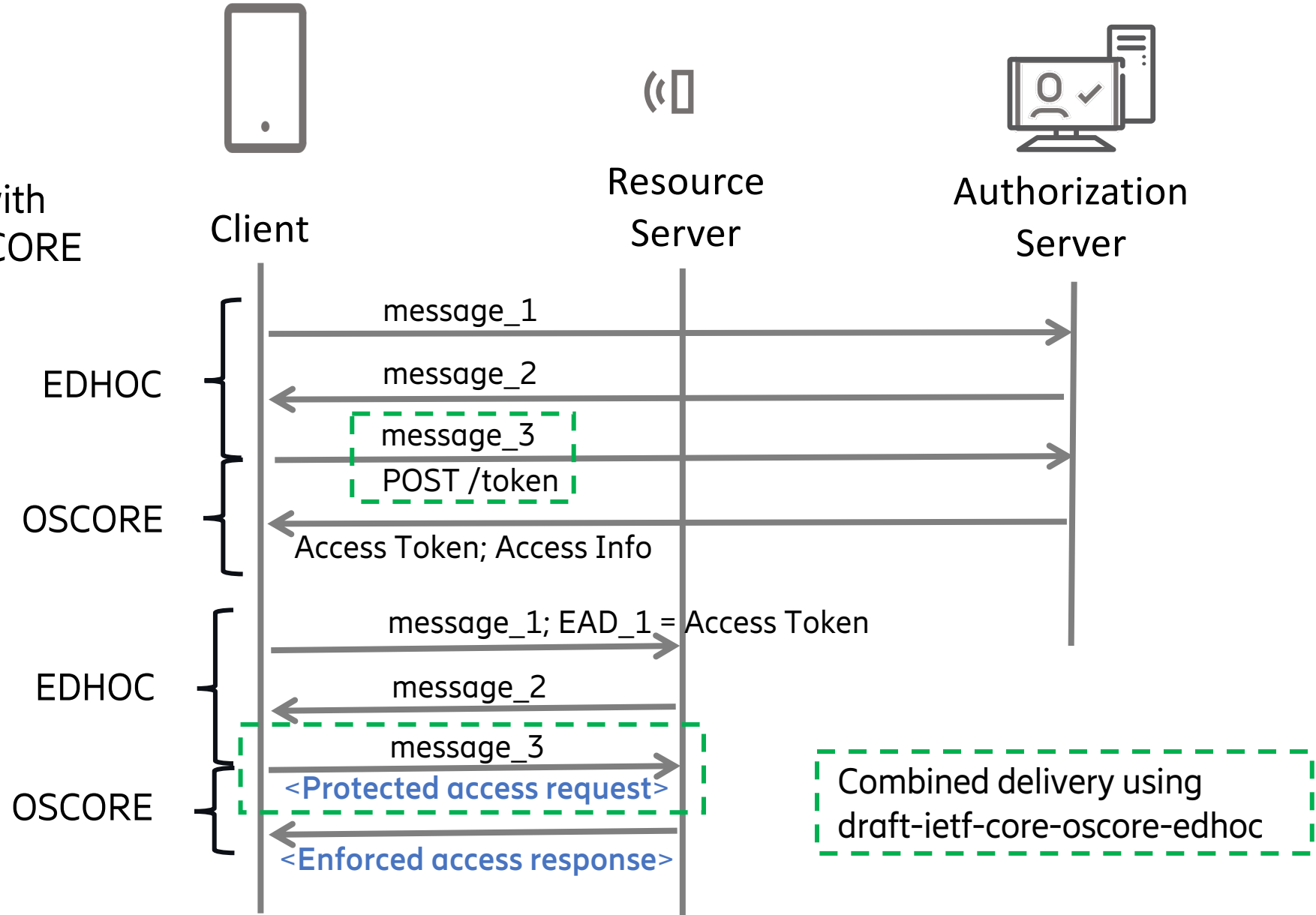


<https://github.com/ace-wg/ace-edhoc-oscore-profile>

IETF 117, ACE WG, July 24, 2023

Recap

- ACE workflow with EDHOC and OSCORE
- Example A.2
 - Optimized



Since IETF 116

- Version -02
 - Simplified protocol
 - Removed use of EDHOC KeyUpdate
 - Security context updated either by KUDOS or rerun of EDHOC
 - Alternative workflow (AS token posting) specified in separate draft
 - Updated examples
- Next steps
 - Proof of possession of client private key to AS
 - Explicit PoP or EDHOC
 - IANA registrations
 - New CWT confirmation methods

Related Discussions

- Optimized Access Token for multiple RSs
 - Privacy of Access Token
- Side meeting
Tuesday 13:00 local time (Hackathon room in Gather)
- Onboarding RS into ACE ecosystem
 - Side meeting
Wednesday 08:30 local time (Hackathon room in Gather)
- Gather: <https://www.ietf.org/how/meetings/gather/>