Since IETF 115

— Version -01 submitted, minor update
  — Appendix with profile requirements
  — Updated parameter names
  — Updated references

— Ongoing discussion: simplifying the flows = content of this presentation
ACE-OAuth Framework Steps

C → AS: Request access rights

AS → C: Access token and RS info

C → RS: Access token

C ↔ RS: Authenticate

C → RS: Authorized access with protected communication

— Simplified sequence of steps, see RFC 9200

— Existing ACE profiles describe alternative flows, see RFC 9202/9203:
  A. Update access rights w/o re-authentication
  B. Update security context w/o changing access rights
     — Provision access token within authentication protocol
A. Update access rights w/o re-authentication

C → AS: Request access rights

AS → C: Access token and RS info

C → RS: Access token

C ↔ RS: Authenticate

C → RS: Authorized access with protected communication

C → AS: Request access rights

AS → C: Access token and RS info

C → RS: Provision new access token protected with existing context

C → RS: Authorized access with protected communication
B. Provision access token in authentication protocol

1. **C → AS**: Request access rights
2. **AS → C**: Access token and RS info
3. **C → RS**: Access token
4. **C ↔ RS**: Authenticate
5. **C → RS**: Authorized access with protected communication

6. **C → AS**: Request access rights
7. **AS → C**: Access token and RS info
8. **C ↔ RS**: Authenticate + provision access token
9. **C → RS**: Authorized access with protected communication
EDHOC-OSCORE profile alternative flows

In version -01:

A. Update access rights w/o re-authentication
B. Update security context w/o changing access rights
   1. Provision access token in EDHOC EAD_1 [1]
   2. Using EDHOC_KeyUpdate [1]

Proposal: Remove option B.2

Comments / suggestions?

[1] draft-ietf-lake-edhoc
[2] draft-ietf-core-oscore-key-update