EDHOC-OSCORE profile of ACE

draft-ietf-ace-edhoc-oscore-profile-01
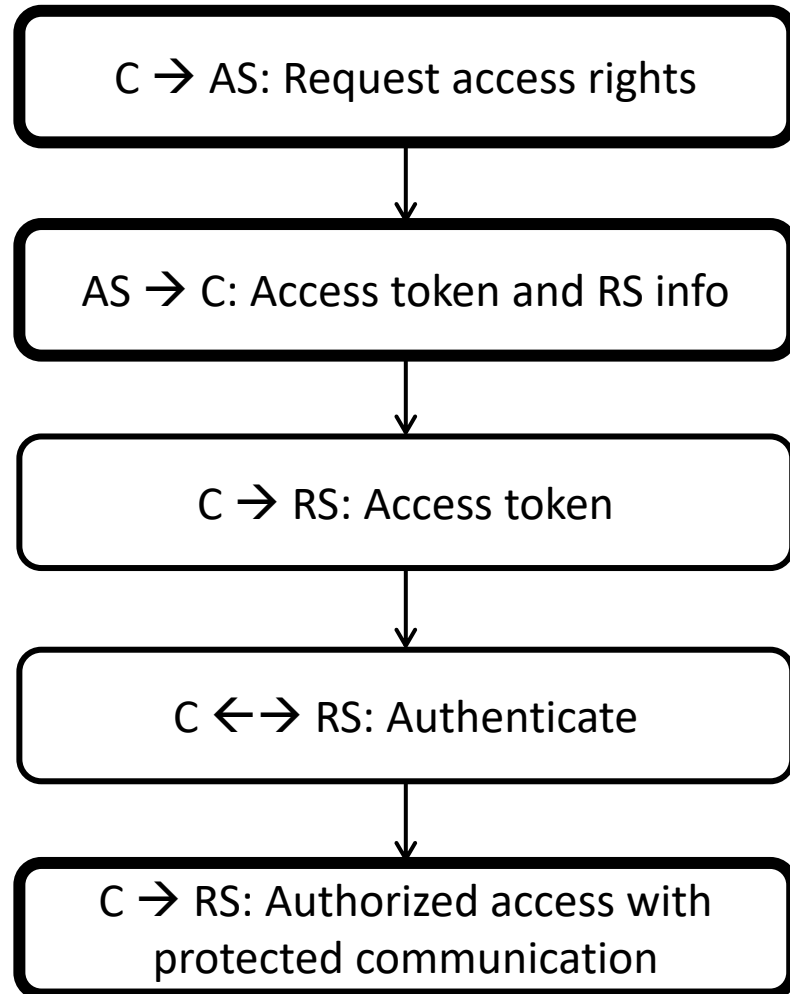
https://github.com/ace-wg/ace-edhoc-oscore-profile

IETF 116, Yokohama, ACE WG, March 30, 2023

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     │
└─────────────────────────────────┘
```
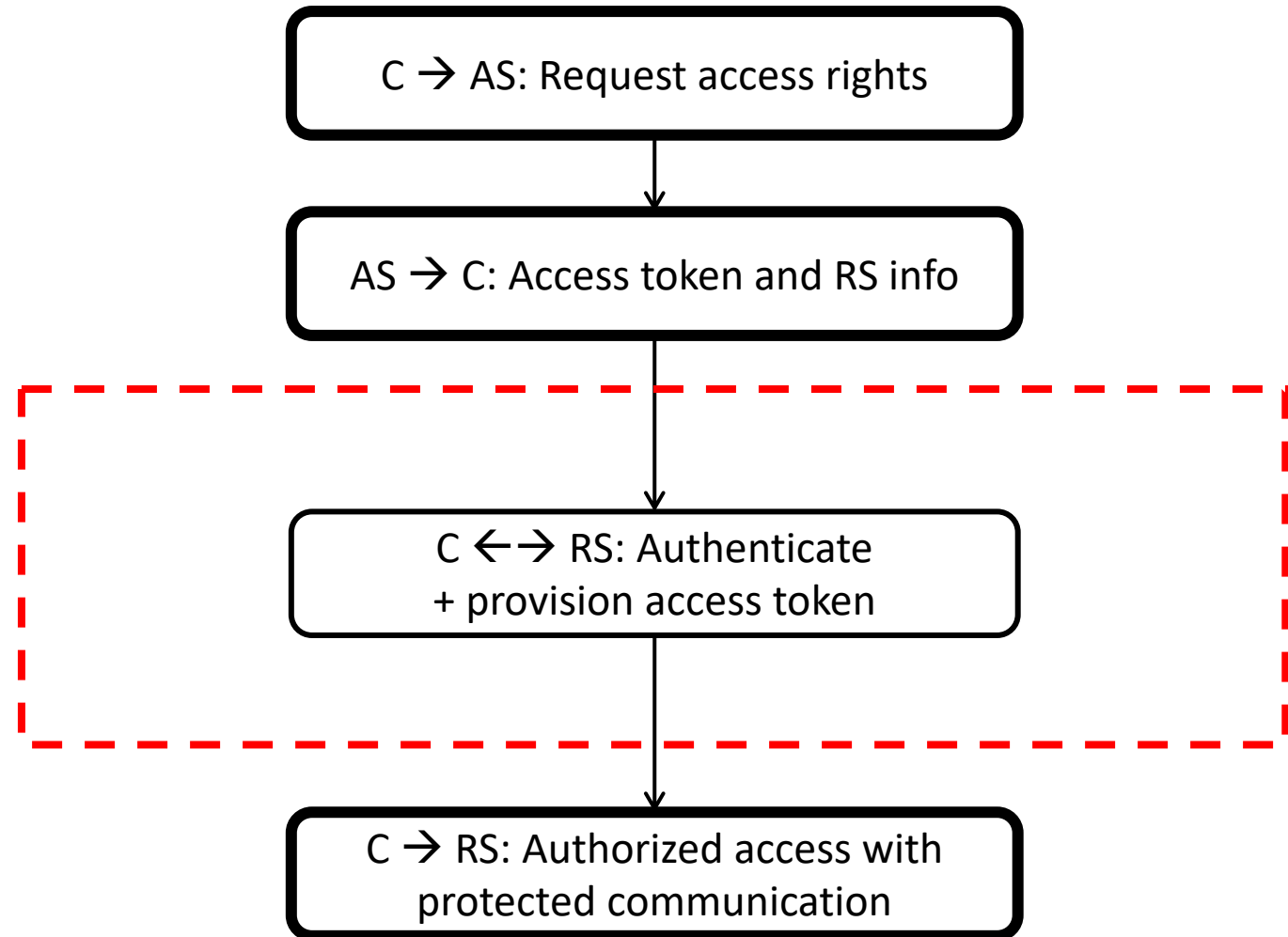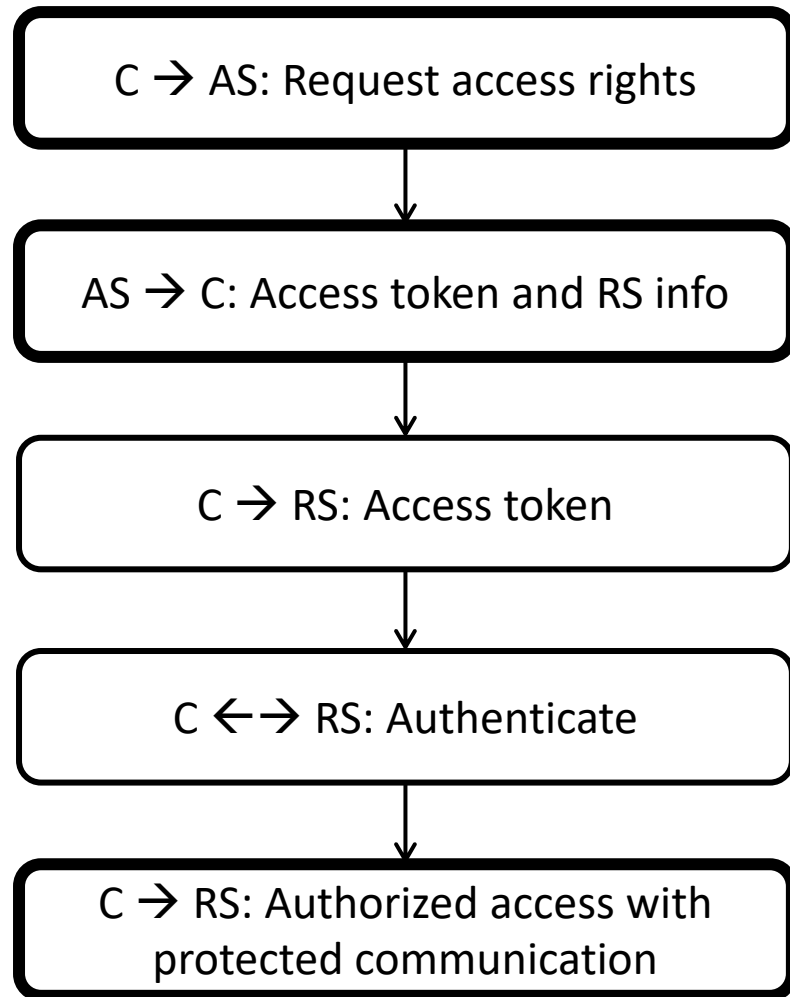
— Simplified sequence of steps, see RFC 9200

— 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
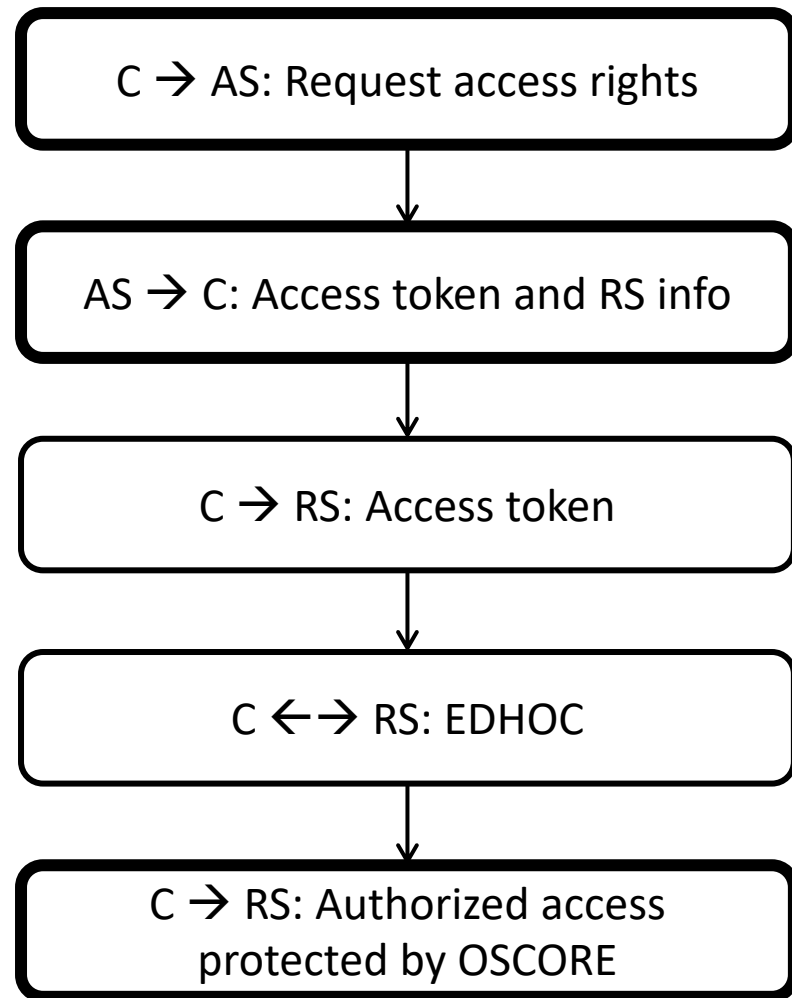   — Provision access token within authentication protocol

3

A. Update access rights w/o re-authentication
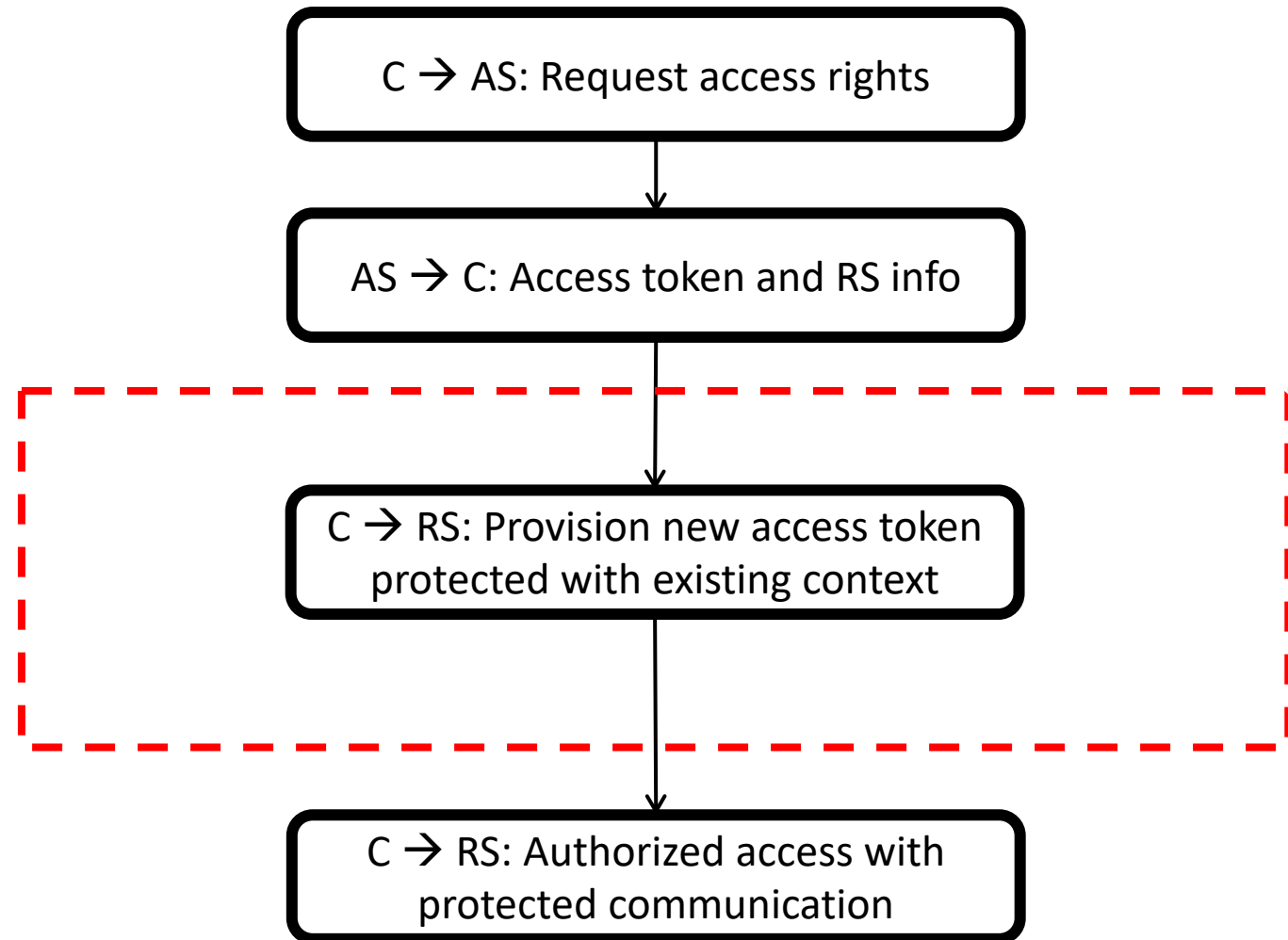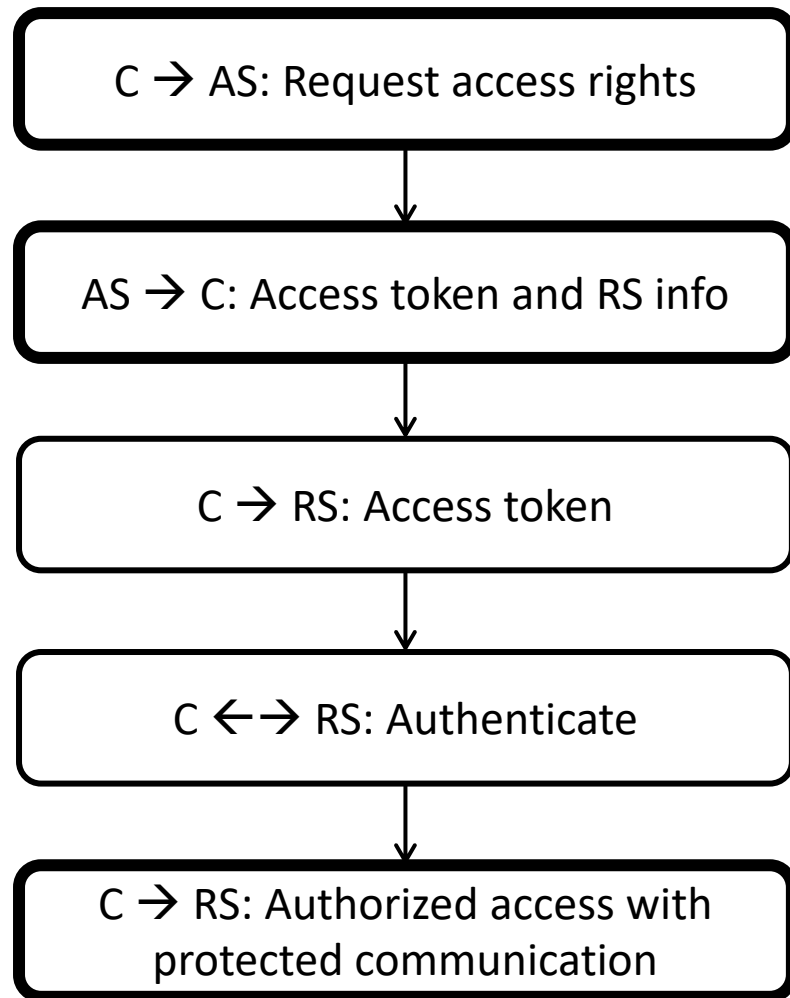
B. Provision access token in authentication protocol

EDHOC-OSCORE profile alternative flows

C → AS: Request access rights

AS → C: Access token and RS info

C → RS: Access token

C ←→ RS: EDHOC

C → RS: Authorized access protected by OSCORE

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]
   3. Using KUDOS [2] (if supported)

Proposal: Remove option B.2

Comments / suggestions?

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