Key Provisioning for Group Communication using ACE

draft-palombini-ace-key-groupcomm-00

Francesca Palombini, Ericsson
Marco Tiloca, RISE SICS

IETF 101, Ace WG, London, Mar 19, 2018

Motivation & Scope

- 2 drafts about joining secure group communication:
  - draft-palombini-ace-coap-pubsub-profile (PubSub) (v-00 at IETF98)
  - draft-tiloca-ace-oscoap-joining (Group Comm using OSCORE) (v-00 at IETF99)

- Feedback from WG about similarities

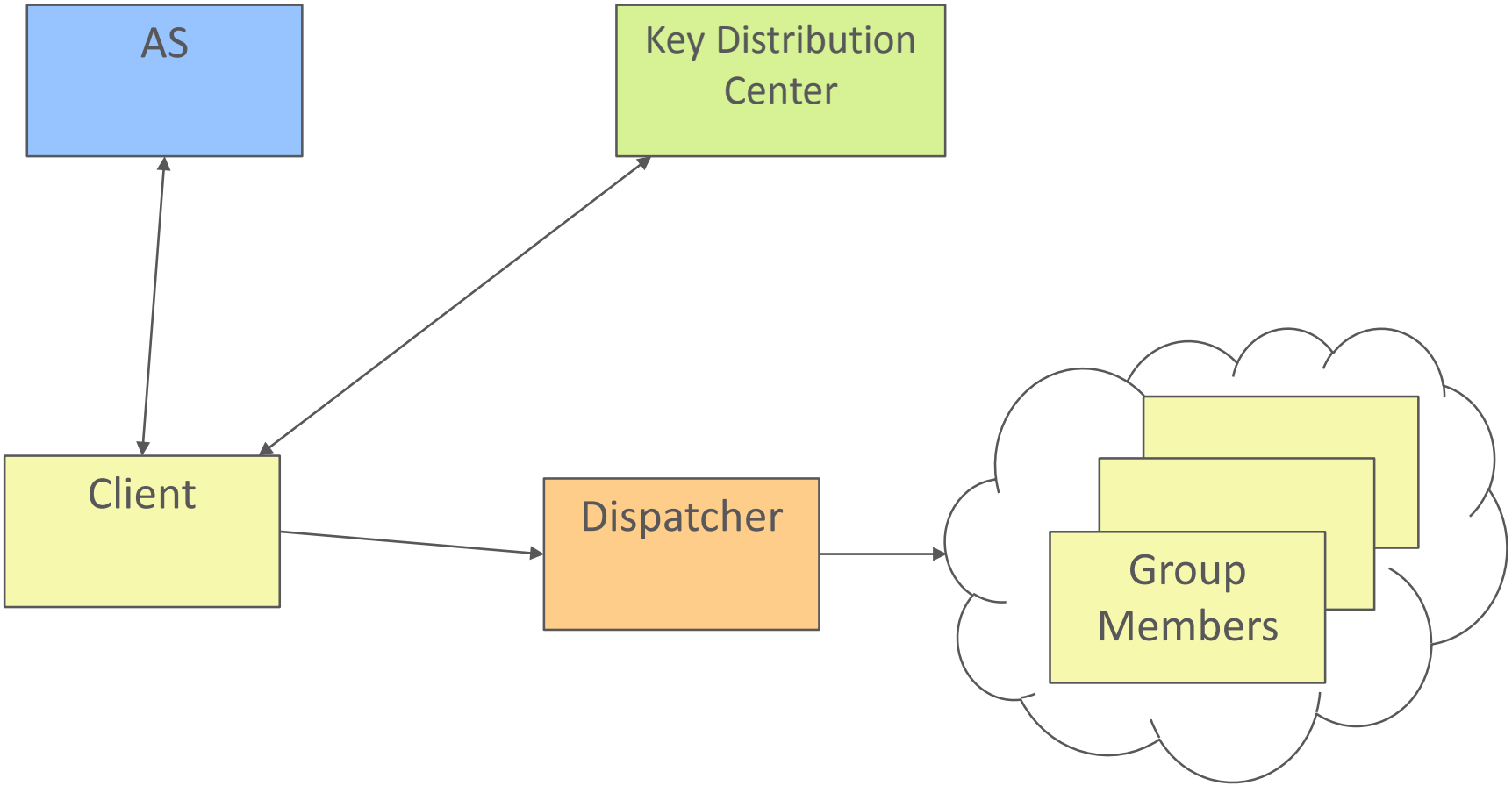
In Scope:

- Message format to authorize and distribute keying material
- Use of ACE framework and profiles

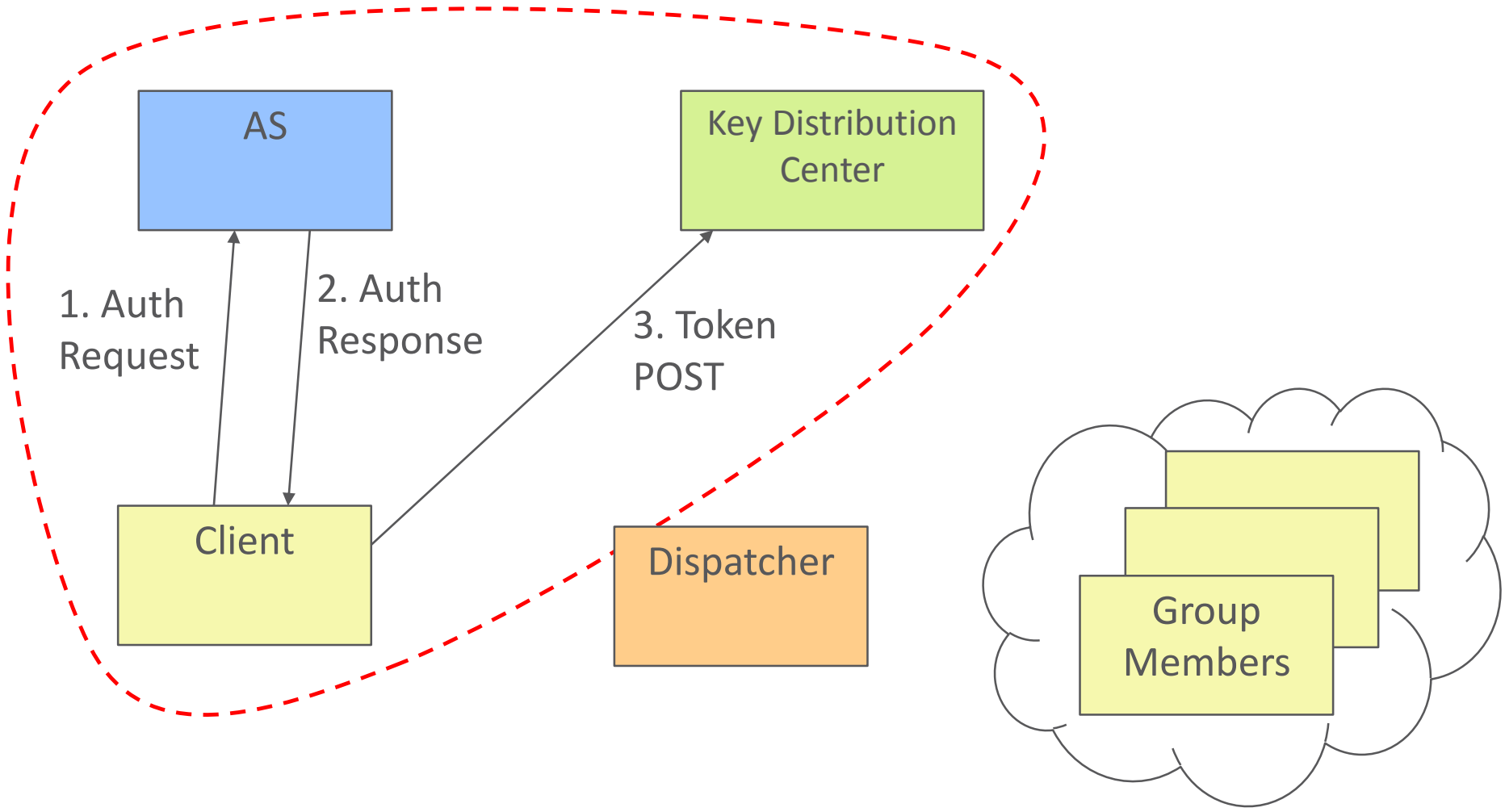
Out of Scope:

- Revocation and Renewal
- Group Communication Protection

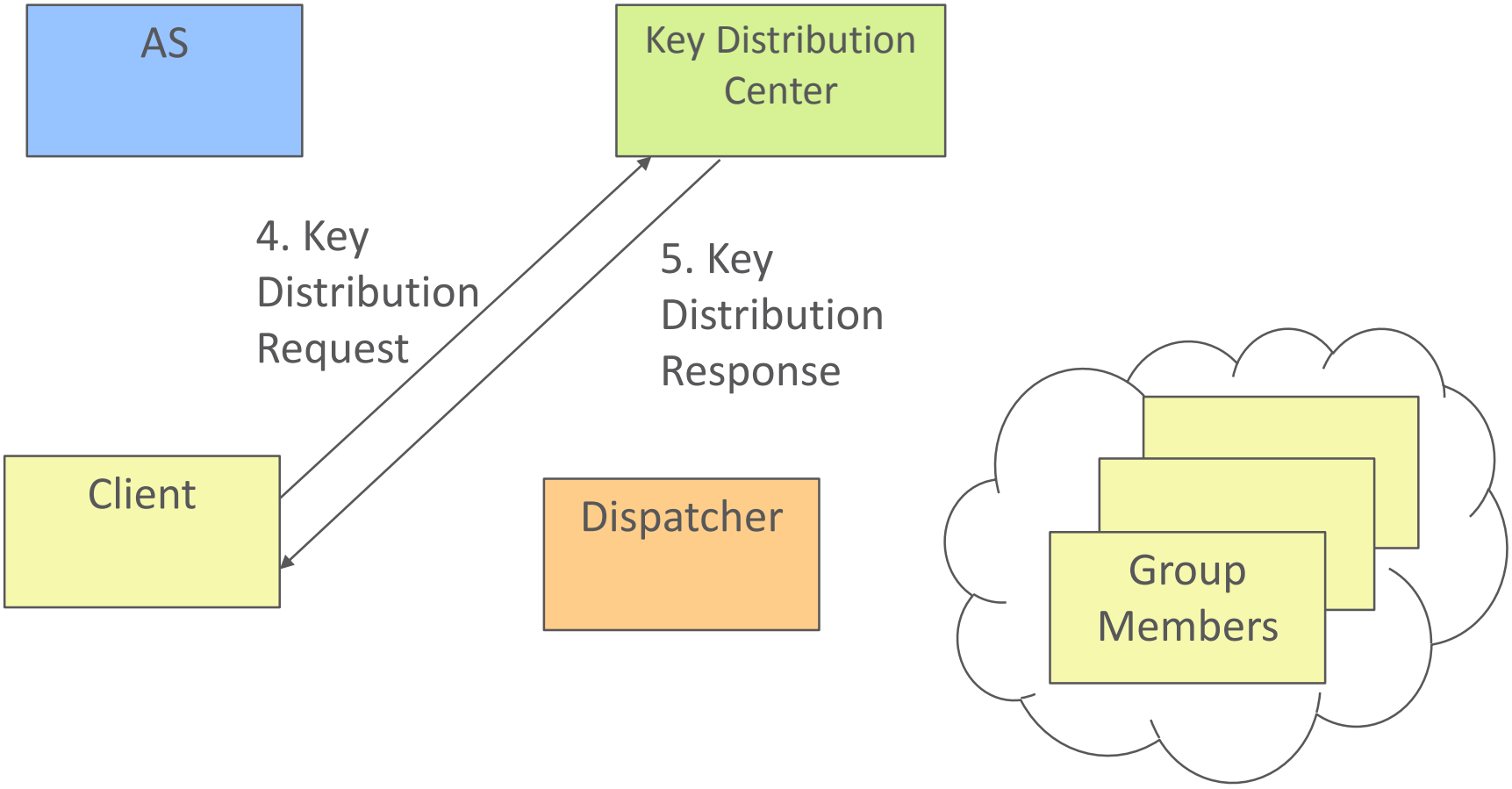
Overview


AS
Key Distribution Center
Client
Dispatcher
Group Members

Phase 1. Using ACE

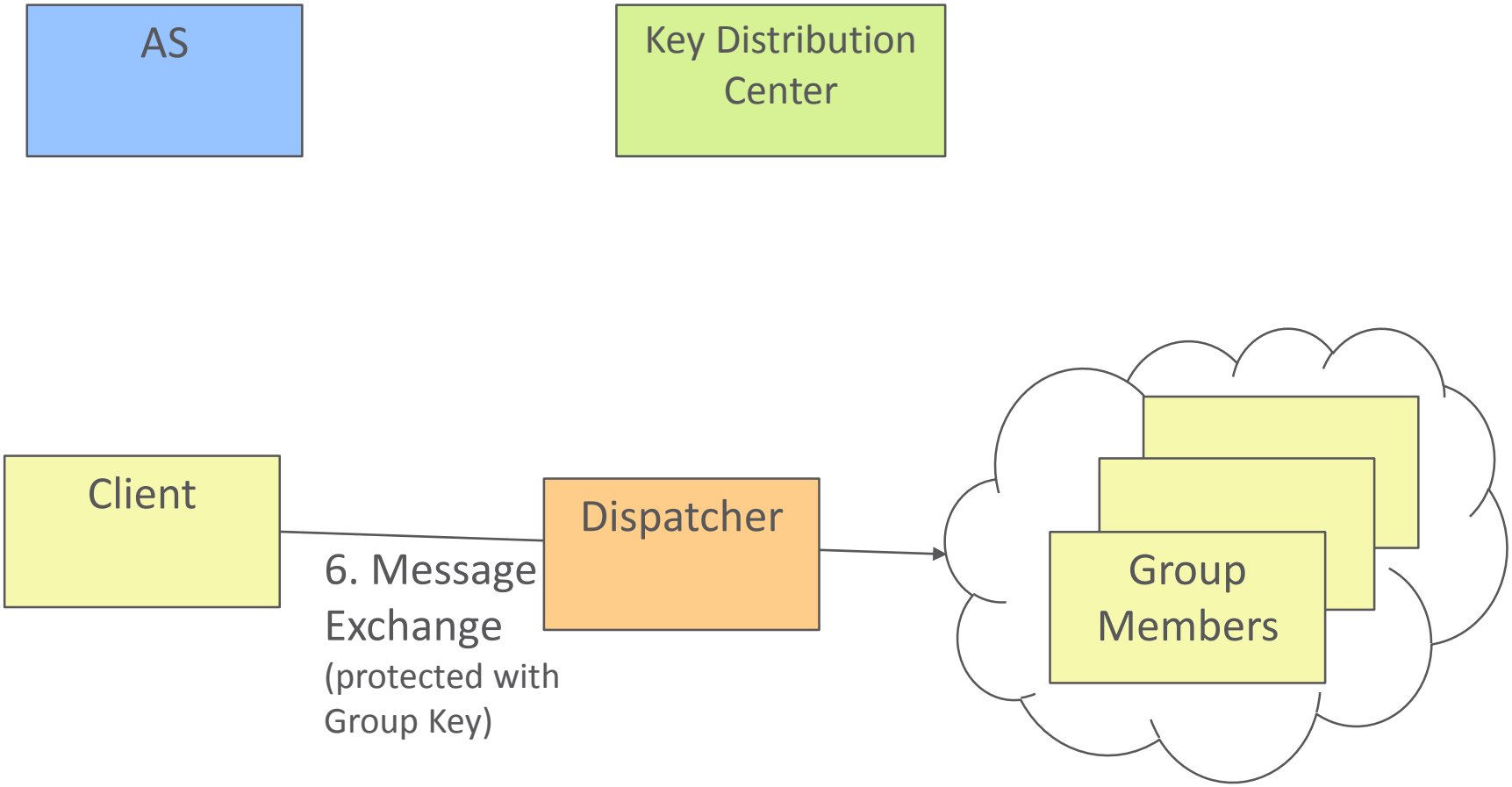


Phase 2. Requesting Group Keying Material



Phase 3. Protected GroupComm

(out of scope)



Authorization Request / Response

Request

- MUST contain:
  - grant_type
- MAY contain:
  - scope ← Group ID/topic/… + role of the client
  - aud ← KDC
  - cnf ← public key (or cert) of the client
  - **get_pub_keys ***, if the client wants to receive public keys of other members of the group

Response

- MUST contain:
  - access_token ←all the param below + scope + get_pub_keys (if present in req)
  - cnf
  - rs_cnf
  - exp
- MAY contain:
  - scope ← if different from Authorization Request

***:** New parameter, defined in this doc

Key Distribution Request/ Response

Request = POST + payload

- MAY contain:
  - scope ← Group ID/topic/… + role of the client
  - **get_pub_keys ***, if the client wants to receive public keys of other members of the group
  - **client_cred *** ← pub key (or cert) of the client
  - **pub_keys_repos *** ← if client_cred contains a cert, list of pub keys repos

***:** do not exist in ACE

Response = 2.01 + payload

- MUST contain:
  - COSE_Key:
    - kty
    - k
    - alg
    - kid
    - base iv
    - clientID
    - serverID
    - kdf
    - slt
    - **cs_alg ***
- MAY contain:
  - **pub_keys *** ← list of pub keys of members
  - **group_policies ***
  - **mgt_key_material *** ←admin key material to revoke and renew