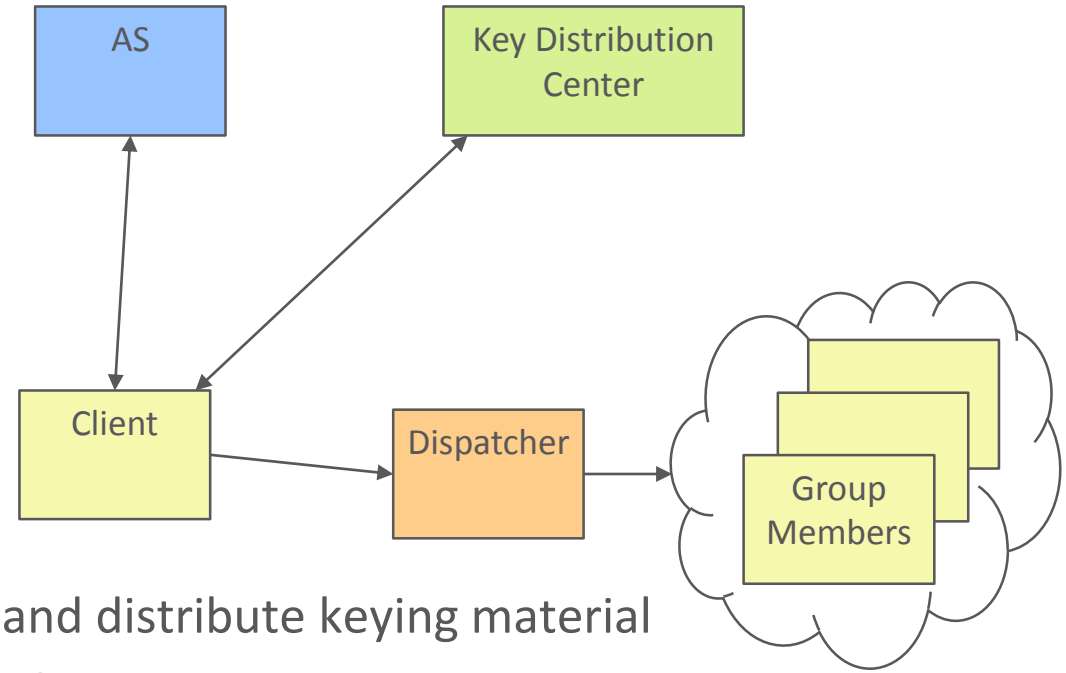
# Key Provisioning for Group Communication using ACE

draft-palombini-ace-key-groupcomm-01

**Francesca Palombini**, Ericsson
Marco Tiloca, RISE SICS

IETF 102, Ace WG, Montreal, Jul 16, 2018

# Recap




- draft about joining secure group communication:
  - Message format to authorize and distribute keying material
  - Use of ACE framework and profiles

Out of Scope:

- Group Communication Protection

- General “Revocation and renewal of keying material” is added to v-01 (detailed algorithm still out of scope)

# Status Update

Updated according to review and discussion at IETF101

- Minor details, including:
  - Get_pub_keys (“I want the public keys of those nodes”) parameter only sent to KDC (not to AS), and has different format: [id1, id2, …] or [ ]
  - Add expiration parameter for COSE_Key (Symmetric Key for groupcomm)

# Status Update

- Revocation (token expiration) or self removal from group:
  - triggers a rekeying from KDC to members of the group

- NEW: Retrieval of Updated Keying Material. The member can request:
  - Symmetric Key → for example if key expired, or reboot, or missed rekeying
    - Format: “Scope”
  - Public Keys for Group Members → for example if new members join
    - Format: “Scope” + “Get_pub_keys”

# Open Issues

Retrieval of updated keying material:

- To retrieve either the symmetric key or the public key(s) of members, the node uses the same format as when it joins *(Key Distribution Request*), simplified with only the param necessary (ex: “get_pub_keys” only if asking for public keys )

- As of now, it is not possible to “combine” these 2 requests, as it is not possible to differentiate between request to ask for symmetric key and request to ask for both.

# Open Issues

3 choices:

- Use different endpoints (1 for symmetric, 1 for public, 1 for both)
- Add an additional parameter to request symmetric
- Don’t combine

- Others?

# Open Issues

- Should the draft define something like that? Is it useful?
- If yes, what is the preferred choice?

# Key Distribution Request/ Response

*Request = POST + payload* *to the specific endpoint associated with the group*

- 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
    - **exp ***
    - 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

# CoAP PubSub profile

draft-palombini-ace-coap-pubsub-profile-03

**Francesca Palombini**, Ericsson

IETF 102, Ace WG, Montreal, Jul 16, 2018

# Status & Steps Forward

- Updated according to draft-palombini-ace-key-groupcomm-01
- Interest in previous meetings, couple of reviews
- Interest? Adoption?