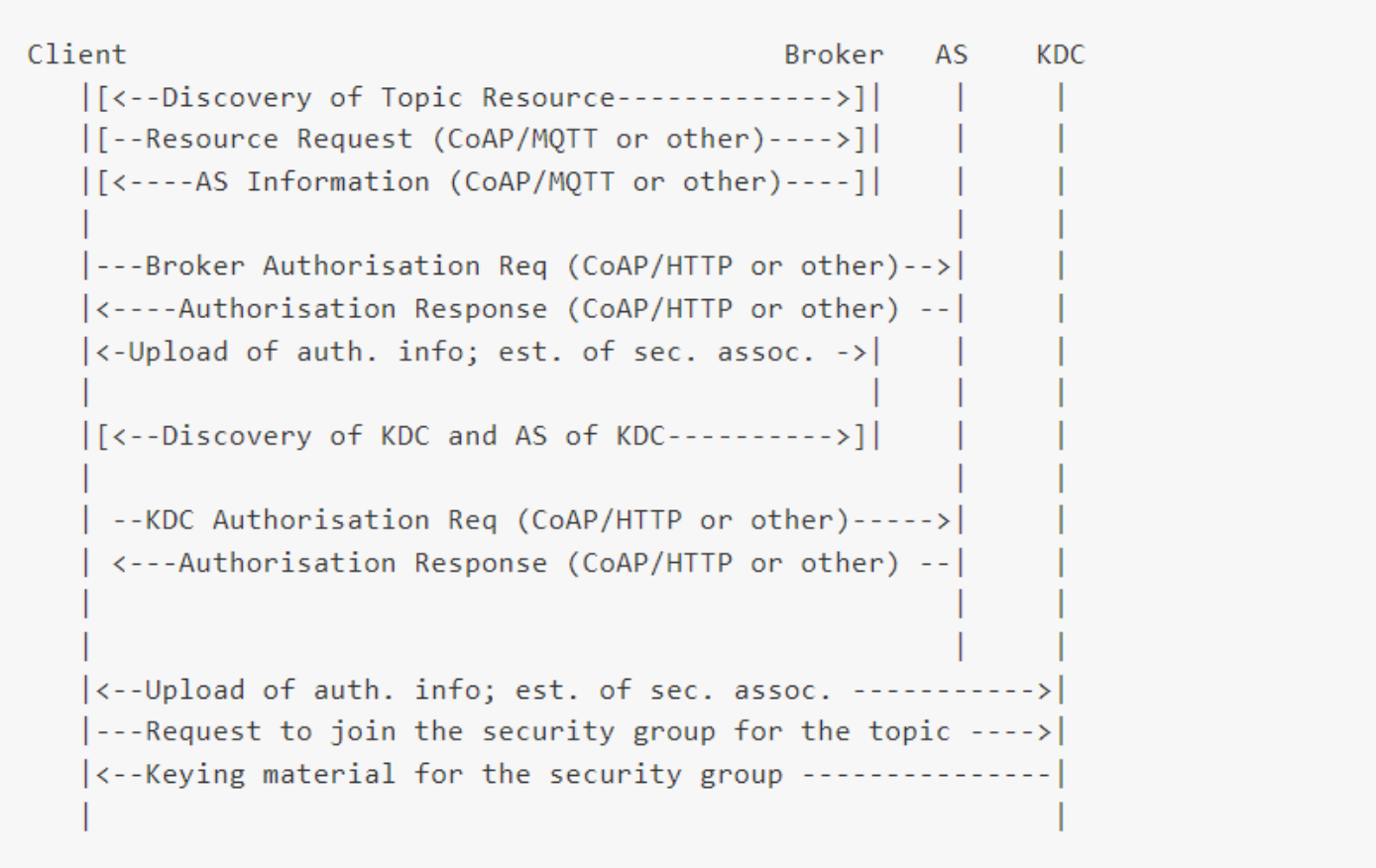
Pub-Sub Profile for Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-pubsub-profile-05

Francesca Palombini
Cigdem Sengul
Marco Tiloca

ACE Interim
05/06/2023

Message Flow with AS/KDC Discovery



KDC discovery:
Client can retrieve the URI of the KDC (and of the AS associated with that KDC).
At this step, **the name of the security group associated with the topic** can also be retrieved from the topic resource.
No unauthorised publisher/subscriber

Scope

- The possible **permissions** for a Client are: Publish (1), **Read (2)** and Delete (3).
- Since such permissions are related to user operations, a scope entry as specified in this application profile does not indicate the permission Admin (0).
  - Such permission is reserved for scope entries that express permissions for Administrators of Pub/Sub groups.
  - That is, in scope entries used as defined in this application profile, the least significant bit of "Tperm" MUST be set to 0.
- Add one more bit 1 "GroupType", with value 0 in case of application, and 1 in case of security group.

```
AIF-PUBSUB-GROUPCOMM = AIF-Generic<pubsub-topic, pubsub-perm>
 pubsub-topic = tstr ; Pub/sub topic name
                     ; (the associated security group)

 pubsub-perm = uint . bits pubsub-roles

 pubsub-roles = &(
  Admin: 0,
  Pub: 1,
  Sub: 2,
  Delete: 3
 )

 scope_entry = [pubsub-topic, pubsub-perm]
```

```
pubsub-perm-details = &(
Admin: 0,
GroupType: 1,
Publish:2,
Read: 3,
Delete: 4
)
```

Figure 5: Pub/Sub scope using the AIF format

To Do

Planned for Cut Off

- Clarify KDC discovery
- Finalise Scope
  - Needs to be expanded to flag KDC vs Broker in Authorisation Request
- Join Response to include the signature algorithm and related parameters used in the group
  - 'cred_fmt', 'sign_alg', 'sign_alg_capab' and 'sign_key_type_capab' parameters
  - 'gkty' -> "Group_PubSub_Keying_Material“ as the Join Response includes more than COSE key
- Replay protection for subscribers

Planned for Later

- Expand on Group Key Management/ Group Rekeying (default point-to-point)
  - KDC publishing new key to a group rekeying topic
- Currently not hosting policies-related resources at KDC? Include?
- Finalise Groupcomm Requirements List