CoAP PubSub profile

draft-palombini-ace-coap-pubsub-profile-02

Francesca Palombini, Ericsson

IETF 101, ACE WG, London, Mar 19, 2018
CoAP PubSub

Figure 1: CoAP pubsub Architecture
Architecture CoAP PubSub with Authorization Servers

What endpoints are allowed to publish to topic A on Broker B

What endpoints are allowed to access topic A

---

Security Association 1

Security Association 2

---

- **Pre-existing Security Association**
- **Authorization Server 1**
- **Authorization Server 2**
- **CoAP Client**
- **CoAP Server**
- **Publisher**
- **Broker**
- **Subscriber**

---

What endpoints are allowed to publish to topic A on Broker B

What endpoints are allowed to access topic A

---

Security Association 1

Security Association 2
Overview (compared to draft-palombini-ace-key-groupcomm)

AS1

Client

Publisher/Subscriber

AS

AS2

Key Distribution Center

Group Members

AS

Dispatcher

Broker
Publisher 1/2: establish a secure channel with the Broker

AS1

AS

Client

Publisher

AS2

AS

Key Distribution Center

Group Members

Broker
Publisher 2/2: retrieve group keying material

AS1

AS

Client

Publisher

Authorization Request + Key Distribution Request

AS2

Key Distribution Center

AS

Dispatcher

Broker

Authorization Response + Key Distribution Response

Group Members
Subscriber: retrieve group keying material

AS1

Authorization Request + Key Distribution Request

Client

Subscriber

AS2

Authorization Response + Key Distribution Response

AS

Key Distribution Center

AS1

Dispatcher

AS2

Group Members

Broker
Phase 3: Protected Group Communication

AS1

AS

AS2

AS

Key Distribution Center

Client

Publisher

Dispatcher

Broker

Group Members

Subscribers
Matching to key-provisioning-groupcomm

**Authorization Request**
› grant_type

**Key Distribution Request**
› 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

*: depending on the role (pub/sub)

**Authorization Response**
› profile
› scope ← if different from Authorization Request

**Key Distribution Response**
› Key (COSE_Key)
   › kty
   › k
   › alg
   › kid
   › base iv
› pub_keys * ← list of pub keys of members
Thank you!

Comments/questions?

https://ericssonresearch.github.io/coap-pubsub-profile