CoAP PubSub profile

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

Francesca Palombini, Ericsson

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

CoAP PubSub

› draft-ietf-core-coap-pubsub

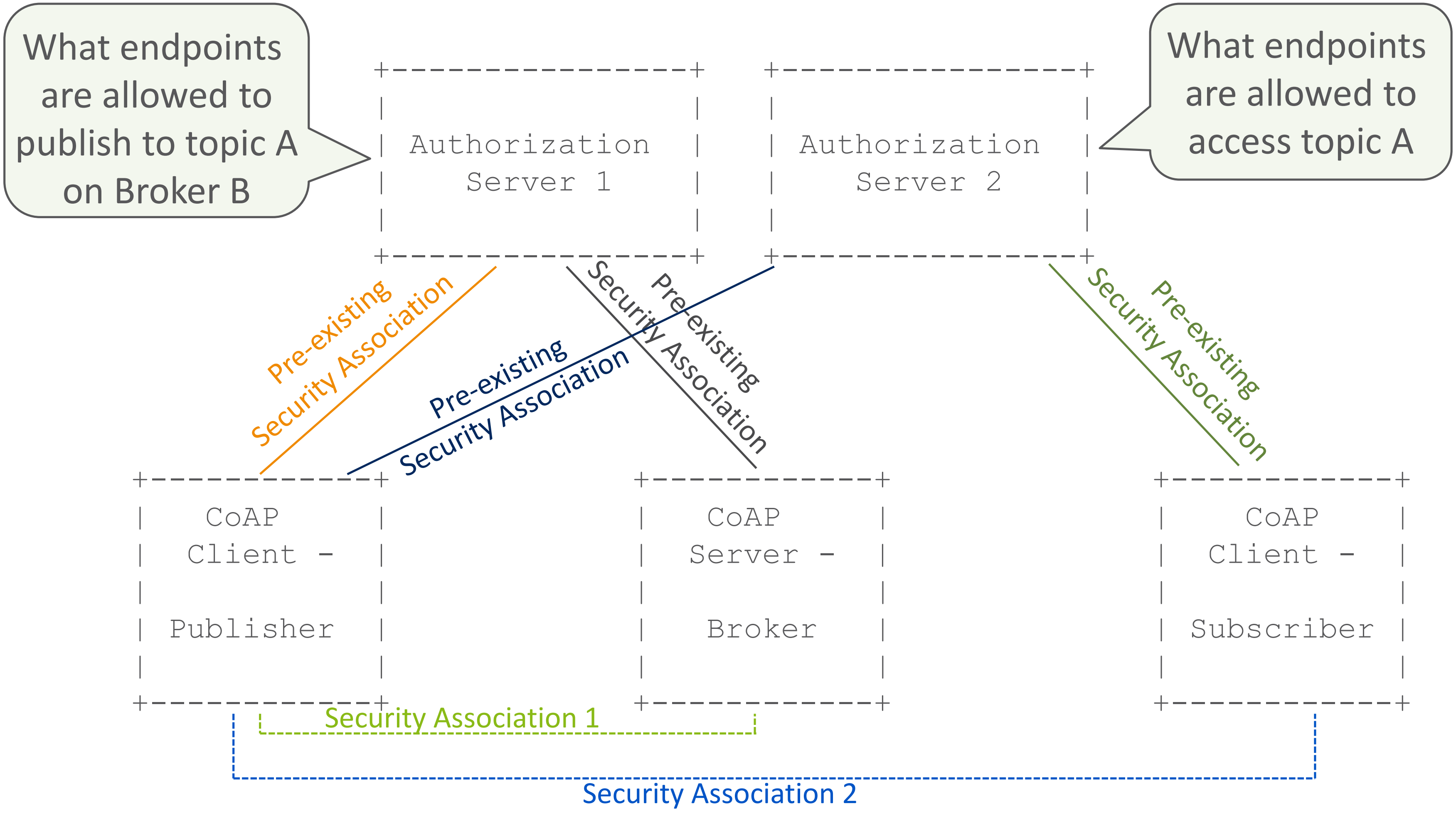
```
 Clients        pubsub         Broker
+-------+         |
| CoAP  |         |
|pubsub |---------|------+
|Client |         |      |    +-------+
+-------+         |      +----| CoAP  |
                  |           |pubsub |
+-------+         |      +----|Broker |
| CoAP  |         |      |    +-------+
|pubsub |---------|------+
|Client |         |
+-------+         |
```

Figure 1: CoAP pubsub Architecture

Architecture CoAP PubSub with Authorization Servers

IETF98

› draft-palombini-ace-coap-pubsub



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

What endpoints are allowed to access topic A

Authorization Server 1

Authorization Server 2

Pre-existing Security Association

Pre-existing Security Association

Pre-existing Security Association

Pre-existing Security Association

CoAP Client - Publisher

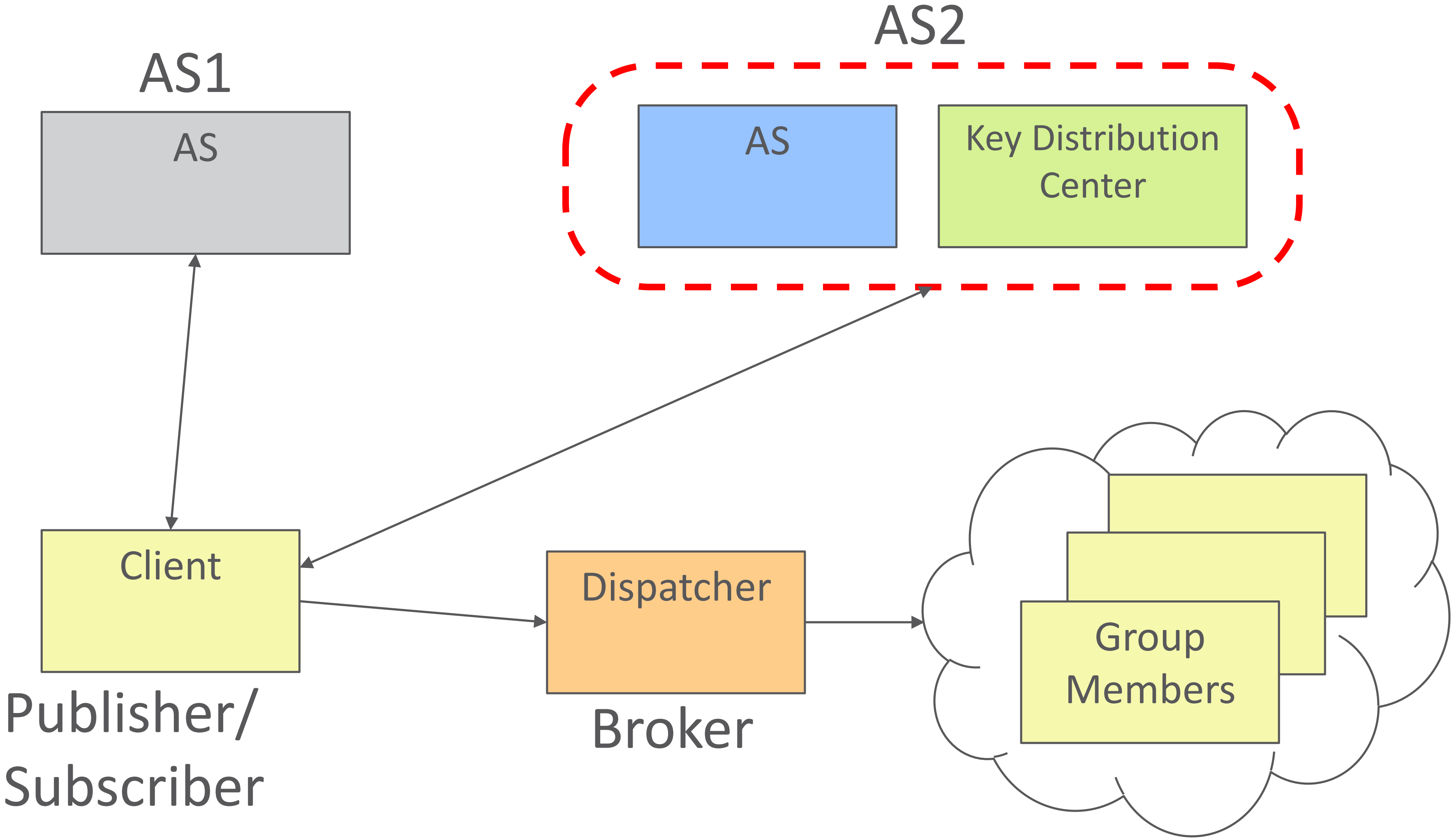
CoAP Server - Broker

CoAP Client - Subscriber

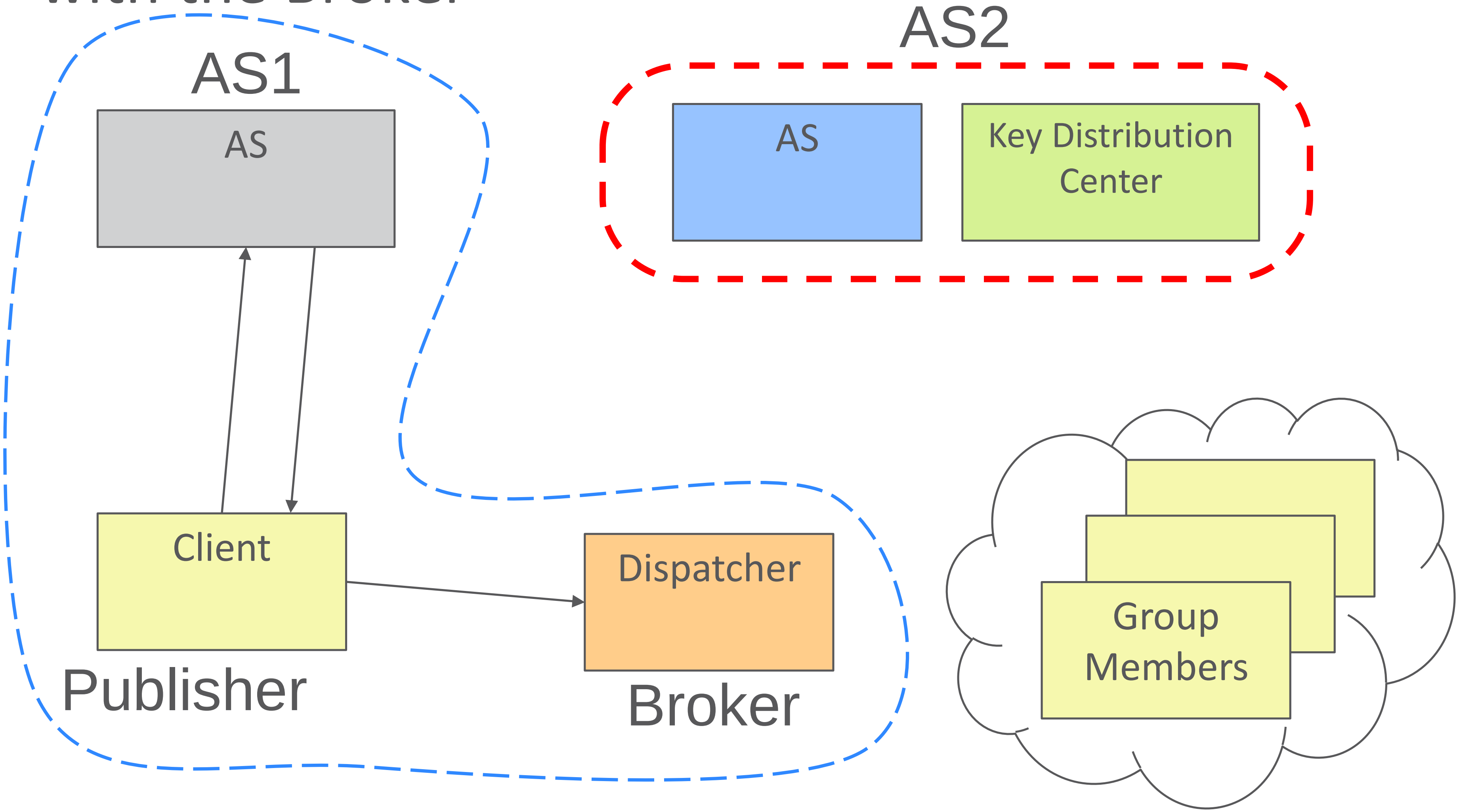
Security Association 1

Security Association 2

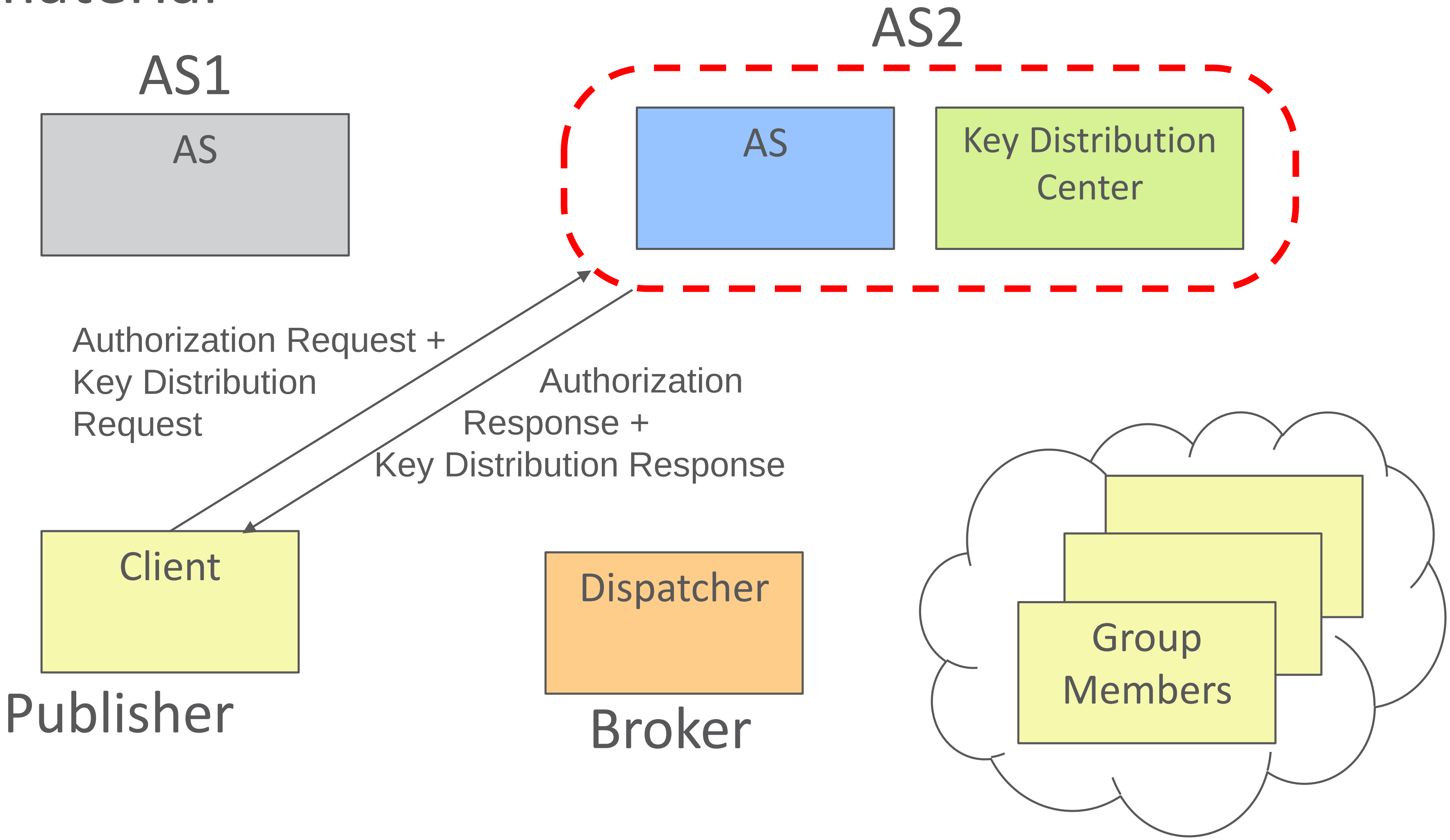
Overview (compared to draft-palombini-ace-key-groupcomm)



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

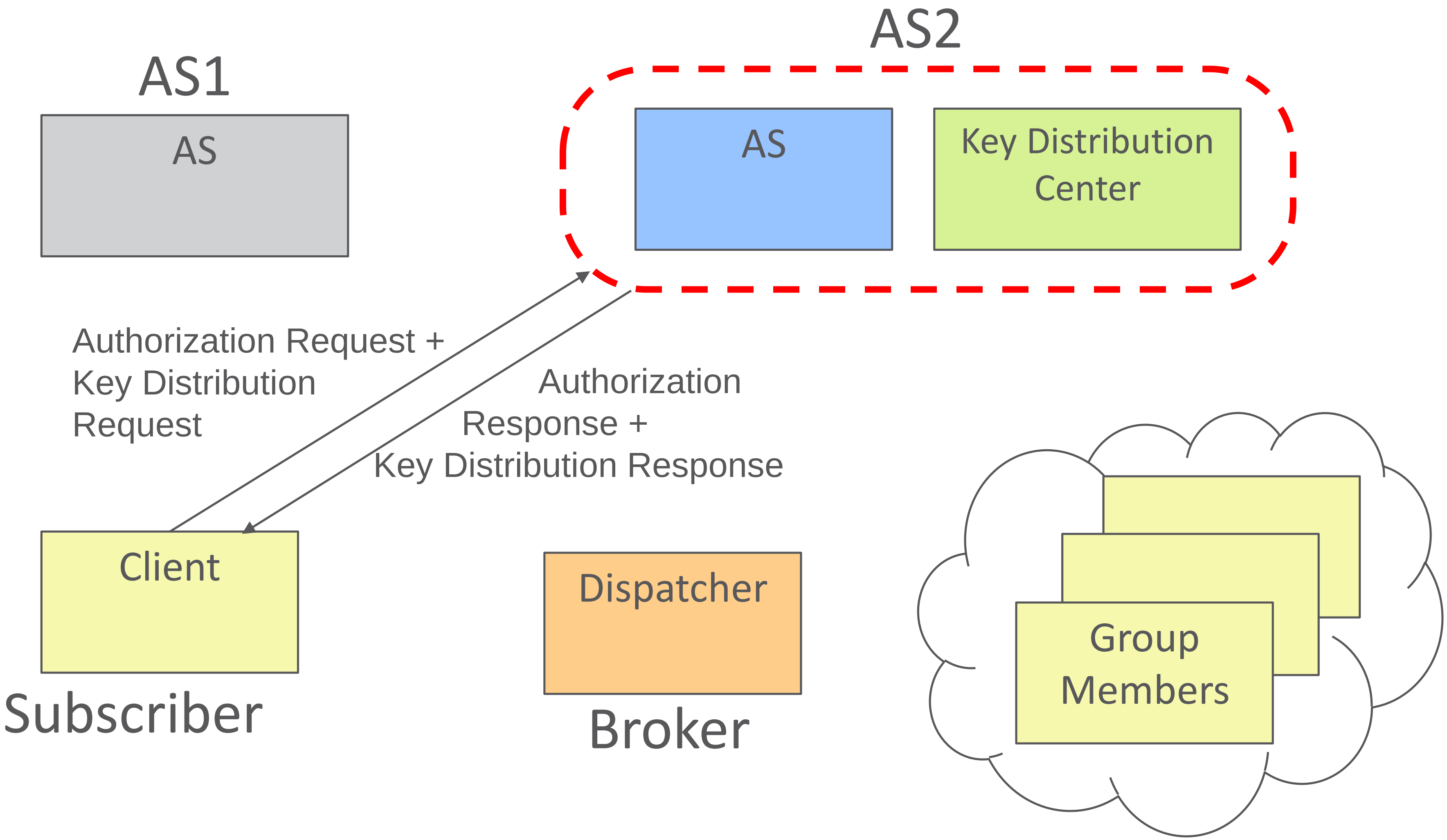


Publisher 2/2: retrieve group keying material

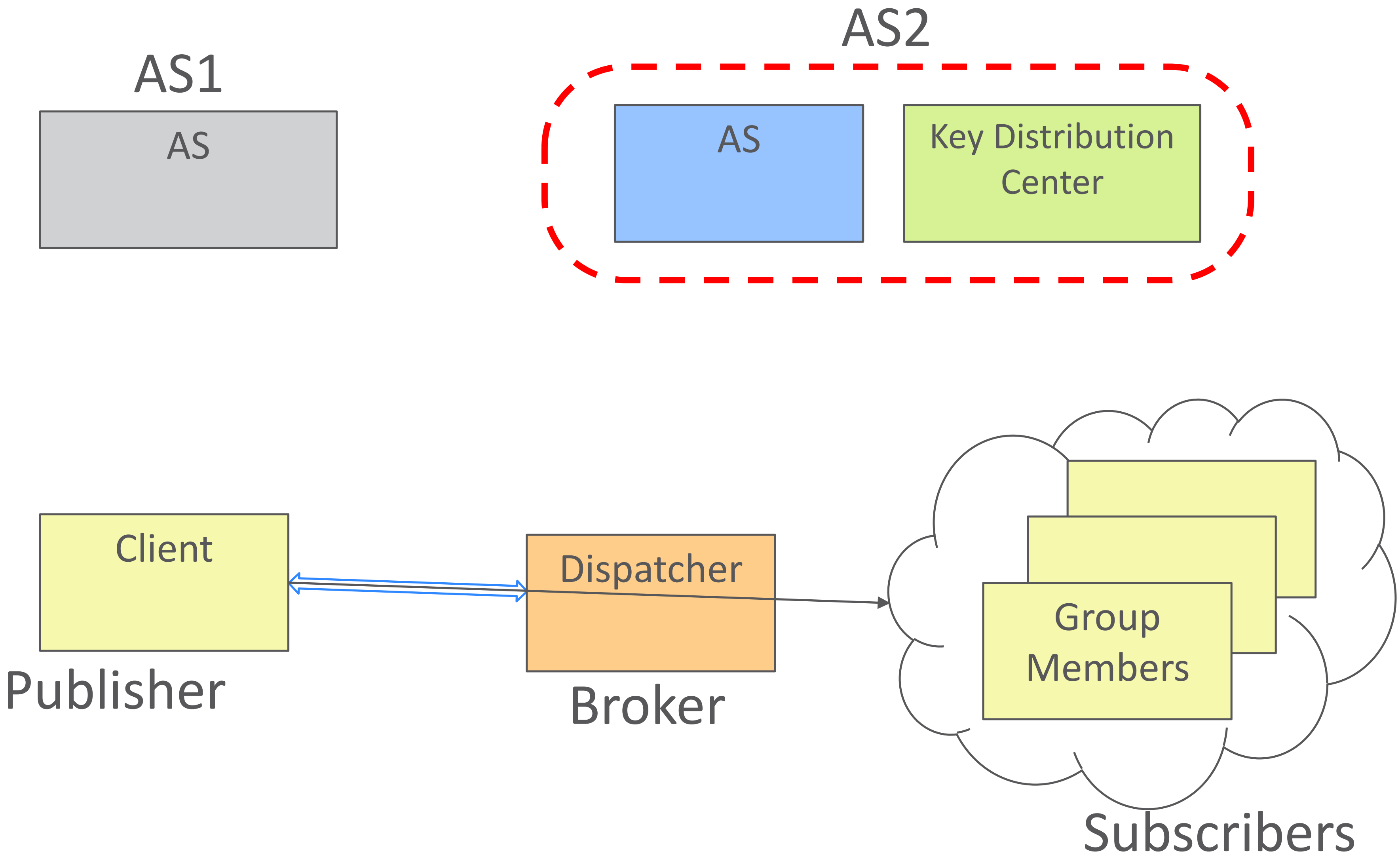


AS2
AS1
AS
AS
Key Distribution Center
Authorization Request + Key Distribution Request
Authorization Response + Key Distribution Response
Client
Publisher
Dispatcher
Broker
Group Members

Subscriber: retrieve group keying material


AS2
AS1
AS
AS
Key Distribution Center
Authorization Request + Key Distribution Request
Authorization Response + Key Distribution Response
Client
Subscriber
Dispatcher
Broker
Group Members

Phase 3: Protected Group Communication



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