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

draft-palombini-ace-coap-pubsub-profile-05

Francesca Palombini, Ericsson

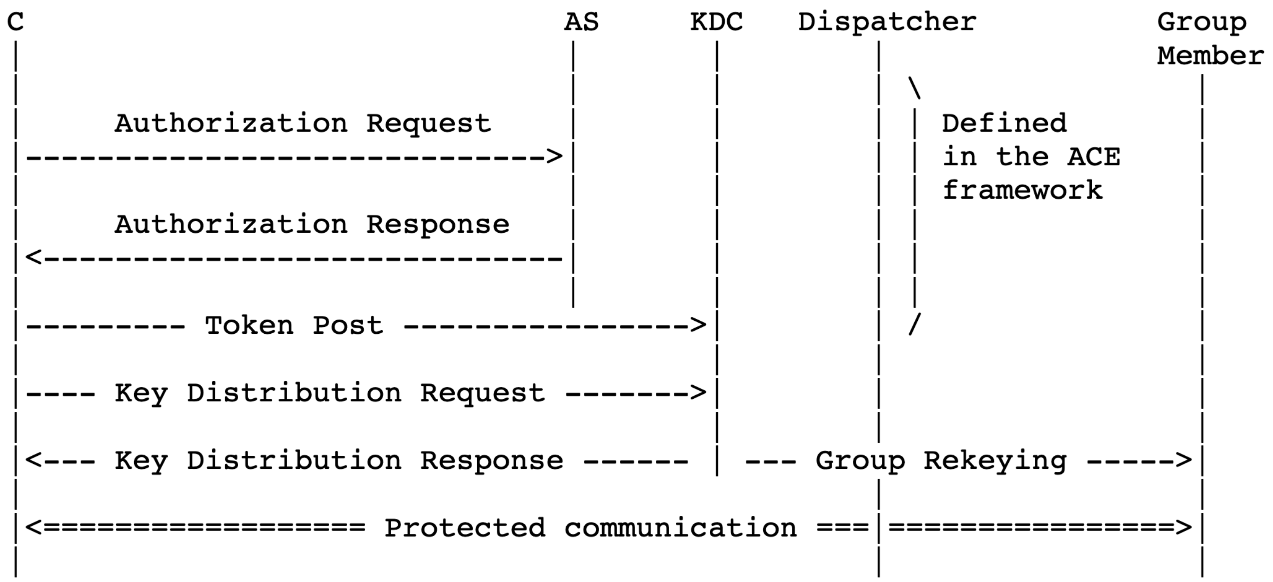
IETF 105, ACE WG, Montreal, July 25th, 2019

How is this different from ace-key-groupcomm?

- **Ace-key-groupcomm**: defines general message format for authorizing and providing keys to group members in the context of group communication

- **Ace-coap-pubsub-profile**: defines specific content of ace-key-groupcomm to profile it to using CoAP pubsub and COSE

- **Ace-key-groupcomm-oscore**: defines specific content of ace-key-groupcomm to profile it to using RFC7390 (CoAP group communication) and OSCORE groupcomm



```
C                              AS     KDC   Dispatcher          Group
|                              |       |        |               Member
|                              |       |        | \               |
|     Authorization Request    |       |        | | Defined       |
|----------------------------->|       |        | | in the ACE    |
|                              |       |        | | framework     |
|     Authorization Response   |       |        | |               |
|<-----------------------------|       |        | |               |
|                              |       |        | |               |
|--------- Token Post ---------------->|        | /               |
|                                      |        |                 |
|---- Key Distribution Request ------->|        |                 |
|                                      |        |                 |
|<--- Key Distribution Response ------ | --- Group Rekeying ----->|
|                                               |                 |
|<================== Protected communication ===|================>|
|                                               |                 |
```

Figure 2: Message Flow Upon New Node's Joining

Ace-key-groupcomm message flow

Quick Recap / Status Update

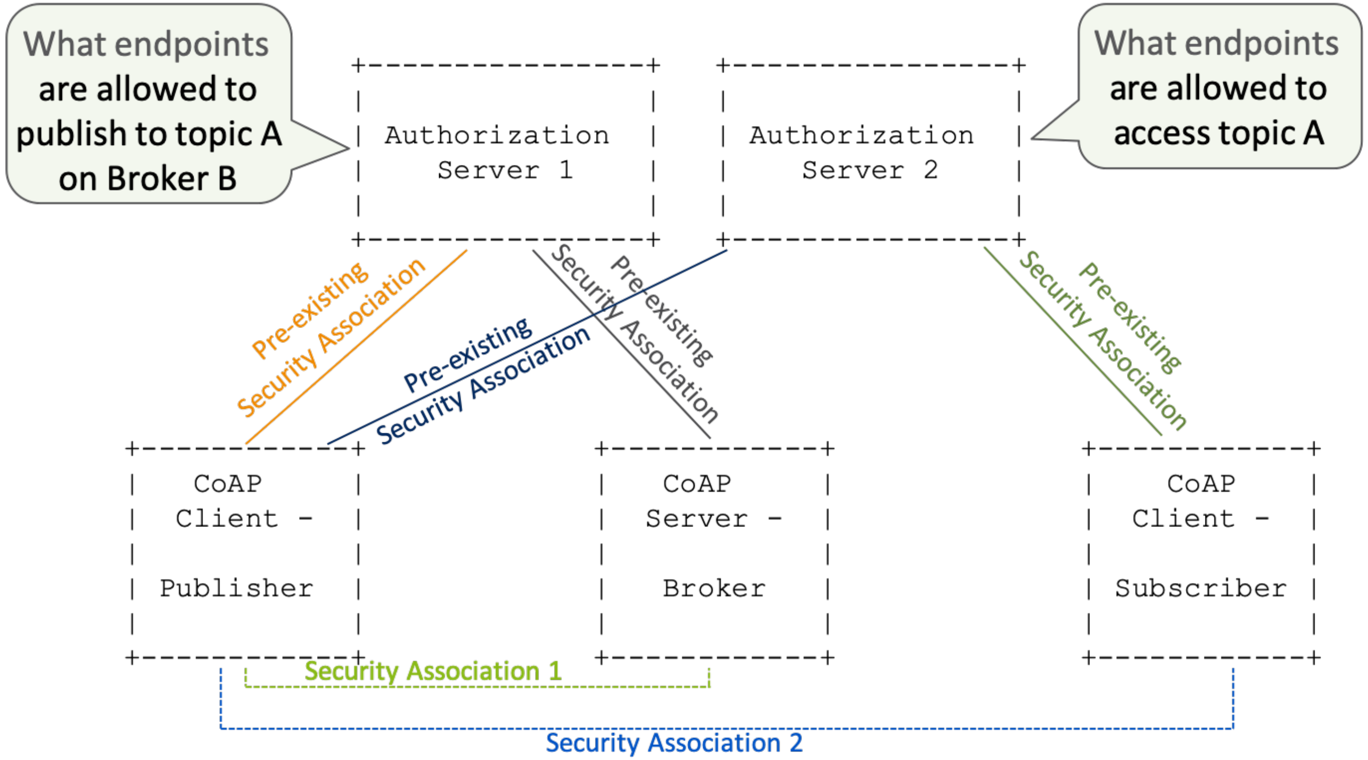
Defines how to:

- use ACE to authorize nodes and provision keys for CoAP pubsub
- protect CoAP pubsub communication using those keys

- Submitted at IETF98
- Got several reviews and positive feedback
- Updated following ace-key-groupcomm updates

Related work:

- Draft-ietf-core-coap-pubsub is closer to being done
- MQTT pubsub profile of Ace has been adopted



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

Authorization Server 1

Authorization Server 2

What endpoints are allowed to access topic A

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

Planned update – Feedback from WG?

- Split Authorization and Key Distribution Request (more similar to ace-key-groupcomm-oscore)
- Re-use OSCORE mechanisms to do key derivation, nonce derivation, replay protection
- Define the additional processing steps: encrypt/decrypt and verify the publication content with the material derived above
- Updates to comply with updates to ace-key-groupcomm

Next steps – Open questions

- Update
- Adoption?
- Sync with MQTT pubsub