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

draft-ietf-ace-pubsub-profile-03

Francesca Palombini

Cigdem Sengul

IETF 111

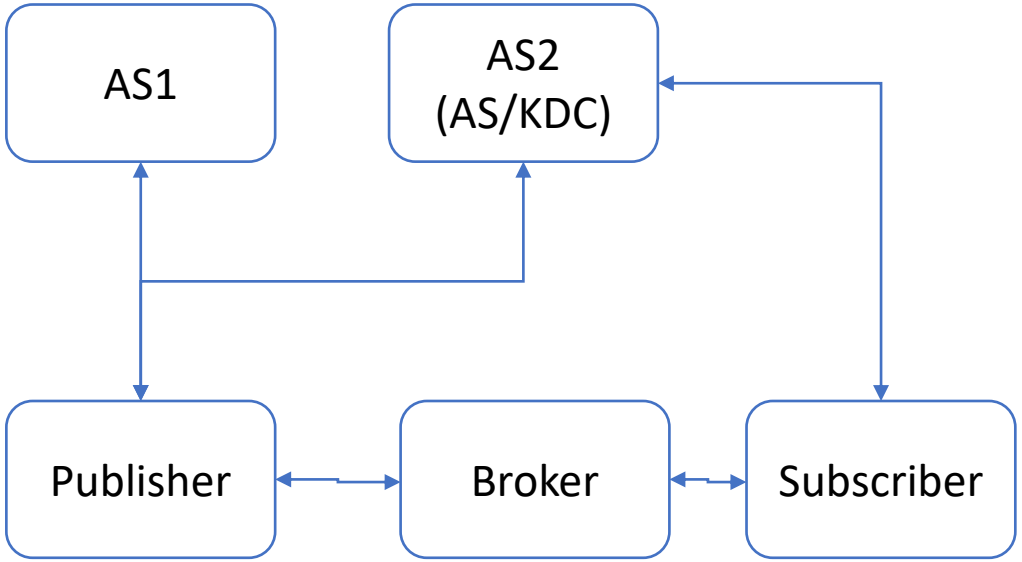
July 2021

Updates to the document

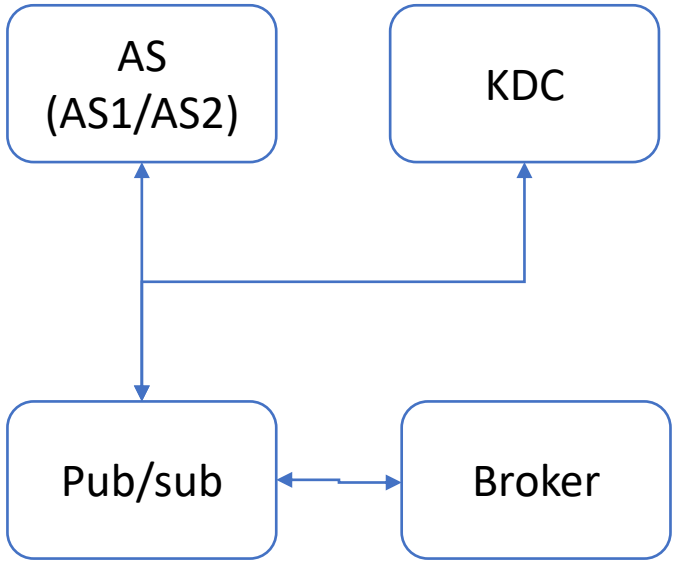
- The document defines a way to authorize pub-sub clients using the ACE framework
  - Previously covered CoAP, **added MQTT**
- Changes the architecture to the one proposed in IETF 110

Architecture Change

Former Architecture



New Architecture



- **Single AS:** AS can be flexible, two separate ASes or single AS (policy synchronisation is not a must, it's a choice).
- **Authorisation request**
  - **Single token, two audiences (KDC and Broker)**
    - To establish a secure connection between a Client and Broker, using an ACE transport profile
    - Retrieval of keying material from KDC
  - **Scope** matched to groupcomm CDLL definition of scope
- **Subscriber-authorisation supported by default**

CoAP Protocol Flow

Also very similar for MQTT

(A) Authorisation Request/Response (Clients, AS)

(B) Establish secure connection; Join Request (Clients, KDC)

(C) Establish secure connection (Clients, Broker)

(D/E/F) Pub/sub operations but with protected payloads

Change to CoAP flow: No joint authorisation + join request to AS2 (AS/KDC)

MQTT Flow

MQTT-specific consideration:

- topic names (i.e., [application] group names) may include wildcards spanning several levels of the topic tree.
- group communication in [I-D.ietf-ace-key-groupcomm] defined for security groups.
- To be able join the right security group associated with requested topics (application groups), the client needs **to discover the (application group, security group) association**.
- In MQTT, **$SYS/** has been widely adopted as a prefix to topics that contain broker-specific information

MQTT Flow

- Client-Broker: learn the (application group, security group) associations from the $SYS topic (RECOMMENDED to be a protected topic).
- Client-AS: Token request with scope covering each security group.
- Client securely connects to KDC,and sends separate join request to KDC to gets the keys for each security group.
- PUBLISH
  - protected with the corresponding key.
  - RS validates topic's security group association and stored token.
- SUBSCRIBE
  - May have one or multiple topic filters.
  - A topic filter may correspond MUST belong to a single security group.
  - If not, these topics SHOULD be separated so that they do.

Next steps

- WG Last call?
- Looking for implementers