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

draft-ietf-ace-pubsub-profile-05

Francesca Palombini

Cigdem Sengul

New author: Marco Tiloca

ACE Interim

20/02/2023

Updates to the document

- Clarified terminology
  - Security group vs application group
  - Application group corresponds to a single topic (which may have sub-topics)
  - One-to-one relationship vs One-to-many relationship
    - One application group has one security group; topic name = security group name
    - One application group has use by multiple security groups
- CoAP Pub/Sub Resource Discovery - The Resource Type (rt=) Link Target Attribute value "core.ps.gm" is registered (REQ10), and can be used to describe group-membership resources and its sub-resources at Broker, e.g., by using a link-format document (REQ 10)
- Added support for “extended format of scope”, and registered content format
- Clarified how KDC acquires authentication credentials for Publisher clients (differentiated new clients vs returning clients) (REQ 8)
- Clarified Join Error Handling
- Described support for token transfer methods other than POST authz-info in the DTLS profile ; registered EXPORTER-ACE-Sign-Challenge-coap-group-pubsub-app

To Do – Planned for Cut Off

- Clarify Client workflow and describe KDC discovery
- AIF-PUBSUB-GROUPCOMM Scope format
  - Needs to be expanded to flag KDC vs Broker in Authorisation Request
  - Other CoAP PubSub operations: DISCOVERY (default?); CREATE; READ; REMOVE
  - Future-proof Reserved for Admin
- Cose_key returned in Join Response (Register Key Type) and AEAD nonce construction
  - Option 1: Base IV and Sender ID provided by KDC; Partial IV same for all senders
  - Option 2: Base IV provided by KDC; Partial IV space divided among senders
- 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?
- Further align with CoAP Core Pub/Sub
  - Brokerless pub/sub?
- Finalise Groupcomm Requirements List