Publish-Subscribe Profile for Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-pubsub-profile-09

Francesca Palombini, Ericsson
Cigdem Sengul, Brunel University
Marco Tiloca, RISE

IETF 119 Meeting – Brisbane – March 19th, 2024
Recap

› **Application profile of ACE for pub-sub group communication**
- Instance of the interfaces and message formats/exchanges in `draft-ietf-ace-key-groupcomm`
- Focus on CoAP, per `draft-ietf-core-coap-pubsub`; also possible to support MQTT

› **Authorize pub-sub clients (ACE Clients) to:**
- Publish and/or subscribe to a topic at a Broker (ACE RS)
  ‣ → Joining an application group (topic), with certain roles
- Obtain from a KDC (ACE RS) the keying material to use for a topic
  ‣ → Joining the security group associated with a topic

› **Secure communication:**
- Between client and Broker/KDC, using a transport profile of ACE (e.g., RFC9202 or RFC9203)
- Between publisher and subscribers, end-to-end protection of data, using COSE (RFC9052)
Updates in v -09 (1/2)

- **Simple updates**
  - Editorial fixes and readability improvements
  - Improved Section 1.1 “Terminology”

- **Alignment with changes made in draft-ietf-ace-key-groupcomm**
  - Now using the parameter ‘exi’ in the Join Response from the KDC
  - Used Problem Details (RFC 9290) instead of the custom format for error responses
  - Updated formulation of requirements in Appendix A

- **End-to-end data protection between publisher and subscribers**
  - Fixes in the steps for composing the COSE_Encrypt0 object

- **When using the (D)TLS profile and uploading the Access Token through the Handshake**
  - Computation of the N_S challenge defined separately for (D)TLS 1.2 and 1.3
Updates in v -09 (2/2)

▶ Format of scope using AIF
  - No substantial changes
  - Improved naming in the AIF data model

▶ More general formulation of Toid and Tperm
  - No effect on this particular profile
  - It better sets the ground for future work on permissions for an Administrator client (e.g., a la *draft-ietf-oscore-gm-admin*)

```
AIF-PUBSUB-GROUPCOMM = AIF-Generic<pubsub-group, pubsub-perm>
pubsub-group = tstr ; name of pub/sub topic or of ; the associated security group

pubsub-perm = uint .bits pubsub-perm-details

pubsub-perm-details = &(
   Admin: 0,
   AppGroup: 1
   Publish: 2,
   Read: 3,
   Delete: 4
)

scope_entry = [pubsub-group, pubsub-perm]
```

Figure 5: Pub/sub scope using the AIF format
Next steps

› Examples: avoid text strings as placeholders for to-be-registered integer abbreviations
  – Instead, use what is proposed in draft-bormann-cbor-e-ref

› Content to add or improve in the next version -10
  – Define the replay-checks at the subscribers
    › Build on the approach used by OSCORE (RFC 8613) and using a Replay Window
  – Define canonical path of topic resources at the Broker
    › More efficient workflow for a Client to retrieve topic metadata
  – Provide additional guidelines on the discovery of topic names
  – Specify default values for group policies, as per REQ20
  – Improve content and considerations on group rekeying
  – Extend the security considerations
Thank you!

Comments/questions?

https://github.com/ace-wg/pubsub-profile
Backup
Associations and workflow

Architecture Overview

Security Associations between Publisher, Broker, and Subscriber

Authorization flow