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

draft-ietf-ace-pubsub-profile-10

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

IETF 120 Meeting – Vancouver – July 22\textsuperscript{nd}, 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
Updates in v-10 (1/2)

› More details on Delete in the scope format
  – If Delete permission on an application group, then the Client does not need to join the corresponding security group.
  – If Delete permission on a security group, then the AS and the KDC ignore that scope entry.

› More details in ‘key’ in Join Response
  – Details on CBOR map that includes parameters: group_key (COSE_Key object) and group_senderID (publisher only), cred_fmt, sign_alg, sign_params

› More details on exchanges between KDC and Group members
  – Obtaining Latest Information on the Group, Group Keying Material, and Sender ID
  – Requesting a New Sender ID
  – Updating Authentication Credentials
  – Leaving a Group
Updates in v -10 (2/2)

› More details on rekeying process and messages
  – On rekeying the group the KDC MUST increment the version number of the group keying material, generate a new Group Identifier (Gid) and preserve the current value of the Sender ID of each Publisher

› Defined replay checks at the subscriber
  – Build on the approach used by OSCORE (RFC 8613)
  – Every Subscriber maintains a Replay Window for each Publisher in the same group

› Tidied up the document
  – Improved examples
  – Improved security considerations (group confidentiality, source authentication, asymmetric crypto, Broker trust, token revocation)
  – Revised IANA considerations
  – Aligned profile requirements with draft-ietf-ace-key-groupcomm.
Next steps

 › Content to add or improve in the next version -11
   – 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
Thank you!

Comments/questions?

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

Architecture Overview

Security Associations between Publisher, Broker, and Subscriber

Authorization flow