Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-04

Francesca Palombini, Ericsson
Marco Tiloca, RISE

Interim, ACE WG, Jan 31, 2020

Planned update v-04: RESTification cont

DONE

Endpoint	Supports	Meaning/How to use
ace-group	-	This specification is used
ace-group/**gid**	GET; POST	GET group keying material. POST public key of joining node + return group keying material and all public keys
ace-group/gid/pub-key	GET; ~~POST~~FETCH	GET all public keys of nodes in the group ~~POST~~FETCH request pub keys for specific nodes
ace-group/gid/policies	GET	GET group policies (app profile dependent)
ace-group/gid/ctx-num	GET	GET version of group keying material (+1 on rekeying)
ace-group/gid/**node**	GET; PUT; DELETE	~~GET~~ PUT to get the KDC to produce and return individual keying material to protect outgoing msg ~~POST 'scope'~~ DELETE to leave the group GET group keying material + individual keying material

1 resource per member of the group

gid is the group ~~identifier~~ name

node is the node name (different from node identifier, which is sent on the wire, part of key derivation, and can be updated)

Operations - planned update

DONE

- Joining: POST /ace-group/gid – Response would return location path ”node”
- Retrieval of Updated Keying Material: GET /ace-group/gid
- Retrieval of Public Keys: ~~POST~~ FETCH/GET /ace-group/gid/pub-key
- Retrieval of Group Policies: GET /ace-group/gid/policies
- Retrieval of Keying Material Version: GET /ace-group/gid/ctx-num
- Retrieval of New Individual Keying Material: ~~GET~~ PUT /ace-group/gid/node
- Retrieval of Updated Group+Individual Keying Material: GET /ace-group/gid/node
- Group Leaving Request: ~~POST~~ DELETE /ace-group/gid/node

Planned update v-04: Others (Jim's review)

DONE

- If Client contacts KDC endpoints not on secure channel, it gets an **Error 4.01 Unauthorized**. Creation Hints (Response to Token POST) in the error's payload.
- Because of the change to the resource "node", all nodes need a "node name", even if they don't use this name because they never send messages (e.g. monitor-only members).
- Upon joining, send the "URI of certificate", instead of the "URI of key repository" (POST to /ace-group/gid , 'pub_keys_repos' parameter, if 'client_cred' includes a certificate).
- Using POST to retrieve public keys of nodes seems like the wrong method. Jim suggested FETCH, but that is optional. Is PUT better? → We used FETCH.
- Other minor comments

- Revised and extended the list of profile requirements
- Content as general or of high-level applicability moved here from *ace-key-groupcomm-oscore*

TODO left

- Open points (following slide)
- Finish including Peter's review (editorials and clarifications)
  https://mailarchive.ietf.org/arch/msg/ace/_PDsf5rnGtVw6y3nSQTJun0t7P4

Open Points

1. In this document, we define a new content type and media type, ace-groupcomm+cbor .
   - In the exchanges with the KDC, we want to use parameters originally defined under ace+cbor .
   - We think we need to re-register these parameters in our “ACE Groupcomm Parameters” registry.
   - Otherwise, just including them in the message would produce collisions between ace and ace-groupcomm parameters. Correct?

2. We think the Token and Join request should possibly cover more than one group/topic at once.
   - Many parameters would become arrays of the current ones.
   - Public key provided in the join request: if it's only one despite more topics/groups covered, the client intends using the same one in all of them.

   Issues with that?

3. We want to define a new optional parameter in the joining response, that includes a multicast address and URI path, where the KDC sends rekeying messages of advanced rekeying protocols.
   Issues with that?

4. We want to define an optional parameter in the joining request, including the URI to a resource where the client is fine to receive unicast rekeying messages from the KDC. Issues with that?