Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-03

Francesca Palombini, Ericsson
Marco Tiloca, RISE

IETF 106, ACE WG, Singapore, Nov 19, 2019
Quick Recap

Figure 2: Message Flow Upon New Node's Joining
Update following reviews of v-02

- Ludwig and Daniel’s reviews were addressed and answered in the mailing list
- Mostly agreed and update accordingly, please get back if not satisfied with our answers
- Discussion at IETF105 + offline chat: RESTification (v-03)
- Major improvement on Appendix A: Requirements of application profiles
- New review of v-03 by Jim, update planned
### Major update v-03: RESTification

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Supports</th>
<th>Meaning/How to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ace-group</td>
<td>-</td>
<td>This specification is used</td>
</tr>
<tr>
<td>ace-group/\texttt{gid}</td>
<td>GET; POST</td>
<td>GET group keying material. POST public key of joining node + return group keying material and all public keys</td>
</tr>
<tr>
<td>ace-group/\texttt{gid/pub-key}</td>
<td>GET; POST</td>
<td>GET all public keys of nodes in the group POST request pub keys for specific nodes</td>
</tr>
<tr>
<td>ace-group/\texttt{gid/policies}</td>
<td>GET</td>
<td>GET group policies (app profile dependent)</td>
</tr>
<tr>
<td>ace-group/\texttt{gid/ctx-num}</td>
<td>GET</td>
<td>GET version of group keying material (+1 on rekeying)</td>
</tr>
<tr>
<td>ace-group/\texttt{gid/node}</td>
<td>GET; POST</td>
<td>GET individual keying material to protect outgoing msg POST ‘scope’ to request to leave the group</td>
</tr>
</tbody>
</table>

\texttt{gid} is the group identifier
Operations are defined by specifying what endpoint to contact...

- Joining: POST ace-group/gid
- Retrieval of Updated Keying: GET ace-group/gid
- Retrieval of New Keying: GET ace-group/gid/node
- Retrieval of Public Keys for Group: POST/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
- Group Leaving Request: POST /ace-group/gid/node
## Planned update v-04: RESTification cont.

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

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

- Joining: POST ace-group/gid – Response would return location path "node"
- Retrieval of Updated Keying: GET ace-group/gid
- Retrieval of New Keying: GET PUT ace-group/gid/node
- Retrieval of Public Keys for Group: POST/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
- Group Leaving Request: POST DELETE /ace-group/gid/node
Planned update v-04: Others (Jim’s review)

• If Client contacts KDC endpoints not on secure channel, it gets an **Error 4.01 Unauthorized**. Include AS 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 (monitor only).

• Instead of sending the "URI of key repository", send the "URI of certificate" (in POST to /ace-group/ gid).

• Using POST to retrieve public keys of nodes seems like the wrong method. Jim suggested FETCH, but that is optional. Is PUT better?

• Other minor comments