Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-01

Francesca Palombini, Ericsson
Marco Tiloca, RISE
### Figure 2: Message Flow Upon New Node's Joining

<table>
<thead>
<tr>
<th>C</th>
<th>AS</th>
<th>KDC</th>
<th>Dispatcher</th>
<th>Group Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Request</td>
<td></td>
<td></td>
<td>\ Defined in the ACE framework</td>
<td></td>
</tr>
<tr>
<td>Authorization Response</td>
<td></td>
<td></td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>Token Post</td>
<td></td>
<td></td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>Key Distribution Request</td>
<td></td>
<td></td>
<td></td>
<td>--- Group Rekeying</td>
</tr>
<tr>
<td>Key Distribution Response</td>
<td></td>
<td></td>
<td></td>
<td>--- Group Rekeying</td>
</tr>
<tr>
<td>Protected communication</td>
<td></td>
<td></td>
<td></td>
<td>--- Group Rekeying</td>
</tr>
</tbody>
</table>

29/03/2019 | Ace WG | IETF 104 | Prague | 2
New: IANA

• Key Distribution Response contains a **general** “key” field
  • its type is defined by the new “kty” field, to be registered in a new “Ace Groupcomm Key” registry:

```
+-----------------+-----------------+-----------------+------------------+
| Name             | Key Type Value  | Profile         | Description      |
+-----------------+-----------------+-----------------+------------------+
| Reserved         | 0               |                 | This value is reserved |
+-----------------+-----------------+-----------------+------------------+
```

• Key Distribution Response contains a new “profile”
  • to be registered in a new “Ace Groupcomm Profile” registry (NOT the same profile as Ace!)

• Key Distribution Response contains a new “exp” field (expiration of the keying material)

• Feedback about general key field? IANA OK?
New: Errors Definition

• KDC error on Requests:

  • If verification fails, the KDC MUST respond with a 4.01 (Unauthorized) error message.

  • If the Request is not formatted correctly (e.g. no 'scope' field present while expected, or unknown fields present), the KDC MUST respond with 4.00 (Bad Request) error message.

• Feedback?
New: Request To Leave the Group

• CoAP POST to /resource associated with group at KDC
  Payload: { ‘leave’:[], ‘scope’: [“group1”], ‘client_cred’: pubkey_id1}

• Leave the group altogether, not role based

• A client can re-request to join a group without contacting AS as long as token is valid

• Feedback?
TODO: Add Finer Granularity to Scope

- Right now, for example:
  
  `'scope' = [ "group1" , "requester" ]`
  
  `'scope' = [ "topic1" , "POST, GET" ]`

- Do we want to add finer granularity on operations and resources?
  
  `'scope' = [ "group1" , [["PUT", "Res1"], ["POST, GET", "Res2"]]]`

- If yes, do we do it here?
Key Redistribution Initiated by KDC (examples)

KDC can distribute keying material by:

1. Using unicast requests to each Client over a secure channel
2. Using Observe (members = observers)
3. Using Pub/Sub (KDC = publisher, members = subscribers)
4. Using Multicast (KDC = multicaster)

“different security properties and require different security associations.”

• We describe 1 in detail. Do we need to expand on the others?