Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-key-groupcomm-oscore-09

Marco Tiloca, RISE
Jiye Park, Universität Duisburg-Essen
Francesca Palombini, Ericsson

IETF 109, ACE WG, November 18th, 2020
Recap

› Message content and exchanges for:
  – Provisioning keying material to joining nodes and groups (rekeying)
  – Joining an OSCORE group through its Group Manager (GM)
  – More operations for current members at the GM

› Builds on *draft-ietf-ace-key-groupcomm*
  – Agnostic of the ACE transport profile used by C and GM

› Out of Scope:
  – Authorizing access to resources at group members
    › *draft-tiloca-ace-group-oscore-profile*
  – Actual secure communication in the OSCORE group
    › *draft-ietf-core-oscore-groupcomm*
Major updates in v -09

› Same path segment from *ace-key-groupcomm*
  – group-oscore/... → ace-group/...

› Summary of admitted REST methods
  – At each sub-resource
  – For each role
  – Member vs. non-member

› FETCH to ace-group/
  – Req: GID → Group name
  – Now also for Verifiers

› Note: AIF is used since -08
  – scope: << [* [Toid, Tperm]] >>

<table>
<thead>
<tr>
<th>Resource</th>
<th>Type1</th>
<th>Type2</th>
<th>Type3</th>
<th>Type4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ace-group/</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/</td>
<td></td>
<td></td>
<td>Po</td>
<td>Po</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/active</td>
<td>G</td>
<td>G</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/pub-key</td>
<td>G F</td>
<td>G F</td>
<td>G F</td>
<td>-</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/policies</td>
<td>G</td>
<td>G</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/num</td>
<td>G</td>
<td>G</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ace-group/GROUPNAME/nodes/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NODENAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ace-group/GROUPNAME/nodes/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NODENAME/pub-key</td>
<td>Po</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Type1 = Member as Requester and/or Responder
Type2 = Member as Monitor
Type3 = Non-member / Authorized to be Verifier
   (* ) = cannot join the group as Verifier
Type4 = Non-member / Not authorized to be Verifier

G = GET
F = FETCH
Po = POST
Pu = PUT
D = DELETE
Major updates in v-09

› Updates to the ‘key’ parameter in the Joining Response

› ‘clientId’ → ‘group_SenderId’
  – Same meaning, i.e. the assigned Sender ID in the joined group
  – Also registered in the OSCORE Security Context Parameters registry

› Added parameters for the pairwise mode of Group OSCORE
  – ‘ecdh_alg’, ‘ecdh_parameters’, ‘ecdh_key_parameters’
  – MUST be present if the pairwise mode is supported, MUST NOT otherwise
  – Also registered in the OSCORE Security Context Parameters registry
  – Default values are defined, as for other analogous parameters

› Removed explicit group policy on supported pairwise mode
Major updates in v -09

› Clarifications on possible group rekeying
  – “together” or “instead of” assigning a new Sender ID to a group member

› Consistency with requirements from Group OSCORE
  – Never re-assign a Sender ID in the same OSCORE group
  – Never re-assign the same Group ID to the same OSCORE group

› Resource type rt=core.osc.gm
  – Registration moved here from draft-tiloca-core-oscore-discovery
Next steps

› One more update expected
  – Alignment to next updates in *ace-key-groupcomm*

› Complete implementation, run more tests

› Then ready for WGLC (?)
Thank you!

Comments/questions?

https://github.com/ace-wg/ace-key-groupcomm-oscore