Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-key-groupcomm-oscore-07

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

IETF ACE WG, Virtual Interim, June 22nd, 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 draf-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
Since virtual meeting 15-04-2020

› Two versions submitted
   – v-06 : addressed Jim’s review of -05 (thanks!)
   – v-07 : aligned with ace-key-groupcomm, comments from Peter (thanks!)

› Registered a new group policy
   – Signal whether the pairwise mode of Group OSCORE is used in the group

› Removed role combination [“Requester”, “Monitor”]
   – … and a new open point came up (see later slide)

› Added new role “Verifier”
   – Not a group member, but authorized to retrieve public keys from the GM
   – Can verify countersignatures of Group OSCORE messages in the group
Since virtual meeting 15-04-2020

› Reverted to ‘kdcchallenge’ **not** for single use
  – Valid as long as the posted Access Token is valid
  – The GM returns it in an error response to a Joining Request
    › If the old one has been deleted, a new one is provided and stored
  – Security considerations updates accordingly

› ‘kdcchallenge’ **MAY** be omitted if:
  – The ‘scope’ in the Access Token has only the “monitor” role or only the “verifier” role, for each specified group.
  – The final choice is for the implementer.
Since virtual meeting 15-04-2020

› Updated format of parameters about the countersignature
  – ‘sign_info’, in the response to the Token post
  – ‘cs_params’ and ‘cs_key_params’ in the Joining Response
  – Now using the Capabilities from the COSE registries

› More considerations on a node missing a group rekeying
  – Missed rekeying → Being unable to decrypt incoming group messages
  – The node has to ask the GM for the current keying material
    › Those messages (may) include a new Gid, not sufficient as a hint
  – If the node is in multiple groups of a same GM
    › Request keying material for one group at the time
  – If multiple GMs are involved
    › Request keying material from one GM at the time
    › The Gid format Prefix+Epoch helps (Appendix of core-oscore-groupcomm)
Open point

- Legitimate role combinations
  - Removed role combination [“Requester”, “Monitor”]
  - It doesn’t make sense inside a group. But, **when** should this be checked?

- Now the AS checks that, when getting a Token Request:
  - [“Requester”, “Responder”] is valid
  - [“Requester”, “Monitor”] is not valid
  - A node wanting to join first as Requester, then as Monitor needs 2 tokens
  - Shouldn’t this be checked by the GM when getting a Joining Request?

- Distinguish ‘scope’ in Token Request and in the Joining Request
  - Token Request: any combination of any admitted role is fine
  - Joining Request: any legitimate combination of roles in the token is fine
  - **Issues with that?**
Next steps

› Submit version -08 before the cut-off
  – Close the open point on role combinations
  – Default values of ‘cs_alg’, ‘cs_params’, ‘cs_key_params’, ‘cs_key_enc’
    › Now defined in draft-tiloca-ace-oscore-gm-admin
    › Jim suggested [1] to move them to this document

› Then ready for WGLC (?)

› Advance the implementation and run interop tests

[1] https://mailarchive.ietf.org/arch/msg/ace/q55WDjJLdEMVvI0bV7k_VrzRglY/
Thank you!

Comments/questions?

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