Key Management for OSCORE Groups in ACE

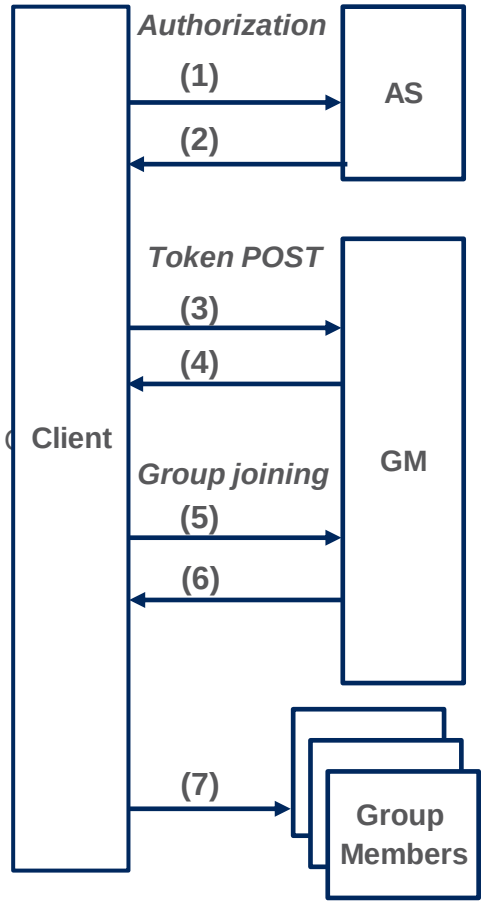
draft-ietf-ace-key-groupcomm-oscore-06

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

IETF ACE WG, Virtual Interim, May 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 *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*



Updates since last interim (1/2)

- 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

Updates since last interim (2/2)

- 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 implementor.

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

- Close open point on role combinations

- 'sign_parameters' and 'sign_key_parameters'
  - Take values from the registries in *draft-cose-rfc8152bis-algs-07*
  - Same as in next update of *draft-core-oscore-groupcomm*

- Thorough sanity check against *ace-key-groupcomm*
  - No contradictions, no repetitions/redefinitions

Thank you!

Comments/questions?

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