Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-groupcomm-oscore-05

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

IETF ACE WG, Virtual Interim, April 15th, 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
What happened since IETF 106

› Version -04 was submitted end of January
  – Closed most points from IETF 106
  – Presented at January ACE interim

› Version -05 was submitted before the cut-off
  – Based on a review and comments from Jim [1][2] – Thanks!
  – Discussion at the February ACE interim

› New review of -05 from Jim [3] – Thanks!
  – Mostly covered in the latest Editor’s version
  – Some open points left (later slides)

› [1] https://mailarchive.ietf.org/arch/msg/ace/Uz1BfltsJfbwsNKdAbn4WT_wm9I/
› [3] https://mailarchive.ietf.org/arch/msg/ace/nPnee1oxabwQoQhohqdLeTR8NIs/
Selected updates from -05

› Security considerations about N_S and N_C
  – Used to build the signature challenge, at minimum 8-byte long each
  – Section 17.2 – Security of their size, also requested by Ben at IETF 106
  – Section 17.3 – Reusage of no random nonces across reboot; no replay

› Registered dedicated TLS Exporter label
  – EXPORTER-ACE-Sign-Challenge-coap-group-oscore-app
  – Used to build the signature challenge, when nonces are not exchanged

› Multi-group scope
  – A single Access Token can cover multiple groups and the roles for them
  – Re-using format defined in draft-ace-key-groupcomm
  – Roles compressed as CBOR integers
Selected updates from -05

- Jim’s proposal of legal requester/responder
  - Node A knows the roles of node B, and can ignore abusive messages
  - Roles come beside public keys, in the `peer_roles` parameter
    - Upon joining, or later when separately requesting public keys

- Detailed operation for uploading a new public key
  - Resource and handler defined in `draft-ace-key-groupcomm`

- Defined a new resource and handler at the GM
  - Return the current status of the group, i.e. active/inactive
  - If inactive, members should not communicate, no new nodes can join
  - Specific to the OSCORE GM, so defined in this document
  - Status set by an Administrator client, see `ace-oscore-gm-admin`
In current Editor’s copy

› Clarified difference between group name and OSCORE Gid

› Removed role combination [“Requester”, “Monitor”]

› Authorization Request to the AS
  – Both scope and audience may be implicit (aligned with the framework)

› When a member asks for a new Sender ID
  – The GM may prefer to opt for a whole group rekeying instead
  – If so, no error returned to the requesting node
  – Rekey the requesting node first, then the rest of the group

› Aligned to Editor’s copy of ace-key-groupcomm
  – ‘rsnonce’ → ‘kdcnonce’
  – New structure for the ‘sign_info’ parameter (multiple groups at once)
Open points

› Group OSCORE is introducing a new pairwise mode
  – Monitor-only nodes need a public key
  – They need also a Sender ID, to enable retrieval of their public key

› Proposed update – Issues with that?
  – Also a monitor-only can provide a public key to the GM
  – If it does, the GM assigns and provides a Sender ID to that node
  – A monitor-only supporting the pairwise mode, provides its public key
  – This would update uploading/retrieval/caching of public keys

› Register a new group policy – Issues with that?
  – Signal whether the pairwise mode is admitted in the group
  – If not, possible to have less public keys in the Joining Response
Open points

› Pending updates on ‘kdcnonce’ (was ‘rsnonce’) from the GM
  – After Token posting, return also to monitor-only nodes
    › They may later send a public key (see pairwise mode of Group OSCORE)
  – It should actually be single-use
    › The value in the response from /authz-info is only to use for the immediately following first Joining Request
    › The value from an error response to a Joining Request is to use only for the following re-attempt of the first Joining Request (assuming a Token POST to /authz-info)
    › Derived challenges are used instead in any other case
  – Tentative text already in the Editor’s copy (Sections 5.2.1 and 5.3).
  – Issues with that?
Next steps

› Close open points

› Keep aligned with ace-key-groupcomm

› Update implementations and start interoping
  – RISE [1], Jim, Peter, ...

Thank you!

Comments/questions?

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