Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-08

Marco Tiloca, RISE
Rikard Höglund, RISE
Peter van der Stok
Francesca Palombini, Ericsson

ACE WG Interim Meeting, June 5th, 2023

Status update

- **Completed document split**

- **Doc 1: To be *draft-ietf-ace-oscore-gm-admin-09***
  - https://github.com/ace-wg/ace-oscore-gm-admin
  - Removed all the content related to CoRAL (*draft-ietf-core-coral*)
  - Use of the pairwise mode changed to be “true” by default
  - Clarified what group members do when learning of a group configuration change
  - Editorial improvements and fixes

- **Doc 2: To be *draft-ietf-ace-oscore-gm-admin-coral-00***
  - https://github.com/ace-wg/ace-oscore-gm-admin-coral
  - Complete and stable

What's left?

- **The Shepherd review of *draft-ietf-core-oscore-groupcomm* is under processing**
  - This stimulated two new open points for *draft-ietf-ace-oscore-gm-admin*

- **Open point #1 is on the actual protocol**
  - Valid all along; the revision of Group OSCORE just put light on it

- **Open point #2 is a consistency fix**
  - Triggered by the revision of Group OSCORE

Open point #1

- **Section 6.6.2 “Effects on Group Members”**
  - ... Following the overriding of a group configuration with a PUT request
- **The Administrator might change the encryption algorithms used in the group**
  - Result of a change to the values of “sign_enc_alg” and “alg”
  - This may change the max size of the OSCORE Sender IDs usable in the group
  - The max size of the Sender IDs depends on the size of the AEAD nonce of the two algorithms
- **Proposal: if the maximum size of the OSCORE Sender IDs changes ...**
  - Evict the group members whose Sender ID has a size larger than the new maximum size
  - Rekey the group accordingly (see *draft-ietf-ace-key-groupcomm-oscore*)
  - The same silently applies in Section 7.6.2, where the update is selective with a PATCH request
  - No changes to *draft-ietf-ace-oscore-gm-admin-coral*, since this is silently inherited

OK with this?

Open point #2

- **Use updated names, consistent with renaming in *draft-ietf-core-oscore-groupcomm***
- **Signature Encryption Algorithm → Group Encryption Algorithm**
- **sign_enc_alg → gp_enc_alg**
  - To be fixed also in *draft-ietf-ace-oscore-gm-admin-coral*
- **Add an Editor's Note**
  - The new naming is consistent with *draft-ietf-core-oscore-groupcomm-18* (upcoming)
  - Old names are still used in *draft-ietf-ace-key-groupcomm-oscore* (to be fixed later the AD review)

OK with this?

Next steps

1. **Next weeks: submit a new version of *draft-ietf-core-oscore-groupcomm***
   - This will also use the new naming
   - Remaining points to process should not have an impact on this document

2. **Submit *draft-ietf-ace-oscore-gm-admin-09* addressing the new open points**

3. **Submit *draft-ietf-ace-oscore-gm-admin-coral-00* referring *-oscore-gm-admin***

4. ***draft-ietf-ace-oscore-gm-admin-09* should be ready for WG Last Call**

Thank you!

Comments/questions?

https://github.com/ace-wg/ace-oscore-gm-admin

Backup

Recap

- **RESTful admin interface at the OSCORE Group Manager**
  - Create, (re-)configure and delete OSCORE groups
  - Support for both: i) Link Format and CBOR ; ii) CoRAL

- **Two new types of resources at the Group Manager**
  - A single *group-collection* resource, at /manage
  - One *group-configuration* resource per group, at /manage/GROUPNAME

- **Using ACE for authentication and authorization**
  - The Administrator is the Client
  - The Group Manager is the Resource Server
  - For secure communication, use transport profiles of ACE

Overview

Configuration Properties

- Security algorithms and parameters

Status Properties

- Any other information (e.g., group name)

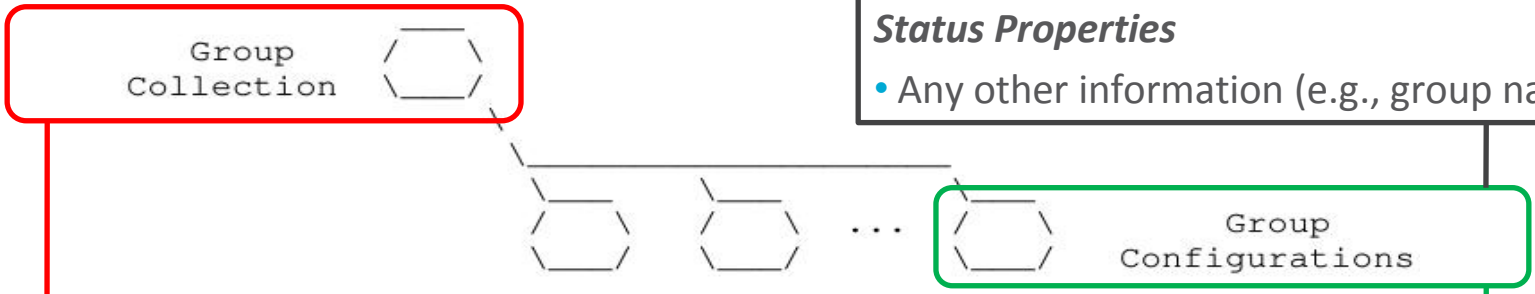

Figure 1: Resources of a Group Manager

***Group-collection* resource**

- Retrieve the list of OSCORE groups
  - All groups (GET)
  - Group selected by filters (FETCH)
- Create a new OSCORE group (POST)
  - A group-configuration resource is created
  - A group-membership for joining nodes is also created, see *draft-ietf-ace-key-groupcomm-oscore*

***Group-configuration* resource**

- Retrieve the group configuration (GET)
- Retrieve part of the group configuration (FETCH)
- Overwrite the group configuration (PUT)
- Update the group configuration (PATCH/iPATCH)
- Delete the group (DELETE)