Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-11

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

IETF 119 Meeting – Brisbane – March 19th, 2024

Recap

- **RESTful admin interface at the OSCORE Group Manager**
  - Create, (re-)configure, and delete OSCORE groups
- **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 ACE Client
  - The Group Manager is the ACE Resource Server
  - For secure communication, use transport profiles of ACE

Overview

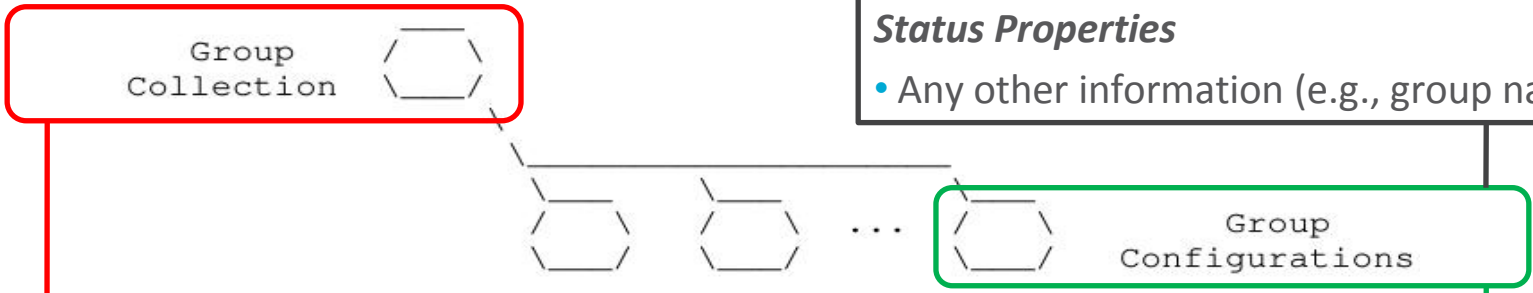

Figure 1: Resources of a Group Manager

Configuration Properties

- Security algorithms and parameters

Status Properties

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

***Group-collection* resource**

- Retrieve the list of OSCORE groups
  - All groups (GET)
  - Groups selected by filters (FETCH)
- Create a new OSCORE group (POST)
  - A group-configuration resource is created
  - A group-membership resource 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 configuration (DELETE)
  - The group-membership resource is also deleted

Since IETF 118

- **Version -10 completed a WG Last Call**
- **Review from Cigdem Sengul**
  - https://mailarchive.ietf.org/arch/msg/ace/JelX3H5rTtOUedGlPhCs0WImun0/
- **Review from Göran Selander**
  - https://mailarchive.ietf.org/arch/msg/ace/4r6CN7GXaS4PVg8CGotD0l8Gi_M/
- **Review from Carsten Bormann (offlist)**
  - Plus a PR fixing nits https://github.com/ace-wg/ace-oscore-gm-admin/pull/5

Thanks!

- **Submitted version -11 before the cut-off**
  - Reviews from Cigdem and Göran: fully addressed
  - Review from Carsten: editorial comments and minor clarifications are addressed
  - It also includes fixes and clarifications already planned by the authors

Updates in v -11 (1/3)

- **Addressed points from Göran's review**
  - Editorial: terminology conventions to be clearer and as early as possible

- **Addressed points from Cigdem's review (higlights)**
  - Status parameter 'group_title' renamed as 'group_description'
  - Editorial: removed moot paragraph on benefits from group name patterns
  - Clarification: the AS can issue Access Tokens (totally) unrelated to these operations
  - Added example of array of scope entries, in CBOR diagnostic notation
    - Including all the three possible types of group name pattern as AIF Toid
  - Additional example of FETCH request to the group-collection resource
    - The filter criteria include 'group_name' as a complex pattern (regular expression)
    - Only for the payload of this request, 'group_name' can be *tstr* or *#6.<uint>(any)*

Updates in v -11 (2/3)

- **Updates already planned by the authors**
  - Clarification: upon creating a group, ‘exp’ (if specified) has to be in the future
  - Clarification: on avoiding accidental deactivation of an OSCORE group
    - TL;DR : include *active = true* in the request for overwriting the group configuration
  - Rule out ways to create a group configuration other than with a POST to /manage
    - PUT/(i)PATCH request to non-existing group-configuration resource → No creation
  - Alignment with changes made in *draft-ietf-ace-key-groupcomm*
    - Specified CBOR integer abbreviations for registered ACE Groupcomm Parameters
    - Used Problem Details (RFC 9290) instead of the custom format for error responses
  - Editorial fixes and readability improvements

Updates in v -11 (3/3)

- **Addressed points from Carsten's review (more remain)**
  - Merged the PR fixing nits https://github.com/ace-wg/ace-oscore-gm-admin/pull/5
  - Several more editorial fixes and readability improvements
  - Use of CBOR Tag 21065 to signal regular expressions as complex patterns
  - No use quotation marks before CBOR Simple Values *false*/*true*/*null*

Todo from Carsten's review

- **Selected points**
  - Examples: avoid text strings as placeholders for to-be-registered integer abbreviations
    - Instead, inaugurate and use what is proposed in *draft-bormann-cbor-e-ref*
  - Multiple Administrators: improve avoidance of race conditions
  - More details on the requirement for some operations to be atomic
  - The PUT request to group-configuration resources should actually use POST
  - Rule out the use of CBOR Tag 35 altogether; just use the CBOR tag 21065 instead
    - https://github.com/ace-wg/ace-oscore-gm-admin/commit/ef677f7bcfcc3e7d6d80c60b9eecb37874b59760#r139386329
  - "Parameters" or "Properties"? (the former)
  - Early centralize and don't repeat definitions (e.g., what "has permission" means)
  - Early recap the meaning of "scope" and "secure communication association"
  - Clarifications on, e.g.: group name; path construct; Group Manager vs. host

Next steps

- **Address remaining points from Carsten's review**

- **Submit version -12 (long) before IETF 120**
  - This version should be ready to be sent to the IESG

Thank you!

Comments/questions?

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