Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-12

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

IETF 120 Meeting – Vancouver – July 22nd, 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

Configuration Parameters

- How Group OSCORE is used in the group (e.g., which security algorithms)

Status Parameters

- Information on the management of the OSCORE Group in itself (e.g., group name, group description, group policies, …)

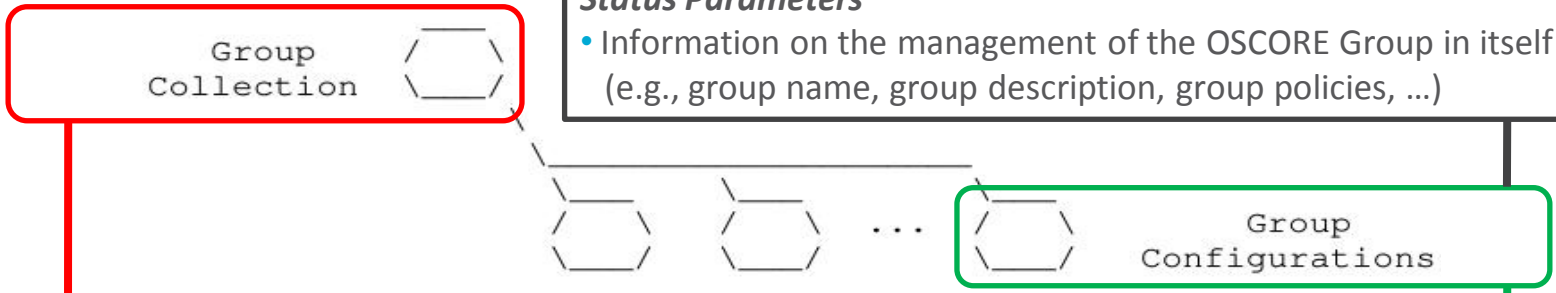

Figure 1: Resources of a Group Manager

***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 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 (POST)
- Update the group configuration (PATCH/iPATCH)
- Delete the group configuration (DELETE)
  - The group-membership resource is also deleted

Status at IETF 119 (March 2024)

- **Version -11 addressed most feedback from WG Last Call**
  - Review from Cigdem Sengul [1]
    - Fully addressed
  - Review from Göran Selander [2]
    - Fully addressed
  - Review from Carsten Bormann (offlist)
    - Partly addressed: merged a PR with editorial fixes [3], plus minor clarifications
  - More fixes and clarifications already planned by the authors

- **What was left to do?**
  - Address all the remaining points from Carsten's review

[1] https://mailarchive.ietf.org/arch/msg/ace/JelX3H5rTtOUedGlPhCs0WImun0/
[2] https://mailarchive.ietf.org/arch/msg/ace/4r6CN7GXaS4PVg8CGotD0l8Gi_M/
[3] https://github.com/ace-wg/ace-oscore-gm-admin/pull/5

Updates in v -12 (1/8)

- **This version -12 addresses all the remaining comments from Carsten**
  - Changes compiled in the PR #6, now merged
  - https://github.com/ace-wg/ace-oscore-gm-admin/pull/6

- **Various editorial improvements and minor clarifications**

- **Section 10 – IANA Considerations**
  - Editorial fixes in presenting the requested new registrations
  - Aligned registrations with conventions used in registries (e.g., CBOR types)

Updates in v -12 (2/8)

Major clarifications (1/2)

- **Section 1.1** – Relation between group name and URI path segment
  - Consistent with the ABNF rule "segment = *pchar" defined in Section 3.3 of RFC 3986

- **Section 1.1** – For the group-collection resource, the url-path /manage is used as an example, but it is not a default one. Implementation can use a different one

- **Section 4.1** – Having a "main Administrator" and an "assistant Administrator" is just an example of multiple Administrators with different responsibilities for the same OSCORE group

Updates in v -12 (3/8)

Major clarifications (2/2)

- **Section 5** – Consistent use of configuration/status "parameters" (not "properties")
  - Also clarified the conceptual difference between the two types
- **Section 5.2** – Improved presentation of default values adopted by the Group Manager for the configuration/status parameters
- **Section 6.3** – Explicit mentioning of the repeatability of the CoAP Location-Path Option
  - In the response from the group-collection resource when creating a new group configuration
- **Section 6.6.2** – Repositioned text from security to operational considerations
  - After a change in the group configuration, the Group Manager should prioritize nodes that rejoin the group, instead of nodes that want to join as new group members

Updates in v -12 (4/8)

Explicit definitions

- **Section 1.1** – Recapped concept of "secure communication association"
- **Section 3.0** – Recapped concept of "scope“
  - Building on Oauth 2.0 (RFC 6749) and ACE (RFC 9200)

Notation in the examples

- The CBOR diagnostic notation uses the construct **e''** (*) to import values from the CDDL model in Appendix B
  - e'SOME_NAME' is replaced by the value assigned to SOME_NAME in the CDDL model
  - For example, {e'group_name': "gp1", e'gp_enc_alg': 10} stands for {-13: "gp1", -4:10}

```
=> 0.05 FETCH
   Uri-Path: manage
   Content-Format: 261 (application/ace-groupcomm+cbor)

   Payload:

   {
       e'group_mode' : true,
       e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
             e'hkdf' : 5 / HMAC-256-256 /
   }
```


(*) Proposed in https://datatracker.ietf.org/doc/draft-ietf-cbor-edn-e-ref/

Updates in v -12 (5/8)

Complex group name patterns in the AIF data model

- **Section 3.0** – The use of the CBOR Tag 35 is not mentioned anymore
  - The CBOR tag 21065 is still suggested …
  - … and used in the examples for indicating regular expressions

- **Appendix A** – Revised description of how the AS can process group name patterns, when processing an Access Token Request from the Administrator
  - This is just an informative example, as a possible starting point to use at the AS

Updates in v -12 (6/8)

On atomicity of operations at the GM

- **Section 4.1** – Added considerations on preventing race conditions and lost updates, in the presence of multiple Administrators for the same OSCORE group

- **Clarified requirement of specific operations to be atomic**
  - **Section 6.3** – Creating a group configuration (POST to the group-collection resource)
  - **Section 6.6** – Overwriting an existing group configuration (POST to the corresponding group-configuration resource)
  - **Section 6.7** – Selectively updating an existing group configuration (PATCH/iPATCH to the corresponding group-configuration resource); same as in Section 6.6
  - **Section 6.8** – Deletion of a group configuration (DELETE to the corresponding group-configuration resource)

Updates in v -12 (7/8)

Execution of specific operations at the GM (1/2)

- **Section 6.0** – Explain only once the meaning of “to have permissions”
  - Single, early definition of access control checks at the Group Manager
  - The later description of specific operations shortly builds on that early definition, using the specific TARGETNAME and PERMISSION to be checked, which pertain to the specific protected request from the Administrator
- **Section 6.6** – Changed REST method for overwriting a group configuration
  - OLD: PUT ➔ NEW: POST // The semantics of this operation is indeed a POST

Updates in v -12 (8/8)

Execution of specific operations at the GM (2/2)

- **Section 6.7** – More details on a reason why an iPATCH request can be invalid
- **Section 6.7** – Example of failed update of a group configuration (PATCH/iPATCH)
  - This must fail if the result of the update would be an inconsistent configuration

Summary and next steps

- **Version -12 should have addressed all the points raised during WG Last Call**
  - Great if Carsten confirms that his comments have been well addressed
- **Editorial pending points**
  1. Editor's note (5 instances): *As per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document …*
     - *draft-ietf-ace-key-groupcomm-oscore* is in AD Evaluation and ahead of the present document
     - Addressing this Editor's note will require only simple, clerical work for name alignment
  2. Comment from IANA: *Until the values have been assigned, please label them as "suggested" or "TBD." This might look like "-1 (suggested)" or "TBD (-1 suggested)" (or similar).*
- **Implementation based on Eclipse Californium**
  - Built on the implementation of the ACE-based Group Manager for Group OSCORE
  - https://bitbucket.org/marco-tiloca-sics/ace-java/src/master/
- **Absent more issues, this version -12 should be ready for the Shepherd review & write-up**

Thank you!

Comments/questions?

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