Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-01

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

IETF 109, ACE WG, November 18th, 2020

Recap

- Admin interface at the OSCORE Group Manager
  - Create and configure an OSCORE group, before a first joining can start
  - Same collection pattern intended for the CoAP pub-sub Broker
  - Supporting 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

- Also 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

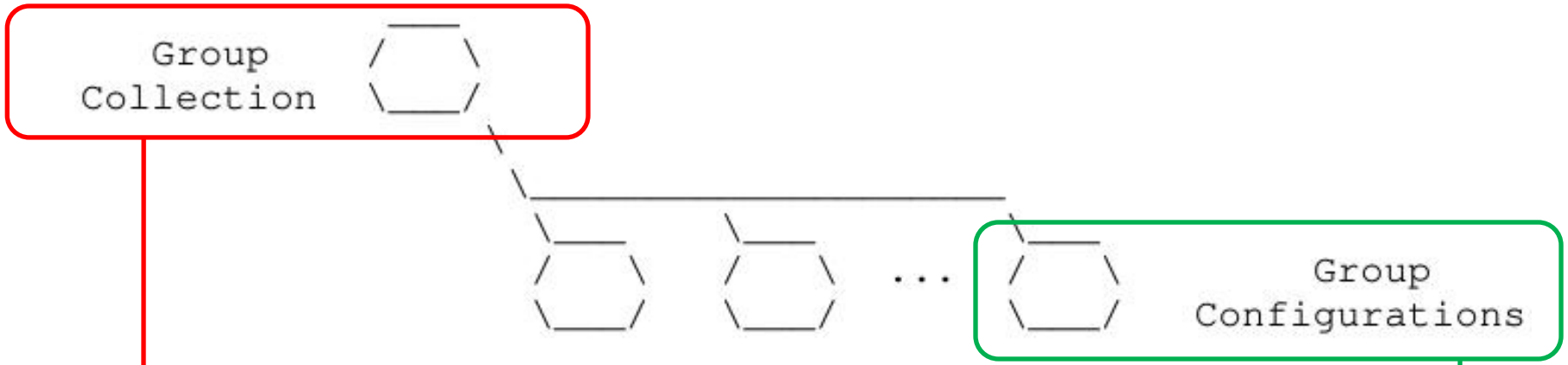

Figure 1: Resources of a Group Manager

***Group-collection* resource**

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

***Group-configuration* resource**

- Retrieve the group configuration (GET)
- Retrieve part of the group configuration (FETCH)
- Update the group configuration (PUT)
- Delete the group (DELETE)

Selected updates from -01

- Covered also the pairwise mode of Group OSCORE
  - Added configuration parameters
    - ‘pairwise_mode’, as true or false
    - ‘ecdh_alg’, ‘ecdh_params’, ‘ecdh_key_params’
  - Default values defines in *ace-key-groupcomm-oscore*

- FETCH handler for group-configuration resources
  - Retrieve only some parameters from the group configuration
  - In CBOR: ‘conf_filter’ array indicating the requested parameters
  - In CoRAL: one top element per requested parameter

- New and updated examples, both in CBOR and CoRAL

Selected updates from -01

- The Group Manager decides the final group name
  - Possibly more constraints than the Administrator knows
  - The Administrator can still suggest a possible name

- Registered also the names of the application groups
  - All those using by the created OSCORE group
  - Added as status parameters in the group configuration
  - Suggested already in the “CoRAL and forms” discussion [1]
  - The Group Manager is also aware of application groups
    - Assumed when registering the OSCORE Group to the RD [2]

[1] https://mailarchive.ietf.org/arch/msg/core/BoYGYmEpJMUS8bk4PNHOEaFFcdU/
[2] https://mailarchive.ietf.org/arch/msg/core/h62d2c2mYmG43ykz52KvbbEpgDc/

Selected updates from -01

- Guidance on registering the OSCORE group to the RD
  - The Group Manager (recommended) or the Administrator can do it
  - Now the names of application groups are surely known
    - Values of target attributes, in registered links to join the OSCORE group
  - Aligned with *draft-tiloca-core-oscore-discovery*

- Registered also the resource type rt=core.osc.gconf
  - Identifying the group configuration resources
  - Also added as status parameter in the group configuration

Value	Description	Reference
core.osc.gcoll	Group-collection resource of an OSCORE Group Manager	[[this document]]
core.osc.gconf	Group-configuration resource of an OSCORE Group Manager	[[this document]]

Summary and next steps

- Admin interface at the OSCORE Group Manager
  - Create and delete OSCORE groups; set and retrieve configurations
  - Support for both i) Link Format and CBOR ; ii) CoRAL

- Next steps
  - PATCH, to selectively update a group configuration
  - Format of scope, using AIF and patterns for group names
    - Allow some actions to administrators that did not create the group [1]
  - More info in response payloads, as CoRAL forms [2]
    - Guidance on group creation and other possible operations
    - In a 4.00 response, what went wrong and how to fix things

[1] https://mailarchive.ietf.org/arch/msg/ace/gLr5NgAURoi5P9f6RcgHkL2jFr8/

[2] https://mailarchive.ietf.org/arch/msg/core/BoYGYmEpJMUS8bk4PNHOEaFFcdU/

Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-ace-oscore-gm-admin

Backup

Group-collection resource

- **GET**
  - Retrieve the full list of existing OSCORE groups
  - In fact, the list of links to the respective *group-configuration* resource

```
=> 0.01 GET
   Uri-Path: manage

<= 2.05 Content
   Content-Format: 40 (application/link-format)

   <coap://[2001:db8::ab]/manage/gp1>;rt="core.osc.gconf",
   <coap://[2001:db8::ab]/manage/gp2>;rt="core.osc.gconf",
   <coap://[2001:db8::ab]/manage/gp3>;rt="core.osc.gconf"
```

```
=> 0.01 GET
   Uri-Path: manage

<= 2.05 Content
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gcoll#>
   #base </manage/>
   item <gp1>
   item <gp2>
   item <gp3>
```

Group-collection resource

- **FETCH**
  - Retrieve a partial list of existing OSCORE groups, by filter criteria
  - In fact, the list of links to the respective *group-configuration* resource

```
=> 0.05 FETCH
   Uri-Path: manage
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
       "alg" : 10,
       "hkdf" : 5
   }

<= 2.05 Content
   Content-Format: 40 (application/link-format)

   <coap://[2001:db8::ab]/manage/gp1>;rt="core.osc.gconf",
   <coap://[2001:db8::ab]/manage/gp2>;rt="core.osc.gconf",
   <coap://[2001:db8::ab]/manage/gp3>;rt="core.osc.gconf"
```

```
=> 0.05 FETCH
   Uri-Path: manage
   Content-Format: TBD1 (application/coral+cbor)

   alg 10
   hkdf 5

<= 2.05 Content
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gcoll#>
   #base </manage/>
   item <gp1>
   item <gp2>
   item <gp3>
```

Group-collection resource

- **POST**
  - Create a new OSCORE group.
  - The GM decides the name, if not specified.

```
=> 0.02 POST
   Uri-Path: manage
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   alg 10
   hkdf 5
   pairwise_mode True
   active True
   group_title "rooms 1 and 2"
   app_group "room1"
   app_group "room2"
   as_uri <coap://as.example.com/token>

<= 2.01 Created
   Location-Path: manage
   Location-Path: gp4
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   group_name "gp4"
   joining_uri <coap://[2001:db8::ab]/ace-group/gp4/>
   as_uri <coap://as.example.com/token>
```

```
=> 0.02 POST
   Uri-Path: manage
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "alg" : 10,
     "hkdf" : 5,
     "pairwise_mode" : True,
     "active" : True,
     "group_title" : "rooms 1 and 2",
     "app_groups": : ["room1", "room2"],
     "as_uri" : "coap://as.example.com/token"
   }

<= 2.01 Created
   Location-Path: manage
   Location-Path: gp4
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
     "as_uri" : "coap://as.example.com/token"
   }
```

- The Group Manager
  - Creates a new *group-configuration* resource (for the Administrator)
  - Creates a new *group-membership* resource (for joining nodes)

Group-configuration resource

- **GET**
  - Retrieve the full current configuration of the OSCORE group

```
=> 0.01 GET
   Uri-Path: manage
   Uri-Path: gp4

<= 2.05 Content
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "alg" : 10,
     "hkdf" : 5,
     "cs_alg" : -8,
     "cs_params" : [[1], [1, 6]],
     "cs_key_params" : [1, 6],
     "cs_key_enc" : 1,
     "pairwise_mode" : True,
     "ecdh_alg" : -27,
     "ecdh_params" : [[1], [1, 6]],
     "ecdh_key_params" : [1, 6],
     "rt" : "core.osc.gconf",
     "active" : True,
     "group_name" : "gp4",
     "group_title" : "rooms 1 and 2",
     "ace-groupcomm-profile" : "coap_group_oscore_app",
     "exp" : "1360289224",
     "app_groups": : ["room1", "room2"],
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
     "as_uri" : "coap://as.example.com/token"
   }
```

```
=> 0.01 GET
   Uri-Path: manage
   Uri-Path: gp4

<= 2.05 Content
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   alg 10
   hkdf 5
   cs_alg -8
   cs_params.alg_capab.key_type 1
   cs_params.key_type_capab.key_type 1
   cs_params.key_type_capab.curve 6
   cs_key_params.key_type 1
   cs_key_params.curve 6
   cs_key_enc 1
   pairwise_mode True
   ecdh_alg -27
   ecdh_params.alg_capab.key_type 1
   ecdh_params.key_type_capab.key_type 1
   ecdh_params.key_type_capab.curve 6
   ecdh_key_params.key_type 1
   ecdh_key_params.curve 6
   rt "core.osc.gconf",
   active True
   group_name "gp4"
   group_title "rooms 1 and 2"
   ace-groupcomm-profile "coap_group_oscore_app"
   exp "1360289224"
   app_group "room1"
   app_group "room2"
   joining_uri <coap://[2001:db8::ab]/ace-group/gp4/>
   as_uri <coap://as.example.com/token>
```

Group-configuration resource

- **FETCH**
  - Retrieve a selection of the current configuration of the OSCORE group

```
=> 0.05 FETCH
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "conf_filter" : ["alg",
                      "hkdf",
                      "pairwise_mode",
                      "active",
                      "group_title",
                      "app_groups"]
   }

<= 2.05 Content
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "alg" : 10,
     "hkdf" : 5,
     "pairwise_mode" : True,
     "active" : True,
     "group_title" : "rooms 1 and 2",
     "app_groups": : ["room1", "room2"]
   }
```

```
=> 0.05 FETCH
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   alg
   hkdf
   pairwise_mode
   active
   group_title
   app_groups

<= 2.05 Content
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   alg 10
   hkdf 5
   pairwise_mode True
   active True
   group_title "rooms 1 and 2"
   app_group "room1"
   app_group "room2"
```

Group-configuration resource

- **PUT**
  - Update the configuration of the OSCORE group
  - Default values apply, like when creating the group

```
=> PUT
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   alg 11
   hkdf 5

<= 2.04 Changed
   Content-Format: TBD1 (application/coral+cbor)

   #using <http://coreapps.org/core.osc.gconf#>
   group_name "gp4"
   joining_uri <coap://[2001:db8::ab]/ace-group/gp4/>
   as_uri <coap://as.example.com/token>
```

```
=> PUT
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "alg" : 11 ,
     "hkdf" : 5
   }

<= 2.04 Changed
   Content-Format: TBD2 (application/ace-groupcomm+cbor)

   {
     "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
     "as_uri" : "coap://as.example.com/token"
   }
```

Group-configuration resource

- **DELETE**
  - Delete the OSCORE group

```
=> DELETE
   Uri-Path: manage
   Uri-Path: gp4

<= 2.02 Deleted
```

- The Group Manager
  - Deallocates the *group-configuration* resource
  - Deallocates the *group-membership* resource