Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-02

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

IETF 110, ACE WG, March 12th, 2021
Recap

› 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

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)
- Overwrite the group configuration (PUT)
- Delete the group (DELETE)
Updates from -02

› Improved error handling, using also the new error types
  – Following the format of error messages in `draft-ace-key-groupcomm`
  – Additional error situations are handled and replied to, e.g.:
    › Deleting a still active group – Error type fixed in the Editor’s copy
    › Notification to a group member, informing of the group deletion

› Admit multiple Administrators
  – All Administrators can access the group-membership resource
  – A set of Administrators can access a group-configuration resource
    › Possibly, only certain operations to certain Administrators
    › Possibly, act on groups created by another Administrator
  – “Classes” of Administrators, to be enforced through ‘scope’ (later ...)

Updates from -02
Updates from -02

Added PATCH/iPATCH handler for group-configuration resources

› Selective updates of an existing group configuration
  – Specify only parameters to update
  – Other parameters keep the same value (don’t default as with PUT)

› Don’t use to create a new group!
  – Use POST to the group-collection resource instead

› Keep the same content formats and its abbreviations
  – Custom CBOR documents: application/ace-groupcomm+cbor
    › Same as in draft-ietf-ace-key-groupcomm(-oscore)
  – CoRAL documents: application/coral+cbor
Group Configuration Parameters

**Configuration properties**
- hkdf
- alg
- cs_alg
- cs_params
- cs_key_params
- cs_key_enc
- pairwise_mode
- ecdh_alg
- ecdh_params
- ecdh_key_params

**Status properties**
- rt = “core.osc.gconf”
- active
- group_name // Plain immutable identifier
- group_title // Descriptive string
- ace_groupcomm_profile
- exp
- joining_uri
- app_groups // Names of application groups
- ? group_policies
- ? as_uri // Link to the AS

- Easy “replacement” update for most parameters
  - Specify the pair (“label”, new_value), like when creating the group
- ‘app_groups’ is a list of names and requires special handling
Configuration update with PATCH

› Two ways to update ‘app_groups’

- **Overwrite** – New array of names as hard replacement
  - app_groups : [“room1”, “room8”]  
    - **Custom CBOR**
  - app_group “room1”
  - app_group “room8”  
    - **CoRAL**

Current value   [“room1”, “room2”]

The result is   [“room1”, “room8”]

› **Addition/deletion** – [ [name_to_remove], [name_to_add] ]
  - app_groups_diff : [ [“room1”], [“room5”] ]  
    - **Custom CBOR**
  - app_group_del “room1”
  - app_group_add “room8”  
    - **CoRAL**

The result is   [“room8”, “room5”]

› Overwrite and addition/deletion **not together** in the same PATCH payload
4.00 (Bad request)
- Any malformed or invalid payload
- iPATCH is used as request method, but:
  - ‘app_groups_diff’ is included (Custom CBOR)
  - ‘app_group_del’ and/or ‘app_group_add’ are included (CoRAL)

4.09 (Conflict)
- New parameter values would yield an inconsistent group configuration

Any reason for using 4.22 (Unprocessable entity)?
Format of ‘scope’

› Section 2.1.1 as placeholder, with a list of design considerations

› New AIF Data Model – Similar to draft-ace-key-groupcomm-oscore

› AIF-Generic<Toid, Tperm> = [ *[Toid, Tperm] ]
  ‒ Toid: Text string, specifying a name pattern for security groups
  ‒ Tperm: Unsigned integer, indicating permissions as flag bits
    › Retrieving the list of security groups is always possible, for any Tperm

› Possible permissions – Over group names matching the pattern!
  ‒ Create the groups, and later do anything on those
  ‒ Read the configuration of groups created by others
  ‒ Overwrite/update the configuration of groups created by others
  ‒ Delete groups created by others

› Useful to enable additional Administrators after a group creation

Any early comment?
Summary and next steps

› Latest updates
  – Improved error handling
  – Admit multiple Administrators
  – PATCH/iPATCH, to selectively update a group configuration

› Next steps
  – Format of ‘scope’, using AIF and patterns for group names
    › Allow some actions to Administrators that did not create the group [1]
  – Implementation, building on the Group Manager in Californium [2]

[1] https://mailarchive.ietf.org/arch/msg/ace/gLr5NgAUROi5P9f6RcgHkL2jFr8/
Thank you!

Comments/questions?

https://github.com/ace-wg/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.

```plaintext
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)

```plaintext
{
   "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)

```json
{
    "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)

```plaintext
#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"]
} `
Group-configuration resource

› PUT

- Overwrite the configuration of the OSCORE group
- Default values apply, like when creating the group

=> 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"
}

=> 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>
Configuration update with PATCH

PATCH

– Selectively update the configuration of the OSCORE group

```
=> 0.06 PATCH
  Uri-Path: manage
  Uri-Path: gp4
  Content-Format: TBD2 (application/ace-groupcomm+cbor)

  {
    "alg" : 10,
    "app_groups_diff" : [["room1"],
                          ["room3", "room4"]]
  }

<= 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"
  }
```

```
=> 0.06 PATCH
  Uri-Path: manage
  Uri-Path: gp4
  Content-Format: TBD1 (application/coral+cbor)

  #using <http://coreapps.org/core.osc.gconf#>
  alg 10
  app_group_del "room1"
  app_group_add "room3"
  app_group_add "room4"

<= 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>
```
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