Admin Interface for the OSCORE Group Manager

Work in progress towards
draft-ietf-ace-oscore-gm-admin-02

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

ACE Interim Meeting, January 14th, 2021
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

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)
Define updates with PATCH

› 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 upon group creation
- ‘app_groups’ is a list of names and requires special handling
Define updates with PATCH

› Two ways to update ‘app_groups’

Current value   [“room1”, “room2”]

› Overwrite – New array of names as hard replacement
  – app_group : [“room1”, “room8”]    // custom CBOR
  – app_group “room1”    // CoRAL
  app_group “room8”

The result is   [“room1”, “room8”]

› Addition/deletion – [ [names_to_remove], [names_to_add] ]
  – app_group_diff : [ [“room1”], [“room5”] ]    // custom CBOR
  – app_group_del “room1”    // CoRAL
  app_group_add “room8”

The result is   [“room8”, “room5”]

› Overwrite and addition/deletion **not together** in the same PATCH payload
Define updates with PATCH

› Error handling to be thought through

› 4.00 (Bad request)
  – Any malformed payload

› 4.09 (Conflict)
  – New parameter values yield an overall inconsistent configuration
  – Possibly to be covered already at group creation/overwriting

› 4.22 (Unprocessable entity)
  – Any obvious reason ???
  – Why/when more appropriate than 5.03 (Service unavailable)
Format of ‘scope’ using AIF

› New AIF Data Model
  – Similar to the one in *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

› Possible permissions – Over group names matching the pattern
  – Retrieve list of security groups and read their configuration – *Keep together?*
  – Overwrite or update the current configuration of a security group
  – Create and delete a security group – *Split?*

› Useful also to later enable additional administrators
  – E.g. only update configurations of groups already created by another Admin
Thank you!
Comments/questions?
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

```plaintext
=> 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"
```

```plaintext
=> 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)

```plaintext
#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)

```plaintext
#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)

```plaintext
{
  "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: TB02 (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: TB01 (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

– Update the configuration of the OSCORE group
– Default values apply, like when creating the group

```yaml
=> 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)

```yaml
#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>
```

```yaml
=> 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)

```yaml
{
  "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