

Admin Interface for the OSCORE Group Manager

draft-tiloca-ace-oscore-gm-admin-01

Marco Tilocca, RISE
Rikard Hoglund, RISE
Peter van der Stok
Francesca Palombini, Ericsson
Klaus Hartke, Ericsson

IETF ACE WG, Virtual Interim, May 18th, 2020

Motivation

- › The OSCORE Group Manager
 - Acts as Key Distribution Center for an OSCORE group
 - Handles the joining of candidate group members
- › *draft-ietf-ace-key-groupcomm-oscore* describes:
 - How to get keying material from the Group Manager, e.g. at joining
 - Based on the RESTful interface defined in *draft-ietf-ace-key-groupcomm*
 - ACE is used for authentication and authorization at the Group Manager
- › Need to specify
 - How to create and delete OSCORE groups at the Group Manager
 - How to set and retrieve configurations of existing OSCORE groups

Contribution

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

- › Two new types of resources at the Group Manager
 - A single *group-collection* resource, at /manage
 - One *group-configuration* resource per group, at /manage/GROUP_NAME

- › 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

Updates from -00

- › Addressed the review from Jim [1] – Thanks!
- › Improved organization and presentation of parameters
 - Configuration properties, Status properties, default values
- › Improved set of available operations
- › Described side effects of some parameter updates
 - E.g., encryption algorithm, signature algorithm
- › Extensive examples: in link format and CBOR; in CoRAL
- › Klaus has joined as co-author!

[1] https://mailarchive.ietf.org/arch/msg/ace/DhAl3fdLB_qf3jF_9oQlqVivdyE/

Overview

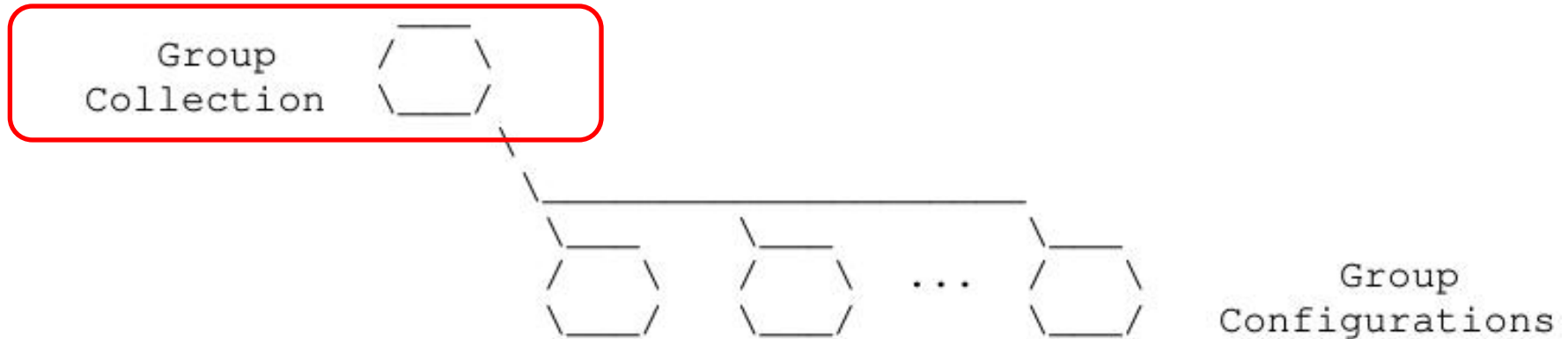


Figure 1: Resources of a Group Manager

› *Group-collection* resource

- Create a new OSCORE group (POST)
 - › Optionally provide an initial configuration
- Retrieve the list of OSCORE groups and their configuration
 - › All groups (GET), or groups selected by filters (FETCH)

Overview

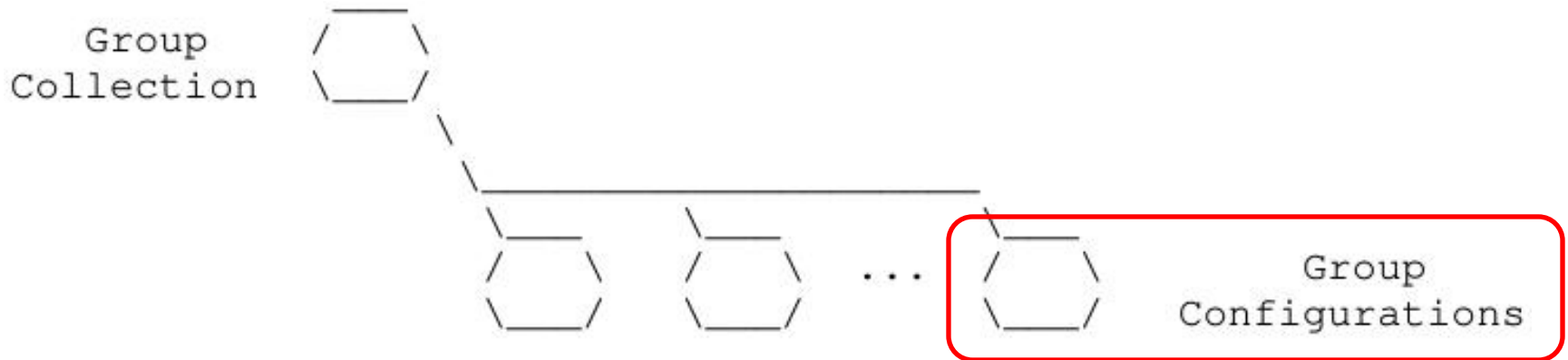


Figure 1: Resources of a Group Manager

› *Group-configuration* resource

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

Parameters

› Configuration properties

- hkdf (*)
- alg (*)
- cs_alg (*)
- cs_params (*)
- cs_key_params (*)
- cs_key_enc (*)

› Status properties

- active (*)
- group_name
 - Plain immutable identifier
- group_title (*)
 - Descriptive string
- ace_groupcomm_profile
- exp
- joining_path
 - Link to the group-membership resource
- ? group_policies
- ? as_uri
 - Link to the Authorization Server

(*) Default values are specified

Group-collection resource

> GET

- Retrieve the 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>,
<coap://[2001:db8::ab]/manage/gp2>,
<coap://[2001:db8::ab]/manage/gp3>
```

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

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

```
#using <http://coreapps.org/ace.oscore.gm#>
#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: TBD2 (application/ace-groupcomm+cbor)
```

```
{
  "alg" : 10,
  "hkdf" : 5,
  "active" : True,
  "group_title" : "rooms 1 and 2",
  "as_uri" : "coap://as.example.com/token"
}
```

```
<= 2.01 Created
Location-Path: manage
Location-Path: gp4
```

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

```
#using <http://coreapps.org/ace.oscore.gm#>
alg 10
hkdf 5
active True
group_title "rooms 1 and 2"
as_uri <coap://as.example.com/token>
```

```
<= 2.01 Created
Location-Path: manage
Location-Path: gp4
```

› The Group Manager

- Handles missing/incomplete configurations with default values
- Creates a new *group-configuration* resource (for the Administrator)
- Creates a new *group-membership* resource (for joining nodes)

Group-configuration resource

> GET

– Retrieve the 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" : -6,
  "cs_key_params" : [-6, 1],
  "cs_key_enc" : 1,
  "active" : True,
  "group_name" : "gp4",
  "group_title" : "rooms 1 and 2",
  "ace-groupcomm-profile" : "coap_group_oscore_app",
  "exp" : "1360289224",
  "joining_path" : "coap://[2001:db8::ab]/group-oscore/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/ace.oscore.gm#>
alg 10
hkdf 5
cs_alg -8
cs_params -6
cs_key_params.curve -6
cs_key_params.type 1
cs_key_enc 1
active True
group_name "gp4"
group_title "rooms 1 and 2"
ace-groupcomm-profile "coap_group_oscore_app"
exp "1360289224"
joining_path <coap://[2001:db8::ab]/group-oscore/gp4/>
as_uri <coap://as.example.com/token>
```

Side effects

- › When updating a group configuration or deleting a group
 - The Group Manager informs the group members individually
 - Group members may observe the group-membership resource

- › When 'active' is changed to false
 - No new nodes can join, current members should stop communicating

- › When 'hkdf' or 'alg' change
 - Group members can use the new values or leave the group

- › When any 'cs_*' changes, group members can
 - Leave or rejoin, possibly providing a new public key
 - Stay in the group, use the new values, possibly provide a new public key

Summary

- › Admin interface at the OSCORE Group Manager
 - Create and delete OSCORE groups; set and retrieve configurations
 - Consistent with the interface for candidate and current group members

- › Examples
 - Link Format and CBOR
 - CoRAL

- › Same pattern of the Pub-Sub Broker. Define as separate document?

- › Need more feedback and reviews

Thank you!

Comments/questions?

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

Backup

Group-collection resource

> GET

- Retrieve the 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>,
<coap://[2001:db8::ab]/manage/gp2>,
<coap://[2001:db8::ab]/manage/gp3>
```

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

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

```
#using <http://coreapps.org/ace.oscore.gm#>
#base </manage/>
item <gp1>
item <gp2>
item <gp3>
```

Group-collection resource

> FETCH

- Retrieve the list of existing OSCORE groups, by filters
- 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>,
<coap://[2001:db8::ab]/manage/gp2>,
<coap://[2001:db8::ab]/manage/gp3>
```

```
=> 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/ace.oscore.gm#>
#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: TBD2 (application/ace-groupcomm+cbor)
```

```
{
  "alg" : 10,
  "hkdf" : 5,
  "active" : True,
  "group_title" : "rooms 1 and 2",
  "as_uri" : "coap://as.example.com/token"
}
```

```
<= 2.01 Created
Location-Path: manage
Location-Path: gp4
```

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

```
#using <http://coreapps.org/ace.oscore.gm#>
alg 10
hkdf 5
active True
group_title "rooms 1 and 2"
as_uri <coap://as.example.com/token>
```

```
<= 2.01 Created
Location-Path: manage
Location-Path: gp4
```

› The Group Manager

- Handles missing/incomplete configurations with default values
- Creates a new *group-configuration* resource (for the Administrator)
- Creates a new *group-membership* resource (for joining nodes)

Group-configuration resource

> GET

– Retrieve the 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" : -6,
  "cs_key_params" : [-6, 1],
  "cs_key_enc" : 1,
  "active" : True,
  "group_name" : "gp4",
  "group_title" : "rooms 1 and 2",
  "ace-groupcomm-profile" : "coap_group_oscore_app",
  "exp" : "1360289224",
  "joining_path" : "coap://[2001:db8::ab]/group-oscore/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/ace.oscore.gm#>
alg 10
hkdf 5
cs_alg -8
cs_params -6
cs_key_params.curve -6
cs_key_params.type 1
cs_key_enc 1
active True
group_name "gp4"
group_title "rooms 1 and 2"
ace-groupcomm-profile "coap_group_oscore_app"
exp "1360289224"
joining_path <coap://[2001:db8::ab]/group-oscore/gp4/>
as_uri <coap://as.example.com/token>
```

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: TBD2 (application/ace-groupcomm+cbor)
{
  "alg" : 11 ,
  "hkdf" : 5
}
```

```
=> PUT
Uri-Path: manage
Uri-Path: gp4
Content-Format: TBD1 (application/coral+cbor)
#using <http://coreapps.org/ace.oscore.gm#>
alg 11
hkdf 5

<= 2.04 Changed
```

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