Admin Interface for the OSCORE Group Manager

draft-tiloca-ace-oscore-gm-admin-02

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

IETF 108, ACE WG, July 29th, 2020
Recap

› 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
  – 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/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
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
  - Retrieve the list of OSCORE groups and their configuration
    - All groups (GET), or groups selected by filters (FETCH)

Figure 1: Resources of a Group Manager
Overview

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

Figure 1: Resources of a Group Manager
Updates from -02

› Addressed the review from Jim [1] – Thanks!

› Addressed comments from Christian [2] and Carsten – Thanks!

› Default values of configuration parameters (‘alg’, ‘hkdf’, …)
   – Moved to draft-ietf-ace-key-groupcomm-oscore

› Revised text on side effects, following a group update
   – Current Section 2.6.5.2, hopefully easier to read now

[1] https://mailarchive.ietf.org/arch/msg/ace/q55WDjJLdEMVvI0bV7k_VrzRgIY/
[2] https://mailarchive.ietf.org/arch/msg/ace/gLr5NgAURoi5P9f6RcgHkL2jFr8/
Updates from -02

› Payload in the response to a group creation/update
  – ‘joining_uri’
  – ‘as_uri’
  – ‘group_name’

› Clarified scope in the introduction
  – In some deployments, the GM application is very knowledgeable
  – The GM can autonomously create and configure OSCORE groups
  – Downside: the GM is application-specific, error prone, and non flexible

› Guidance on registering the OSCORE group to the RD
  – Either the Group Manager or the Administrator can do it
  – Aligned with draft-tiloca-core-oscore-discovery
Open points

Different group name for management and joining nodes [1]
– ‘group_name_admin’, for admin operations
– ‘group_name_members’, to be advertised for joining nodes
– Possible, with no big penalty. Any big advantage?

Who takes the final decision on the group name?
– Now: the Administrator proposes a name, the GM may change it
– Proposed update: the Administrator gives the exact name to use
– In either case, en error is returned if the name is already taken
– Issues with that? Opinions?

[1] https://mailarchive.ietf.org/arch/msg/ace/q55WDjJLdEMVvI0bV7k_VrzRgIY/
Open points

› Cover the case of multiple administrators [2]
  – The Admin creating a group G is allowed to configure it
  – Another Admin may read and/or modify G
  – Define a proper ‘scope’ format also enabling this

› Register also the names of the application groups
  – All those using the created OSCORE group
  – Suggested by Jim in the “CoRAL and forms” discussion [3]
  – The Group Manager is also aware of application groups
    ‣ Assumed when registering the OSCORE Group to the RD [4]

[2] https://mailarchive.ietf.org/arch/msg/ace/gLr5NgAURoi5P9f6RcgHkL2jFr8/
[3] https://mailarchive.ietf.org/arch/msg/core/BoYGYmEpJMUS8bk4PNHOEaFFcdU/
Summary and next steps

› Admin interface at the OSCORE Group Manager
  – Create and delete OSCORE groups; set and retrieve configurations

› Next steps
  – Address the open points
  – Format of scope, using AIF
  – PATCH, to selectively update a group configuration
  – More info in response payloads, as CoRAL forms [3]
    › Guidance on group creation and other possible operations
    › In a 4.00 response, what went wrong and how to fix things

› Adoption call ended on the 6th of July – Chairs evaluation?

[3] 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 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

```json
=> 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>
```
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
Content-Format: TBD2 (application/ace-groupcomm+cbor)
{
  "group_name": "gp4",
  "joining_uri": "coap://[2001:db8::ab]/group-oscore/gp4/",
  "as_uri": "coap://as.example.com/token"
}

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

#using <http://coreapps.org/ace.oscore.gm#>
group_name "gp4"
joining_uri <coap://[2001:db8::ab]/group-oscore/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 current configuration of the OSCORE group

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

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

```json
#using <http://coreapps.org/ace.oscore.gm#>
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
active True
group_name "gp4"
group_title "rooms 1 and 2"
ace-groupcomm-profile "coap_group_oscore_app"
exp "1360289224"
joining_uri <coap://[2001:db8::ab]/group-oscore/gp4/>
as_uri <coap://as.example.com/token>
```

IETF 108 | ACE WG | 2020-07-29 | Page 15
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
   }

<= 2.04 Changed
   Content-Format: TBD2 (application/ace-groupcomm+cbor)
   {
     "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/group-oscore/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/ace.oscore.gm#>
   alg 11
   hkdf 5

<= 2.04 Changed
   Content-Format: TBD1 (application/coral+cbor)
   #using <http://coreapps.org/ace.oscore.gm#>
   group_name "gp4"
   joining_uri <coap://[2001:db8::ab]/group-oscore/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
Side effects

› When updating a group configuration or deleting a group
  – The Group Manager informs the group members individually

› 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