Admin Interface for the OSCORE Group Manager

draft-tiloca-ace-oscore-gm-admin-00

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

IETF 106, ACE WG, Singapore, November 19th, 2019
Motivation

› The OSCORE Group Manager
   – Acts as Key Distribution Center for Group OSCORE nodes
   – 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 groups
Contribution

› Admin interface at the OSCORE Group Manager
  – Create a configure an OSCORE group, before a first joining can start
  – Strongly inspired by the latest proposal for the CoAP pub-sub Broker

› 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

› 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
Overview

Group-collection resource

– Create a new OSCORE group, optionally provide a starting configuration
– Retrieve the list of all existing OSCORE groups
Overview

Group Manager + --- /manage
+ Group-collection resource
+ /gp1 Group-configuration resource
+ /gp2 Group-configuration resource
... ... 

› Group-configuration resource
   – Update or retrieve the group configuration
   – Delete the OSCORE group
Group-collection resource

› GET

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

Request: Administrator -> Group Manager

Req: GET coap://gm.example.com/manage

Response: Group Manager -> Administrator

Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/manage/gp1>;ct=40,
<coap://[2001:db8::ab]/manage/gp2>;ct=40,
<coap://[2001:db8::ab]/manage/gp3>;ct=40
Group-collection resource

› POST

– Create a new OSCORE group “NAME”
– Optionally, suggest an initial configuration

Request: Administrator → Group Manager

Req: POST coap://gm.example.com/manage
Content-Format: 60
Payload:

```json
{
  "group_name": "gp4",
  "group_conf": {
    (remainder of 'group_conf' omitted for brevity)
  }
}
```

› “group_name”
– Invariant identifier, MUST be present

› “group_conf”
– Suggested configuration, MAY be present

› 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-collection resource

› POST

– Create a new OSCORE group “NAME”
– Optionally, suggest an initial configuration

Response: Group Manager → Administrator

Res: 2.01 Created
Content-Format: 60
Location-Path: /manage/gp4
Payload:

```json
{
    "group_name": "gp4",
    "group_conf": {
        (remainder of ‘group_conf’ omitted for brevity)
    }
    "profile": "coap_group_oscore_app",
    "exp": "1360289224",
    "joining_path": "coap://[2001:db8::ab]/group-oscore/gp4/",
}
```

› Location-Path

– Path of the group-configuration resource

› “group_name”

– Invariant identifier, MUST be present

› “group_conf”

– Enforced configuration, MUST be present

› “joining_path”

– Link to group-membership resource, MUST be present
Group-configuration resource

› GET
  – Retrieve the current configuration of the OSCORE group

Request: Administrator -> Group Manager

Req: GET coap://gm.example.com/manage/gp2

› Format of response payload
  – Same of response to the POST to the group-collection resource
  – That is, “group_name”, “group_conf”, …
Group-configuration resource

› POST
  – Update the configuration of the OSCORE group

› Format of request payload
  – Same of POST request to the group-collection resource
  – However, “group_name” MUST NOT be present
  – Missing parameter in “group_conf” -> Unchanged configuration parameter

› Format of response payload
  – Same of response to the POST to the group-collection resource
  – “group_conf” specifies the new configuration, i.e. as after the update
Group-configuration resource

DELETE

– Delete the OSCORE group

Request: Administrator -> Group Manager

Req: DELETE coap://gm.example.com/manage/gp1

Response: Group Manager -> Administrator

Res: 2.02 Deleted

The Group Manager

– Deallocates the group-configuration resource
– Deallocates the group-membership resource
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

› Implementations
  – Peter van der Stok – Available for libcoap (C)
  – RISE – Starting for Californium (Java)

› Started as an Experimental draft
  – Should it be a Standards track document?

› Need feedback and reviews
Thank you!

Comments/questions?

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