

ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2021

M. Tiloca
R. Hoeglund
RISE AB
P. van der Stok
Consultant
F. Palombini
K. Hartke
Ericsson AB
July 13, 2020

Admin Interface for the OSCORE Group Manager
draft-tiloca-ace-oscore-gm-admin-02

Abstract

Group communication for CoAP can be secured using Group Object Security for Constrained RESTful Environments (Group OSCORE). A Group Manager is responsible to handle the joining of new group members, as well as to manage and distribute the group key material. This document defines a RESTful admin interface at the Group Manager, that allows an Administrator entity to create and delete OSCORE groups, as well as to retrieve and update their configuration. The ACE framework for Authentication and Authorization is used to enforce authentication and authorization of the Administrator at the Group Manager. Protocol-specific transport profiles of ACE are used to achieve communication security, proof-of-possession and server authentication.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 14, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Terminology	4
2.	Group Administration	5
2.1.	Getting Access to the Group Manager	6
2.2.	Managing OSCORE Groups	7
2.3.	Group Configurations	8
2.3.1.	Group Configuration Representation	8
2.3.2.	Default Values	10
2.4.	Discovery	10
2.5.	Collection Representation	10
2.6.	Interactions	11
2.6.1.	Get All Groups Configurations	11
2.6.2.	Fetch Group Configurations By Filters	12
2.6.3.	Create a New Group Configuration	13
2.6.4.	Retrieve a Group Configuration	17
2.6.5.	Update a Group Configuration	18
2.6.6.	Delete a Group Configuration	21
3.	Security Considerations	23
4.	IANA Considerations	23
4.1.	ACE Groupcomm Parameters Registry	23
4.2.	Resource Types	24
5.	References	24
5.1.	Normative References	25
5.2.	Informative References	27
	Acknowledgments	28
	Authors' Addresses	28

1. Introduction

The Constrained Application Protocol (CoAP) [[RFC7252](#)] can be used in group communication environments where messages are also exchanged over IP multicast [[I-D.dijk-core-groupcomm-bis](#)]. Applications relying on CoAP can achieve end-to-end security at the application layer by using Object Security for Constrained RESTful Environments (OSCORE) [[RFC8613](#)], and especially Group OSCORE [[I-D.ietf-core-oscore-groupcomm](#)] in group communication scenarios.

When group communication for CoAP is protected with Group OSCORE, nodes are required to explicitly join the correct OSCORE group. To this end, a joining node interacts with a Group Manager (GM) entity responsible for that group, and retrieves the required key material to securely communicate with other group members using Group OSCORE.

The method in [[I-D.ietf-ace-key-groupcomm-oscore](#)] specifies how nodes can join an OSCORE group through the respective Group Manager. Such a method builds on the ACE framework for Authentication and Authorization [[I-D.ietf-ace-oauth-authz](#)], so ensuring a secure joining process as well as authentication and authorization of joining nodes (clients) at the Group Manager (resource server).

In some deployments, the application running on the Group Manager may know when a new OSCORE group has to be created, as well as how it should be configured and later on updated or deleted, e.g. based on the current application state or on pre-installed policies. In this case, the Group Manager application can create and configure OSCORE groups when needed, by using a local application interface. However, this requires the Group Manager to be application-specific, which in turn leads to error prone deployments and is poorly flexible.

In other deployments, a separate Administrator entity, such as a Commissioning Tool, is directly responsible for creating and configuring the OSCORE groups at a Group Manager, as well as for maintaining them during their whole lifetime until their deletion. This allows the Group Manager to be agnostic of the specific applications using secure group communication.

This document specifies a RESTful admin interface at the Group Manager, intended for an Administrator, as a separate entity external to the Group Manager and its application. The interface allows the Administrator to create and delete OSCORE groups, as well as to configure and update their configuration.

Interaction examples are provided, in Link Format [[RFC6690](#)] and CBOR [[RFC7049](#)], as well as in CoRAL [[I-D.ietf-core-coral](#)]. While all the CoRAL examples use the CoRAL textual serialization format, the CBOR

or JSON [\[RFC8259\]](#) binary serialization format is used when sending such messages on the wire.

The ACE framework is used to ensure authentication and authorization of the Administrator (client) at the Group Manager (resource server). In order to achieve communication security, proof-of-possession and server authentication, the Administrator and the Group Manager leverage protocol-specific transport profiles of ACE, such as [\[I-D.ietf-ace-oscore-profile\]](#)[\[I-D.ietf-ace-dtls-authorize\]](#). These include also possible forthcoming transport profiles that comply with the requirements in [Appendix C](#) of [\[I-D.ietf-ace-oauth-authz\]](#).

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [\[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

Readers are expected to be familiar with the terms and concepts related to CBOR [\[RFC7049\]](#) and COSE [\[I-D.ietf-cose-rfc8152bis-struct\]](#)[\[I-D.ietf-cose-rfc8152bis-algs\]](#), the CoAP protocol [\[RFC7252\]](#), as well as the protection and processing of CoAP messages using OSCORE [\[RFC8613\]](#), also in group communication scenarios using Group OSCORE [\[I-D.ietf-core-oscore-groupcomm\]](#). These include the concept of Group Manager, as the entity responsible for a set of groups where communications among members are secured using Group OSCORE.

Readers are also expected to be familiar with the terms and concept related to the management of keying material for groups in ACE defined in [\[I-D.ietf-ace-key-groupcomm\]](#), and in particular to the joining process for OSCORE groups defined in [\[I-D.ietf-ace-key-groupcomm-oscore\]](#). These include the concept of group-membership resource hosted by the Group Manager, that new members access to join the OSCORE group, while current members can access to retrieve updated keying material.

Readers are also expected to be familiar with the terms and concepts described in the ACE framework for authentication and authorization [\[I-D.ietf-ace-oauth-authz\]](#). The terminology for entities in the considered architecture is defined in OAuth 2.0 [\[RFC6749\]](#). In particular, this includes Client (C), Resource Server (RS), and Authorization Server (AS).

Note that, unless otherwise indicated, the term "endpoint" is used here following its OAuth definition, aimed at denoting resources such

as /token and /introspect at the AS, and /authz-info at the RS. This document does not use the CoAP definition of "endpoint", which is "An entity participating in the CoAP protocol".

This document also refers to the following terminology.

- o Administrator: entity responsible to create, configure and delete OSCORE groups at a Group Manager.
- o Group name: stable and invariant name of an OSCORE group. The group name MUST be unique under the same Group Manager, and MUST include only characters that are valid for a URI path segment, namely unreserved and pct-encoded characters [[RFC3986](#)].
- o Group-collection resource: a single-instance resource hosted by the Group Manager. An Administrator accesses a group-collection resource to create a new OSCORE group, or to retrieve the list of existing OSCORE groups, under that Group Manager. As an example, this document uses /manage as the url-path of the group-collection resource; implementations are not required to use this name, and can define their own instead.
- o Group-configuration resource: a resource hosted by the Group Manager, associated to an OSCORE group under that Group Manager. A group-configuration resource is identifiable with the invariant group name of the respective group. An Administrator accesses a group-configuration resource to retrieve or update the configuration of the respective OSCORE group, or to delete that group. The url-path to a group-configuration resource has NAME as last segment, with NAME the invariant group name assigned upon its creation. Building on the considered url-path of the group-collection resource, this document uses /manage/NAME as the url-path of a group-configuration resource; implementations are not required to use this name, and can define their own instead.
- o Admin endpoint: an endpoint at the Group Manager associated to the group-collection resource or to a group-configuration resource hosted by that Group Manager.

2. Group Administration

With reference to the ACE framework and the terminology defined in OAuth 2.0 [[RFC6749](#)]:

- o The Group Manager acts as Resource Server (RS). It provides one single group-collection resource, and one group-configuration resource per existing OSCORE group. Each of those is exported by a distinct admin endpoint.

- o The Administrator acts as Client (C), and requests to access the group-collection resource and group-configuration resources, by accessing the respective admin endpoint at the Group Manager.
- o The Authorization Server (AS) authorizes the Administrator to access the group-collection resource and group-configuration resources at a Group Manager. Multiple Group Managers can be associated to the same AS. The AS MAY release Access Tokens to the Administrator for other purposes than accessing admin endpoints of registered Group Managers.

2.1. Getting Access to the Group Manager

All communications between the involved entities rely on the CoAP protocol and MUST be secured.

In particular, communications between the Administrator and the Group Manager leverage protocol-specific transport profiles of ACE to achieve communication security, proof-of-possession and server authentication. To this end, the AS may explicitly signal the specific transport profile to use, consistently with requirements and assumptions defined in the ACE framework [[I-D.ietf-ace-oauth-authz](#)].

With reference to the AS, communications between the Administrator and the AS (/token endpoint) as well as between the Group Manager and the AS (/introspect endpoint) can be secured by different means, for instance using DTLS [[RFC6347](#)][[I-D.ietf-tls-dtls13](#)] or OSCORE [[RFC8613](#)]. Further details on how the AS secures communications (with the Administrator and the Group Manager) depend on the specifically used transport profile of ACE, and are out of the scope of this specification.

In order to get access to the Group Manager for managing OSCORE groups, an Administrator performs the following steps.

1. The Administrator requests an Access Token from the AS, in order to access the group-collection and group-configuration resources on the Group Manager. The Administrator will start or continue using secure communications with the Group Manager, according to the response from the AS.
2. The Administrator transfers authentication and authorization information to the Group Manager by posting the obtained Access Token, according to the used profile of ACE, such as [[I-D.ietf-ace-dtls-authorize](#)] and [[I-D.ietf-ace-oscore-profile](#)]. After that, the Administrator must have secure communication established with the Group Manager, before performing any admin operation on that Group Manager. Possible ways to provide secure

communication are DTLS [RFC6347][I-D.ietf-tls-dtls13] and OSCORE [RFC8613]. The Administrator and the Group Manager maintain the secure association, to support possible future communications.

3. The Administrator performs admin operations at the Group Manager, as described in the following sections. These include the retrieval of the existing OSCORE groups, the creation of new OSCORE groups, the update and retrieval of group configurations, and the removal of OSCORE groups. Messages exchanged among the Administrator and the Group Manager are specified in [Section 2.6](#).

2.2. Managing OSCORE Groups

Figure 1 shows the resources of a Group Manager available to an Administrator.

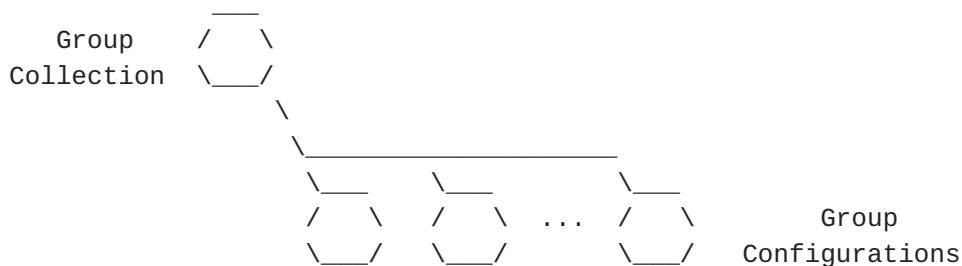


Figure 1: Resources of a Group Manager

The Group Manager exports a single group-collection resource. The full interface for the group-collection resource allows the Administrator to:

- o Retrieve the list of existing OSCORE groups, possibly by filters.
- o Create a new OSCORE group, specifying its invariant group name and, optionally, its configuration.

The Group Manager exports one group-configuration resource for each of its OSCORE groups. Each group-configuration resource is identified by the group name specified upon creating the group. The full interface for a group-configuration resource allows the Administrator to:

- o Retrieve the current configuration of the OSCORE group.
- o Update the current configuration of the OSCORE group.
- o Delete the OSCORE group.

2.3. Group Configurations

A group configuration consists of a set of parameters.

2.3.1. Group Configuration Representation

The group configuration representation is a CBOR map which MUST include configuration properties and status properties.

2.3.1.1. Configuration Properties

The CBOR map MUST include the following configuration parameters:

- o 'hkdf', defined in [Section 4.1](#) of this document, specifies the HKDF algorithm used in the OSCORE group, encoded as a CBOR text string. Possible values are the same ones admitted for the 'hkdf' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 3.2.1 of [[I-D.ietf-ace-oscore-profile](#)].
- o 'alg', defined in [Section 4.1](#) of this document, specifies the AEAD algorithm used in the OSCORE group, encoded as a CBOR text string. Possible values are the same ones admitted for the 'alg' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 3.2.1 of [[I-D.ietf-ace-oscore-profile](#)].
- o 'cs_alg', defined in [Section 4.1](#) of this document, specifies the countersignature algorithm used in the OSCORE group, encoded as a CBOR text string or integer. Possible values are the same ones admitted for the 'cs_alg' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 6.4 of [[I-D.ietf-ace-key-groupcomm-oscore](#)].
- o 'cs_params', defined in [Section 4.1](#) of this document, specifies the additional parameters for the countersignature algorithm used in the OSCORE group, encoded as a CBOR array. Possible formats and values are the same ones admitted for the 'cs_params' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 6.4 of [[I-D.ietf-ace-key-groupcomm-oscore](#)].
- o 'cs_key_params', defined in [Section 4.1](#) of this document, specifies the additional parameters for the key used with the countersignature algorithm in the OSCORE group, encoded as a CBOR array. Possible formats and values are the same ones admitted for the 'cs_key_params' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 6.4 of [[I-D.ietf-ace-key-groupcomm-oscore](#)].

- o 'cs_key_enc', defined in [Section 4.1](#) of this document, specifies the encoding of the public keys of group members, encoded as a CBOR integer. Possible values are the same ones admitted for the 'cs_key_enc' parameter of the "OSCORE Security Context Parameters" registry, defined in Section 6.4 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#).

2.3.1.2. Status Properties

The CBOR map MUST include the following status parameters:

- o 'active', encoding the CBOR simple value True if the group is currently active, or the CBOR simple value False otherwise. This parameter is defined in [Section 4.1](#) of this specification.
- o 'group_name', with value the group name of the OSCORE group encoded as a CBOR text string. This parameter is defined in [Section 4.1](#) of this specification.
- o 'group_title', with value either a human-readable description of the group encoded as a CBOR text string, or the CBOR simple value Null if no description is specified. This parameter is defined in [Section 4.1](#) of this specification.
- o 'ace-groupcomm-profile', defined in Section 4.1.2.1 of [\[I-D.ietf-ace-key-groupcomm\]](#), with value "coap_group_oscore_app".
- o 'exp', defined in Section 4.1.2.1 of [\[I-D.ietf-ace-key-groupcomm\]](#).
- o 'joining_uri', with value the URI of the group-membership resource for joining the newly created OSCORE group, encoded as a CBOR text string. This parameter is defined in [Section 4.1](#) of this specification.

The CBOR map MAY include the following status parameters:

- o 'group_policies', defined in Section 4.1.2.1 of [\[I-D.ietf-ace-key-groupcomm\]](#), and consistent with the format and content defined in Section 6.4 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#).
- o 'as_uri', defined in [Section 4.1](#) of this document, specifies the URI of the Authorization Server associated to the Group Manager for the OSCORE group, encoded as a CBOR text string. Candidate group members will have to obtain an Access Token from that Authorization Server, before starting the joining process with the Group Manager to join the OSCORE group (see [\[I-D.ietf-ace-key-groupcomm-oscore\]](#)).

2.3.2. Default Values

This section defines the default values that the Group Manager assumes for configuration and status parameters.

2.3.2.1. Configuration Parameters

For each configuration parameter, the Group Manager MUST assume a pre-configured default value, if none is specified by the Administrator.

In particular, the Group Manager SHOULD use the same default values defined in Section 18 of [[I-D.ietf-ace-key-groupcomm-oscore](#)].

2.3.2.2. Status Parameters

For the following status parameters, the Group Manager MUST assume a pre-configured default value, if none is specified by the Administrator.

- o For 'active', the CBOR simple value False.
- o For 'group_title', the CBOR simple value Null.

2.4. Discovery

The Administrator can discover the group-collection resource from a resource directory, for instance [[I-D.ietf-core-resource-directory](#)] and [[I-D.hartke-t2trg-coral-reef](#)], or from .well-known/core , by using the resource type "ace.oscore.gm" defined in [Section 4.2](#) of this specification.

The Administrator can discover group-configuration resources for the group-collection resource as specified below in [Section 2.6.1](#) and [Section 2.6.2](#).

2.5. Collection Representation

A list of group configurations is represented as a document containing the corresponding group-configuration resources in the list. Each group-configuration is represented as a link, where the link target is the URI of the group-configuration resource.

The list can be represented as a Link Format document [[RFC6690](#)] or a CoRAL document [[I-D.ietf-core-coral](#)]. In the latter case, the CoRAL document contains the group-configuration resources in the list as top-level elements. In particular, the link to each group-

configuration resource has <http://coreapps.org/ace.oscore.gm#item> as relation type.

2.6. Interactions

This section describes the operations available on the group-collection resource and the group-configuration resources.

When custom CBOR is used, the Content-Format in messages containing a payload is set to application/ace-groupcomm+cbor, defined in Section 8.2 of [I-D.ietf-ace-key-groupcomm]. Furthermore, the entry labels defined in Section 4.1 MUST be used, when specifying the corresponding configuration and status parameters.

2.6.1. Get All Groups Configurations

The Administrator can send a GET request to the group-collection resource, in order to retrieve the list of the existing OSCORE groups at the Group Manager. This is returned as a list of links to the corresponding group-configuration resources.

Example in Link Format:

```
=> 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>
```

Example in CoRAL:

```
=> 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>
```


2.6.2. Fetch Group Configurations By Filters

The Administrator can send a FETCH request to the group-collection resource, in order to retrieve the list of the existing OSCORE groups at the Group Manager that fully match a set of specified filter criteria. This is returned as a list of links to the corresponding group-configuration resources.

The set of filter criteria is specified in the request payload as a CBOR map, where possible entry labels are all the ones used for configuration properties (see [Section 2.3.1.1](#)), as well as "group_name" and "active" for the corresponding status property (see [Section 2.3.1.2](#)).

Entry values are the ones admitted for the corresponding labels in the POST request for creating a group configuration (see [Section 2.6.3](#)). A valid request MUST NOT include the same entry multiple times.

Example in custom CBOR and Link Format:

```
=> 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>
```

Example in CoRAL:


```
=> 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>
```

2.6.3. Create a New Group Configuration

The Administrator can send a POST request to the group-collection resource, in order to create a new OSCORE group at the Group Manager. The request MAY specify the intended group name NAME and group title, and MAY specify pieces of information concerning the group configuration.

The request payload is a CBOR map, whose possible entries are specified in [Section 2.3.1](#). In particular:

- o The CBOR map MAY include any of the configuration parameter defined in [Section 2.3.1.1](#).
- o The CBOR map MAY include any of the status parameter 'group_name', 'group_title', 'exp', 'group_policies', 'as_uri' and 'active' defined in [Section 2.3.1.2](#).
- o The CBOR map MUST NOT include any of the status parameter 'ace-groupcomm-profile' and 'joining_uri' defined in [Section 2.3.1.2](#).

If any of the following occurs, the Group Manager MUST respond with a 4.00 (Bad Request) response, which MAY include additional information to clarify what went wrong.

- o Any of the received parameters is specified multiple times.
- o Any of the received parameters is not recognized, or not valid, or not consistent with respect to other related parameters.
- o The 'group_name' parameter specifies the group name of an already existing OSCORE group.

- o The Group Manager does not trust the Authorization Server with URI specified in the 'as_uri' parameter, and has no alternative Authorization Server to consider for the OSCORE group to create.

After a successful processing of the request above, the Group Manager performs the following actions.

First, the Group Manager creates a new group-configuration resource, accessible to the administrator at /manage/NAME , where NAME is the group name as either indicated in the parameter 'group_name' of the request or uniquely assigned by the Group Manager. The values specified in the request are used as group configuration information for the newly created OSCORE group. For each configuration parameter not specified in the request, the Group Manager MUST assume the default value specified in [Section 2.3.2](#).

After that, the Group Manager creates a new group-membership resource, accessible to joining nodes and future group members at group-oscore/NAME , as specified in [\[I-D.ietf-ace-key-groupcomm-oscore\]](#). In particular, the Group Manager will rely on the current group configuration to build the Joining Response message defined in Section 5.4 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#), when handling the joining of a new group member. Furthermore, the Group Manager generates the following pieces of information, and assigns them to the newly created OSCORE group:

- o The OSCORE Master Secret.
- o The OSCORE Master Salt (optionally).
- o The OSCORE ID Context, acting as Group ID, which MUST be unique within the set of OSCORE groups under the Group Manager.

Finally, the Group Manager replies to the Administrator with a 2.01 (Created) response. The Location-Path option MUST be included in the response, indicating the location of the just created group-configuration resource. The response MUST NOT include a Location-Query option. The response payload is a CBOR map, which MUST include the following parameters:

- o 'group_name', with value the group name of the OSCORE group encoded as a CBOR text string. This value can be different from the group name possibly specified by the Administrator in the POST request, and reflects the final choice of the Group Manager as 'group_name' status property for the OSCORE group.

- o 'joining_uri', with value the URI of the group-membership resource for joining the newly created OSCORE group, encoded as a CBOR text string.
- o 'as_uri', with value the URI of the Authorization Server associated to the Group Manager for the newly created OSCORE group, encoded as a CBOR text string. This value can be different from the URI possibly specified by the Administrator in the POST request, and reflects the final choice of the Group Manager as 'as_uri' status property for the OSCORE group.

At this point, the Group Manager can register the link to the group-membership resource with URI specified in 'joining_uri' to the CoRE Resource Directory [[I-D.ietf-core-resource-directory](#)], as defined in Section 2 of [[I-D.tiloca-core-oscore-discovery](#)].

Alternatively, the Administrator can perform the registration to the Resource Directory on behalf of the Group Manager, acting as Commissioning Tool. The Administrator considers the following when specifying additional information for the link to register.

- o The name of the OSCORE group MUST take the value specified in 'group_name' from the 2.01 (Created) response above.
- o If present, parameters describing the cryptographic algorithms used in the group MUST follow the values that the Administrator specified in the POST request above, or the corresponding default values specified in [Section 2.3.2.1](#) otherwise.
- o If also registering a related link to the Authorization Server associated to the OSCORE group, the related link MUST have the URI specified in 'as_uri' from the 2.01 (Created) response above.

Example in custom CBOR:


```
=> 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"
  }
```

Example in CoRAL:

```
=> 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>
```


2.6.4. Retrieve a Group Configuration

The Administrator can send a GET request to the group-configuration resource `manage/NAME` associated to an OSCORE group with group name `NAME`, in order to retrieve the current configuration of that group.

After a successful processing of the request above, the Group Manager replies to the Administrator with a 2.05 (Content) response. The response has as payload the representation of the group configuration as specified in [Section 2.3.1](#). The exact content of the payload reflects the current configuration of the OSCORE group. This includes both configuration properties and status properties.

Example in custom CBOR:

```
=> 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" : [[1], [1, 6]],
  "cs_key_params" : [1, 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"
}
```

Example in CoRAL:


```
=> 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.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>
```

2.6.5. Update a Group Configuration

The Administrator can send a PUT request to the group-configuration resource associated to an OSCORE group, in order to update the current configuration of that group. The payload of the request has the same format of the POST request defined in [Section 2.6.3](#), with the exception of the status parameter 'group_name' that MUST NOT be included.

The error handling for the PUT request is the same as for the POST request defined in [Section 2.6.3](#). If no error occurs, the Group Manager performs the following actions.

First, the Group Manager updates the configuration of the OSCORE group, consistently with the values indicated in the PUT request from the Administrator. For each configuration parameter not specified in the PUT request, the Group Manager MUST use the default value specified in [Section 2.3.2](#). From then on, the Group Manager relies on the latest update configuration to build the Joining Response message defined in [Section 5.4](#) of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#), when handling the joining of a new group member.

Then, the Group Manager replies to the Administrator with a 2.04 (Changed) response. The payload of the response has the same format of the 2.01 (Created) response defined in [Section 2.6.3](#).

If the link to the group-membership resource was registered in the Resource Directory (see [[I-D.ietf-core-resource-directory](#)]), the GM is responsible to refresh the registration, as defined in Section 3 of [[I-D.tiloca-core-oscore-discovery](#)].

Alternatively, the Administrator can update the registration to the Resource Directory on behalf of the Group Manager, acting as Commissioning Tool. The Administrator considers the following when specifying additional information for the link to update.

- o The name of the OSCORE group MUST take the value specified in 'group_name' from the 2.04 (Changed) response above.
- o If present, parameters describing the cryptographic algorithms used in the group MUST follow the values that the Administrator specified in the POST request above, or the corresponding default values specified in [Section 2.3.2.1](#) otherwise.
- o If also registering a related link to the Authorization Server associated to the OSCORE group, the related link MUST have the URI specified in 'as_uri' from the 2.04 (Changed) response above.

Example in custom CBOR:

```
=> 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"
  }
```

Example in CoRAL:


```
=> 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>
```

2.6.5.1. Effects on Joining Nodes

If the value of the status parameter 'active' is changed from True to False, the Group Manager MUST stop admitting new members in the group. In particular, upon receiving a Joining Request (see Section 5.3 of [[I-D.ietf-ace-key-groupcomm-oscore](#)]), the Group Manager MUST respond with a 5.03 (Service Unavailable) response to the joining node, and MAY include additional information to clarify what went wrong.

If the value of the status parameter 'active' is changed from False to True, the Group Manager resumes admitting new members in the group, by processing their Joining Requests (see Section 5.3 of [[I-D.ietf-ace-key-groupcomm-oscore](#)]).

2.6.5.2. Effects on the Group Members

After having updated a group configuration, the Group Manager informs the group members, over the pairwise secure communication channels established when joining the OSCORE group (see Section 5 of [[I-D.ietf-ace-key-groupcomm-oscore](#)]).

To this end, the Group Manager can individually target the 'control_path' URI path of each group member (see Section 4.1.2.1 of [[I-D.ietf-ace-key-groupcomm](#)]), if provided by the intended recipient upon joining the group (see Section 5 of [[I-D.ietf-ace-key-groupcomm-oscore](#)]). Alternatively, group members can subscribe for updates to the group-membership resource of the OSCORE group, e.g. by using CoAP Observe [[RFC7641](#)].

Every group member, upon learning that the group has been deactivated (i.e. 'active' has value False), SHOULD stop communicating in the OSCORE group.

Every group member, upon learning that the group has been reactivated (i.e. 'active' has value True again), can resume communicating in the OSCORE group.

Every group member, upon receiving updated values for 'alg' and 'hkdf', MUST either:

- o Leave the group (see Section 14 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#)), e.g. if not supporting the indicated new algorithms; or
- o Use the new parameter values, and accordingly re-derive the OSCORE Security Context for the group (see Section 2 of [\[I-D.ietf-core-oscore-groupcomm\]](#)).

Every group member, upon receiving updated values for 'cs_alg', 'cs_params', 'cs_key_params' and 'cs_key_enc', MUST either:

- o Leave the group, e.g. if not supporting the indicated new algorithm, parameters and encoding; or
- o Leave the group and rejoin it (see Section 5 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#)), providing the Group Manager with a public key which is compatible with the indicated new algorithm, parameters and encoding; or
- o Use the new parameter values, and, if required, provide the Group Manager with a new public key to use in the group, as compatible with the indicated parameters (see Section 10 of [\[I-D.ietf-ace-key-groupcomm-oscore\]](#)).

2.6.6. Delete a Group Configuration

The Administrator can send a DELETE request to the group-configuration resource, in order to delete that group. A group deletion would be successful only on an inactive group.

That is, the DELETE request actually yields a successful deletion of the group, only if the corresponding status parameter 'active' has current value False. The administrator can ensure that, by first performing an update of the group-configuration resource associated to the group (see [Section 2.6.5](#)), and setting the corresponding status parameter 'active' to False.

If, upon receiving the DELETE request, the current value of the status parameter 'active' is True, the Group Manager MUST respond with a 4.09 (Conflict) response, which MAY include additional information to clarify what went wrong.

After a successful processing of the request above, the Group Manager performs the following actions.

First, the Group Manager deletes the OSCORE group and deallocates both the group-configuration resource as well as the group-membership resource.

Then, the Group Manager replies to the Administrator with a 2.02 (Deleted) response.

Example:

```
=> DELETE
    Uri-Path: manage
    Uri-Path: gp4
```

```
<= 2.02 Deleted
```

2.6.6.1. Effects on the Group Members

After having deleted a group, the Group Manager can inform the group members by means of the following two methods. When contacting a group member, the Group Manager uses the pairwise secure communication channel established with that member during its joining process (see Section 5 of [[I-D.ietf-ace-key-groupcomm-oscure](#)]).

- o The Group Manager sends an individual request message to each group member, targeting the respective resource used to perform the group rekeying process (see Section 16 of [[I-D.ietf-ace-key-groupcomm-oscure](#)]). The Group Manager uses the same format of the Joining Response message in Section 5.4 of [[I-D.ietf-ace-key-groupcomm-oscure](#)], where only the parameters 'gkty', 'key', and 'ace-groupcomm-profile' are present, and the 'key' parameter is empty.
- o A group member may subscribe for updates to the group-membership resource of the group. In particular, if this relies on CoAP Observe [[RFC7641](#)], a group member would receive a 4.04 (Not Found) notification response from the Group Manager, since the group-configuration resource has been deallocated upon deleting the group.

When being informed about the group deletion, a group member deletes the OSCORE Security Context that it stores as associated to that group, and possibly deallocates any dedicated control resource intended for the Group Manager that it has for that group.

3. Security Considerations

Security considerations are inherited from the ACE framework for Authentication and Authorization [[I-D.ietf-ace-oauth-authz](#)], and from the specific transport ace-groupcomm-profile of ACE used between the Administrator and the Group Manager, such as [[I-D.ietf-ace-dtls-authorize](#)] and [[I-D.ietf-ace-oscore-profile](#)].

4. IANA Considerations

This document has the following actions for IANA.

4.1. ACE Groupcomm Parameters Registry

IANA is asked to register the following entries in the "ACE Groupcomm Parameters" Registry defined in Section 8.5 of [[I-D.ietf-ace-key-groupcomm](#)].

Name	CBOR Key	CBOR Type	Reference
hkdf	TBD3	tstr	[[this document]]
alg	TBD4	tstr	[[this document]]
cs_alg	TBD5	tstr / int	[[this document]]
cs_params	TBD6	array	[[this document]]
cs_key_params	TBD7	array	[[this document]]
cs_key_enc	TBD8	int	[[this document]]
active	TBD9	simple type	[[this document]]
group_name	TBD10	tstr	[[this document]]
group_title	TBD11	tstr / simple type	[[this document]]
joining_uri	TBD12	tstr	[[this document]]
as_uri	TBD13	tstr	[[this document]]

4.2. Resource Types

IANA is asked to enter the following value into the Resource Type (rt=) Link Target Attribute Values subregistry within the Constrained Restful Environments (CoRE) Parameters registry defined in [\[RFC6690\]](#).

Value	Description	Reference
ace.oscore.gm	Group-collection resource of an OSCORE Group Manager	[[this document]]

5. References

5.1. Normative References

- [COSE.Algorithms]
IANA, "COSE Algorithms",
<<https://www.iana.org/assignments/cose/cose.xhtml#algorithms>>.
- [COSE.Elliptic.Curves]
IANA, "COSE Elliptic Curves",
<<https://www.iana.org/assignments/cose/cose.xhtml#elliptic-curves>>.
- [COSE.Key.Types]
IANA, "COSE Key Types",
<<https://www.iana.org/assignments/cose/cose.xhtml#key-type>>.
- [I-D.ietf-ace-key-groupcomm]
Palombini, F. and M. Tiloca, "Key Provisioning for Group Communication using ACE", [draft-ietf-ace-key-groupcomm-08](#) (work in progress), July 2020.
- [I-D.ietf-ace-key-groupcomm-oscore]
Tiloca, M., Park, J., and F. Palombini, "Key Management for OSCORE Groups in ACE", [draft-ietf-ace-key-groupcomm-oscore-08](#) (work in progress), July 2020.
- [I-D.ietf-ace-oauth-authz]
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", [draft-ietf-ace-oauth-authz-35](#) (work in progress), June 2020.
- [I-D.ietf-ace-oscore-profile]
Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "OSCORE profile of the Authentication and Authorization for Constrained Environments Framework", [draft-ietf-ace-oscore-profile-11](#) (work in progress), June 2020.
- [I-D.ietf-core-coral]
Hartke, K., "The Constrained RESTful Application Language (CoRAL)", [draft-ietf-core-coral-03](#) (work in progress), March 2020.

[I-D.ietf-core-oscore-groupcomm]

Tiloca, M., Selander, G., Palombini, F., and J. Park,
"Group OSCORE - Secure Group Communication for CoAP",
[draft-ietf-core-oscore-groupcomm-09](#) (work in progress),
June 2020.

[I-D.ietf-cose-rfc8152bis-algs]

Schaad, J., "CBOR Object Signing and Encryption (COSE):
Initial Algorithms", [draft-ietf-cose-rfc8152bis-algs-11](#)
(work in progress), July 2020.

[I-D.ietf-cose-rfc8152bis-struct]

Schaad, J., "CBOR Object Signing and Encryption (COSE):
Structures and Process", [draft-ietf-cose-rfc8152bis-struct-11](#) (work in progress), July 2020.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<https://www.rfc-editor.org/info/rfc2119>>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform
Resource Identifier (URI): Generic Syntax", STD 66,
[RFC 3986](#), DOI 10.17487/RFC3986, January 2005,
<<https://www.rfc-editor.org/info/rfc3986>>.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link
Format", [RFC 6690](#), DOI 10.17487/RFC6690, August 2012,
<<https://www.rfc-editor.org/info/rfc6690>>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework",
[RFC 6749](#), DOI 10.17487/RFC6749, October 2012,
<<https://www.rfc-editor.org/info/rfc6749>>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object
Representation (CBOR)", [RFC 7049](#), DOI 10.17487/RFC7049,
October 2013, <<https://www.rfc-editor.org/info/rfc7049>>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained
Application Protocol (CoAP)", [RFC 7252](#),
DOI 10.17487/RFC7252, June 2014,
<<https://www.rfc-editor.org/info/rfc7252>>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained
Application Protocol (CoAP)", [RFC 7641](#),
DOI 10.17487/RFC7641, September 2015,
<<https://www.rfc-editor.org/info/rfc7641>>.

- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", [RFC 8613](#), DOI 10.17487/RFC8613, July 2019, <<https://www.rfc-editor.org/info/rfc8613>>.

5.2. Informative References

- [I-D.dijk-core-groupcomm-bis]
Dijk, E., Wang, C., and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", [draft-dijk-core-groupcomm-bis-03](#) (work in progress), March 2020.
- [I-D.hartke-t2trg-coral-reef]
Hartke, K., "Resource Discovery in Constrained RESTful Environments (CoRE) using the Constrained RESTful Application Language (CoRAL)", [draft-hartke-t2trg-coral-reef-04](#) (work in progress), May 2020.
- [I-D.ietf-ace-dtls-authorize]
Gerdes, S., Bergmann, O., Bormann, C., Selander, G., and L. Seitz, "Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)", [draft-ietf-ace-dtls-authorize-12](#) (work in progress), July 2020.
- [I-D.ietf-core-resource-directory]
Shelby, Z., Koster, M., Bormann, C., Stok, P., and C. Amsuess, "CoRE Resource Directory", [draft-ietf-core-resource-directory-24](#) (work in progress), March 2020.
- [I-D.ietf-tls-dtls13]
Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", [draft-ietf-tls-dtls13-38](#) (work in progress), May 2020.
- [I-D.tiloca-core-oscore-discovery]
Tiloca, M., Amsuess, C., and P. Stok, "Discovery of OSCORE Groups with the CoRE Resource Directory", [draft-tiloca-core-oscore-discovery-05](#) (work in progress), March 2020.
- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", [RFC 6347](#), DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, [RFC 8259](https://www.rfc-editor.org/info/rfc8259), DOI 10.17487/RFC8259, December 2017, <<https://www.rfc-editor.org/info/rfc8259>>.

Acknowledgments

The authors sincerely thank Christian Amsuess, Carsten Bormann and Jim Schaad for their comments and feedback.

The work on this document has been partly supported by VINNOVA and the Celtic-Next project CRITISEC.

Authors' Addresses

Marco Tiloca
RISE AB
Isafjordsgatan 22
Kista SE-16440 Stockholm
Sweden

Email: marco.tiloca@ri.se

Rikard Hoeglund
RISE AB
Isafjordsgatan 22
Kista SE-16440 Stockholm
Sweden

Email: rikard.hoglund@ri.se

Peter van der Stok
Consultant

Phone: +31-492474673 (Netherlands), +33-966015248 (France)
Email: consultancy@vanderstok.org
URI: www.vanderstok.org

Francesca Palombini
Ericsson AB
Torshamnsgatan 23
Kista SE-16440 Stockholm
Sweden

Email: francesca.palombini@ericsson.com

Klaus Hartke
Ericsson AB
Torshamnsgatan 23
Kista SE-16440 Stockholm
Sweden

Email: klaus.hartke@ericsson.com