Workgroup: ACE Working Group
Internet-Draft:
draft-ietf-ace-oscore-gm-admin-09
Published: 1 July 2023
Intended Status: Standards Track
Expires: 2 January 2024
Authors: M. Tiloca R. Höglund P. van der Stok
RISE AB RISE AB Consultant
F. Palombini
Ericsson AB

Admin Interface for the OSCORE Group Manager

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 keying 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.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Authentication and Authorization for Constrained Environments Working Group mailing list (ace@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ace/.

Source for this draft and an issue tracker can be found at https://github.com/ace-wg/ace-oscore-gm-admin.

Status of This Memo

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 2 January 2024.

Copyright Notice

Table of Contents

1. Introduction

The Constrained Application Protocol (CoAP) [RFC7252] can also be used for group communication [I-D.ietf-core-groupcomm-bis], where messages are exchanged between members of a group, e.g., over IP multicast. 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 keying 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 [RFC9200], 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 specify and update their configuration.

Interaction examples are provided in Link Format [RFC6690] and in CBOR [RFC8949]. The examples in CBOR are expressed in CBOR diagnostic notation without the tag and value abbreviations.

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 [RFC9202][RFC9203]. These include also possible forthcoming transport profiles that comply with the requirements in Appendix C of [RFC9200].

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 from the following specifications.

* CBOR [RFC8949] and COSE [RFC9052][RFC9053].

* The CoAP protocol [RFC7252], also in group communication scenarios [I-D.ietf-core-groupcomm-bis]. These especially include the following concepts.

  - "application group", as a set of CoAP nodes that share a common set of resources.

  - "security group", as a set of CoAP nodes that share the same security material, and use it to protect and verify exchanged messages.

* The OSCORE [RFC8613] and Group OSCORE [I-D.ietf-core-oscore-groupcomm] security protocols. These especially include the following concepts.

  - Group Manager, as the entity responsible for a set of OSCORE groups where communications among members are secured using Group OSCORE. An OSCORE group is used as security group for one or many application groups.

  - Authentication credential, as the set of information associated with an entity, including that entity's public key and parameters associated with the public key. Examples of authentication credentials are CBOR Web Tokens (CWTs) and CWT Claims Sets (CCSs) [RFC8392], X.509 certificates [RFC5280], and C509 certificates [I-D.ietf-cose-cbor-encoded-cert].

* The ACE framework for authentication and authorization [RFC9200]. 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).

* The management of keying material for groups in ACE [I-D.ietf-ace-key-groupcomm] and specifically for OSCORE groups [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.

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.

- Administrator: entity responsible to create, configure and delete OSCORE groups at a Group Manager.

- 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.

- Group-collection resource: a single-instance resource hosted by the Group Manager. An Administrator accesses a group-collection resource to retrieve the list of existing OSCORE groups, or to create a new OSCORE group, 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.

- Group-configuration resource: a resource hosted by the Group Manager, associated with an OSCORE group under that Group Manager. A group-configuration resource is identifiable with the invariant group name of the respective OSCORE group. An Administrator accesses a group-configuration resource to retrieve or change the configuration of the respective OSCORE group, or to delete that group.

  The url-path to a group-configuration resource has GROUPNAME as last segment, with GROUPNAME the invariant group name assigned upon its creation. Building on the considered url-path of the group-collection resource, this document uses /manage/GROUPNAME as the url-path of a group-configuration resource; implementations are not required to use this name, and can define their own instead.

- Admin resource: a group-collection resource or a group-configuration resource hosted by the Group Manager.

2. Group Administration

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

- The Group Manager acts as Resource Server (RS). It provides one single group-collection resource, and one group-configuration resource per existing OSCORE group.

- The Administrator acts as Client (C), and requests to access the group-collection resource and group-configuration resources at the Group Manager.

- 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 with the same AS.

  The authorized access for an Administrator can be limited to performing only a subset of operations, according to what is allowed by the authorization information in the Access Token issued to that Administrator (see Section 3 and Section 4). The AS can authorize multiple Administrators to access the group-collection resource and the (same) group-configuration resources at the Group Manager.

  The AS MAY release Access Tokens to the Administrator for other purposes than accessing admin resources of registered Group Managers.

2.1. Managing OSCORE Groups

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

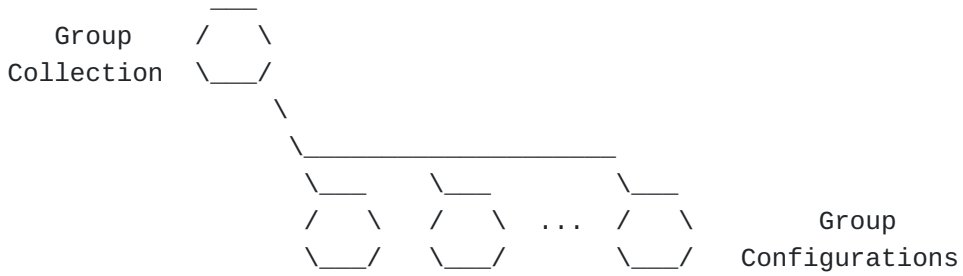

Figure 1: Admin Resources of a Group Manager

The Group Manager exports a single group-collection resource, with resource type "core.osc.gcoll" defined in Section 10.3 of this

document. The interface for the group-collection resource defined in Section 6 allows the Administrator to:

- Retrieve the list of existing OSCORE groups.

- Retrieve the list of existing OSCORE groups matching with specified filter criteria.

- 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 has resource type "core.osc.gconf" defined in Section 10.3 of this document, and is identified by the group name specified upon creating the OSCORE group. The interface for a group-configuration resource defined in Section 6 allows the Administrator to:

- Retrieve the complete current configuration of the OSCORE group.

- Retrieve part of the current configuration of the OSCORE group, by applying filter criteria.

- Overwrite the current configuration of the OSCORE group.

- Selectively update only part of the current configuration of the OSCORE group.

- Delete the OSCORE group.

2.2. Collection Representation

A collection of group configurations is represented as a Link Format document [RFC6690] containing the list of corresponding group-configuration resources.

Each group configuration is represented as a link, which specifies the URI of the group-configuration resource as link target, and the link target attribute 'rt' (Resource Type) with value "core.osc.gconf" defined in Section 10.3 of this document.

2.3. Discovery

The Administrator can discover the group-collection resource from a Resource Directory [RFC9176] or from .well-known/core, by using the resource type "core.osc.gcoll" defined in Section 10.3 of this document.

The Administrator can discover group-configuration resources for the group-collection resource as specified in Section 6.1 and Section 6.2.

3. Format of Scope

This section defines the exact format and encoding of scope to use, in order to express authorization information for the Administrator (see Section 4).

To this end, this document uses the Authorization Information Format (AIF) [RFC9237]. In particular, it uses and extends the AIF specific data model AIF-OSCORE-GROUPCOMM defined in Section 3 of [I-D.ietf-ace-key-groupcomm-oscore].

The original definition of the data model AIF-OSCORE-GROUPCOMM specifies a scope as structured in scope entries, which express authorization information for users of an OSCORE group, i.e., actual group members or external signature verifiers. In the rest of this section, these are referred to as "user scope entries".

This document extends the same AIF specific data model AIF-OSCORE-GROUPCOMM as defined below. In particular, it defines how the same scope can (also) include scope entries that express authorization information for Administrators of OSCORE groups. In the rest of this section, these are referred to as "admin scope entries".

Like in the original definition of the data model AIF-OSCORE-GROUPCOMM, and with reference to the generic AIF model

AIF-Generic<Toid, Tperm> = [* [Toid, Tperm]]

the value of the CBOR byte string used as scope encodes the CBOR array [* [Toid, Tperm]], where each [Toid, Tperm] element corresponds to one scope entry.

Then, the following applies for each admin scope entry intended to express authorization information for an Administrator, as defined in this document.

* The object identifier ("Toid") is specialized as either of the following, and specifies a group name pattern P for the admin scope entry.

  - Wildcard pattern: "Toid" is specialized as the CBOR simple value "true" (0xf5), specifying the wildcard pattern. That is, any group name expressed as a literal text string matches with this group name pattern.

- Literal pattern: "Toid" is specialized as a CBOR text string, whose value specifies an exact group name as a literal string. That is, only one specific group name expressed as a literal text string matches with this group name pattern.

- Complex pattern: "Toid" is specialized as a tagged CBOR data item, specifying a more complex group name pattern with the semantics signaled by the CBOR tag. That is, multiple group names expressed as a literal text string match with this group name pattern.

  For example, and as typically expected, the data item can be a CBOR text string marked with the CBOR tag 35. This indicates that the group name pattern specified as value of the CBOR text string is a regular expression (see Section 3.4.5.3 of [RFC8949]).

  In case the AIF specific data model AIF-OSCORE-GROUPCOMM is used in a JSON payload, the semantics information conveyed by the CBOR tag can be equivalently conveyed, for example, in a nested JSON object.

  The AS and the Group Manager are expected to have agreed on commonly supported semantics for group name patterns. This can happen, for instance, as part of the registration process of the Group Manager at the AS.

* The permission set ("Tperm") is specialized as a CBOR unsigned integer with value Q. This specifies the permissions that the Administrator has to perform operations on the admin resources at the Group Manager, as pertaining to any OSCORE group whose name matches with the pattern P. The value Q is computed as follows.

  - Each permission in the permission set is converted into the corresponding numeric identifier X from the "Value" column of the "Group OSCORE Admin Permissions" registry, for which this document defines the entries in Figure 2.

  - The set of N numbers is converted into the single value Q, by taking two to the power of each numeric identifier X_1, X_2, ..., X_N, and then computing the inclusive OR of the binary representations of all the power values.

  In general, a single permission can be associated with multiple different operations that are possible to be performed when interacting with the Group Manager. For example, the "List" permission allows the Administrator to retrieve a list of group configurations (see Section 6.1) or only a subset of that according to specified filter criteria (see Section 6.2), by

issuing a GET or FETCH request to the group-collection resource, respectively.

Name	Value	Description
List	0	Retrieve list of group configurations
Create	1	Create new group configurations
Read	2	Retrieve group configurations
Write	3	Change group configurations
Delete	4	Delete group configurations

Figure 2: Numeric identifier of permissions on the admin resources at a Group Manager

The following CDDL [RFC8610] notation defines an admin scope entry that uses the data model AIF-OSCORE-GROUPCOMM and expresses a set of permissions from those in Figure 2.

```
AIF-OSCORE-GROUPCOMM = AIF-Generic<oscore-gname, oscore-gperm>

oscore-gname = true / tstr / #6.nnn(any) ; Group name pattern
oscore-gperm = uint .bits admin-permissions

admin-permissions = &(
   List: 0,
   Create: 1,
   Read: 2,
   Write: 3,
   Delete: 4
)

scope_entry = [oscore-gname, oscore-gperm]
```

Future specifications that define new permissions on the admin resources at the Group Manager MUST register a corresponding numeric identifier in the "Group OSCORE Admin Permissions" registry defined in Section 10.4 of this document.

When using the scope format as defined in this section, the permission set ("Tperm") of each admin scope entry MUST include the "List" permission. It follows that, when expressing permissions for Administrators of OSCORE groups as defined in this document, an

admin scope entry has the least significant bit of "Tperm" always set to 1.

Therefore, an Administrator is always allowed to retrieve a list of existing group configurations. The exact elements included in the returned list are determined by the Group Manager, based on the group name patterns specified in the admin scope entries of the Administrator's Access Token, as well as on possible filter criteria specified in the request from the Administrator (see Section 6.1 and Section 6.2).

Building on the above, the same single scope can include user scope entries as well as admin scope entries, whose specific format is defined in Section 3 of [I-D.ietf-ace-key-groupcomm-oscore] and earlier in this section, respectively. The two types of scope entries can be unambiguously distinguished by means of the least significant bit of their permission set "Tperm", which has value 0 for the user scope entries and 1 for the admin scope entries.

The coexistence of user scope entries and admin scope entries within the same scope makes it possible to issue a single Access Token, in case the requesting Client wishes to be a user for some OSCORE groups and at the same time Administrator for some (other) OSCORE groups under the same Group Manager.

Throughout the rest of this document, the term "scope entry" is used as referred to "admin scope entry", unless otherwise indicated.

3.1. On Using Group Name Patterns

Having the object identifier ("Toid") specialized as a pattern displays a number of advantages.

* When relying on wildcard patterns and complex patterns, the encoded scope can be compact in size while allowing the Administrator to operate on large pools of group names.

* When relying on wildcard patterns and complex patterns, the Administrator and the AS do not need to know exact group names for requesting and issuing an Access Token, respectively (see Section 4). In turn, the Group Manager can effectively take the final decision about the name to assign to an OSCORE group, upon its creation (see Section 6.3).

* The Administrator may have established a secure communication association with the Group Manager based on a first Access Token T1, and then created an OSCORE group G. Following the invalidation of T1 (e.g., due to expiration) and the establishment of a new secure communication association with the Group Manager based on a new Access Token T2, the Administrator

can seamlessly perform authorized operations on the previously created group G.

4. 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 [RFC9200].

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 [RFC9147] 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 document.

In order to specify authorization information for Administrators, the format and encoding of scope defined in Section 3 of this document MUST be used, for both the 'scope' claim in the Access Token, as well as for the 'scope' parameter in the Authorization Request and Authorization Response exchanged with the AS (see Sections 5.8.1 and 5.8.2 of [RFC9200]).

Furthermore, the AS MAY use the extended format of scope defined in Section 7 of [I-D.ietf-ace-key-groupcomm] for the 'scope' claim of the Access Token. In such a case, the AS MUST use the CBOR tag with tag number TAG_NUMBER, associated with the CoAP Content-Format CF_ID for the media type application/aif+cbor registered in Section 16.9 of [I-D.ietf-ace-key-groupcomm-oscore].

Note to RFC Editor: In the previous paragraph, please replace "TAG_NUMBER" with the CBOR tag number computed as TN(ct) in Section 4.3 of [RFC9277], where ct is the ID assigned to the CoAP Content-Format CF_ID registered in Section 16.9 of [I-D.ietf-ace-key-groupcomm-oscore]. Then, please replace "CF_ID" with the ID assigned to that CoAP Content-Format. Finally, please delete this paragraph.

This indicates that the binary encoded scope, as conveying the actual access control information, follows the scope semantics of the AIF specific data model AIF-OSCORE-GROUPCOMM defined in Section 3 of [I-D.ietf-ace-key-groupcomm-oscore] and extended as per Section 3 of this document.

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. To this end, the Administrator sends to the AS an Authorization Request as defined in Section 5.8.1 of [RFC9200].

   If the 'scope' parameter in the Authorization Request includes scope entries whose "Toid" specifies a complex pattern (see Section 3), then all such scope entries MUST adhere to the same pattern semantics.

   The Administrator will start or continue using a secure communication association with the Group Manager, according to the response from the AS and the specifically used transport profile of ACE.

2. The AS processes the Authorization Request as defined in Section 5.8.2 of [RFC9200], especially verifying that the Administrator is authorized to obtain the requested permissions, or possibly a subset of those.

   The AS specifies the information on the authorization granted to the Administrator as the value of the 'scope' claim to include in the Access Token, in accordance with the scope format specified in Section 3. It is implementation specific which particular approach the AS takes to evaluate the requested permissions against the access policies pertaining to the Administrator for the Group Manager in question. Appendix A provides an example of such an approach that the AS can use.

   If the 'scope' parameter in the Authorization Request includes scope entries whose "Toid" specifies a complex pattern adhering to a certain pattern semantics, then that semantics MUST be used for all the scope entries in the 'scope' claim that specify a complex pattern.

   The AS MUST include the 'scope' parameter in the Authorization Response defined in Section 5.8.2 of [RFC9200], when the value included in the Access Token differs from the one specified by the Administrator in the Authorization Request. In such a case, scope specifies the set of permissions that the Administrator actually has to perform operations at the Group Manager, encoded as specified in Section 3.

   If the 'scope' parameter in the Authorization Request includes scope entries whose "Toid" specifies a complex pattern and any of the following conditions holds, then the AS MUST reply with

a 4.00 (Bad Request) error response (see Section 5.8.3 of [RFC9200]). The 'error_description' parameter carried out in the response payload MUST specify the CBOR value 1 (invalid_scope).

- The "Toid" of the different scope entries that specify a complex pattern do not all adhere to the same pattern semantics.

- The "Toid" of the different scope entries that specify a complex pattern adhere to the same pattern semantics, but this is not supported by the AS or by the Group Manager.

Finally, as discussed in Section 3, the authorization information included in the Authorization Request or specified by the AS might also include permissions for the same Client as a user of an OSCORE group, i.e., as an actual group member or an external signature verifier. As per Section 3, such authorization information is expressed by "user scope entries", whose format and processing is specified in [I-D.ietf-ace-key-groupcomm-oscore].

3. 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 [RFC9202] and [RFC9203]. After that, the Administrator must have a secure communication association established with the Group Manager, before performing any administrative operation on that Group Manager. Possible ways to provide secure communication are DTLS [RFC9147] and OSCORE [RFC8613]. The Administrator and the Group Manager maintain the secure association, to support possible future communications.

4. Consistently with what is allowed by the authorization information in the Access Token, the Administrator performs administrative operations at the Group Manager, as described in Section 6. These include retrieving a list of existing OSCORE groups, creating new OSCORE groups, retrieving and changing OSCORE group configurations, and removing OSCORE groups. Messages exchanged among the Administrator and the Group Manager are specified in Section 6.

   Upon receiving a request from the Administrator targeting the group-configuration resource or a group-collection resource, the Group Manager MUST check that it is storing a valid Access Token for that Administrator. If this is not the case, the Group Manager MUST reply with a 4.01 (Unauthorized) error response.

If the request targets the group-configuration resource associated with a group with name GROUPNAME, the Group Manager MUST check that it is storing a valid Access Token from that Administrator, such that the 'scope' claim specified in the Access Token: i) expresses authorization information through scope entries as defined in Section 3; and ii) specifically includes a scope entry where:

- The group name GROUPNAME matches with the pattern specified by the "Toid" of the scope entry; and

- The permission set specified by the "Tperm" of the scope entry allows the Administrator to perform the requested administrative operation on the targeted group-configuration resource.

Note that the checks defined above only consider scope entries expressing permissions for administrative operations, namely "admin scope entries" as defined in Section 3, while the alternative "user scope entries" defined in [I-D.ietf-ace-key-groupcomm-oscore] are not considered.

Further detailed checks to perform are defined separately for each operation at the Group Manager, when specified in Section 6.

In case the Group Manager stores a valid Access Token but the verifications above fail, the Group Manager MUST reply with a 4.03 (Forbidden) error response. This response MAY be an AS Request Creation Hints, as defined in Section 5.3 of [RFC9200], in which case the Content-Format MUST be set to application/ace+cbor.

If the request is not formatted correctly (e.g., required fields are not present or are not encoded as expected), the Group Manager MUST reply with a 4.00 (Bad Request) error response.

4.1. Multiple Administrators for the Same OSCORE Group

In addition to a "main" primary Administrator responsible for an OSCORE group at the Group Manager, it is also possible to have "assistant" secondary Administrators that are effectively authorized to perform some operations on the same OSCORE group.

With respect to the main Administrator, such assistant Administrators are expected to have less permissions to perform administrative operations related to the OSCORE group at the Group Manager. For example, they may not be authorized to create the

OSCORE group if not existing already, or to delete the OSCORE group and its configuration.

In case the main Administrator of an OSCORE group is dismissed or relinquishes its role, one of the assistant Administrators can be "promoted" and become main Administrator for that OSCORE group. Practically, this requires that the access policies associated with the promoted Administrator are updated accordingly at the Authorization Server. Also, the promoted Administrator has to request from the Authorization Server a new Access Token and to upload it to the Group Manager. If allowed by the used transport profile of ACE, this process can efficiently enforce a dynamic update of access rights, thus preserving the current secure association between the promoted Administrator and the Group Manager.

If an Administrator is not sure about being the only Administrator responsible for an OSCORE group, then it is RECOMMENDED that the Administrator ensures to have a recent representation of the group-configuration resource associated with the OSCORE group before overwriting (see Section 6.6), updating (see Section 6.7), or deleting (see Section 6.8) the group configuration. This can be achieved in the following ways.

* The Administrator performs a regular polling of the group configuration, by sending a GET request to the corresponding group-configuration resource (see Section 6.4).

* If the group-configuration resource associated with the OSCORE group is Observable, then the Administrator subscribes to that resource by using CoAP Observe [RFC7641]. The Observation request is a GET request sent to the group-configuration resource (see Section 6.4). In such a case, the Group Manager will also send a 4.04 (Not Found) response in case another Administrator deletes the group-configuration resource, as a result of deleting the associated OSCORE group and its configuration.

If the Administrator gains knowledge that the group configuration has changed compared to the latest known representation, then the Administrator might hold the execution of writing or deletion operation on the group-configuration resource, and first attempt checking with other Administrators responsible for the same OSCORE group about the changes they have made.

5. Group Configurations

A group configuration consists of a set of parameters.

5.1. Group Configuration Representation

The group configuration representation is a CBOR map, which includes configuration properties and status properties.

5.1.1. Configuration Properties

The CBOR map includes the following configuration parameters, whose CBOR abbreviations are defined in Section 7 of this document.

* 'hkdf', which specifies the HKDF Algorithm used in the OSCORE group (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR text string or a CBOR integer. Possible values are the same ones admitted for the 'hkdf' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'cred_fmt', which specifies the Authentication Credential Format used in the OSCORE group (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR integer. Possible values are the same ones admitted for the 'cred_fmt' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'group_mode', encoded as a CBOR simple value. Its value is "true" (0xf5) if the OSCORE group uses the group mode of Group OSCORE (see Section 8 of [I-D.ietf-core-oscore-groupcomm]), or "false" (0xf4) otherwise.

* 'gp_enc_alg', which is formatted as follows. If the configuration parameter 'group_mode' has value "false" (0xf4), this parameter has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the Group Encryption Algorithm used in the OSCORE group to encrypt messages protected with the group mode (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR text string or a CBOR integer. Possible values are the same ones admitted for the 'sign_enc_alg' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

  Editor's note: as per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document and consistently with the naming used in the latest version of [I-D.ietf-core-oscore-groupcomm].

* 'sign_alg', which is formatted as follows. If the configuration parameter 'group_mode' has value "false" (0xf4), this parameter

has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the Signature Algorithm used in the OSCORE group (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR text string or a CBOR integer. Possible values are the same ones admitted for the 'sign_alg' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'sign_params', which is formatted as follows. If the configuration parameter 'group_mode' has value "false" (0xf4), this parameter has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the additional parameters for the Signature Algorithm used in the OSCORE group, encoded as a CBOR array. Possible formats and values are the same ones admitted for the 'sign_params' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'pairwise_mode', encoded as a CBOR simple value. Its value is "true" (0xf5) if the OSCORE group uses the pairwise mode of Group OSCORE (see Section 9 of [I-D.ietf-core-oscore-groupcomm]), or "false" (0xf4) otherwise.

* 'alg', which is formatted as follows. If the configuration parameter 'pairwise_mode' has value "false" (0xf4), this parameter has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the AEAD Algorithm used in the OSCORE group to encrypt messages protected with the pairwise mode (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR text string or a CBOR integer. Possible values are the same ones admitted for the 'alg' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'ecdh_alg', which is formatted as follows. If the configuration parameter 'pairwise_mode' has value "false" (0xf4), this parameter has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the Pairwise Key Agreement Algorithm used in the OSCORE group (see Section 2 of [I-D.ietf-core-oscore-groupcomm]), encoded as a CBOR text string or a CBOR integer. Possible values are the same ones admitted for the 'ecdh_alg' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'ecdh_params', which is formatted as follows. If the configuration parameter 'pairwise_mode' has value "false" (0xf4), this parameter has as value the CBOR simple value "null" (0xf6). Otherwise, this parameter specifies the parameters for the

Pairwise Key Agreement Algorithm used in the OSCORE group, encoded as a CBOR array. Possible formats and values are the same ones admitted for the 'ecdh_params' parameter of the Group_OSCORE_Input_Material object, defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'det_req', encoded as a CBOR simple value. Its value is "true" (0xf5) if the OSCORE group uses deterministic requests as defined in [I-D.amsuess-core-cachable-oscore], or "false" (0xf4) otherwise. This parameter MUST NOT be present if the configuration parameter 'group_mode' has value "false" (0xf4).

* 'det_hash_alg', encoded as a CBOR integer or text string. If present, this parameter specifies the Hash Algorithm used in the OSCORE group when producing deterministic requests, as defined in [I-D.amsuess-core-cachable-oscore]. This parameter takes values from the "Value" column of the "COSE Algorithms" Registry [COSE.Algorithms].

  This parameter MUST NOT be present if the configuration parameter 'det_req' is not present or if it is present with value "false" (0xf4). If the configuration parameter 'det_req' is present with value "true" (0xf5) and 'det_hash_alg' is not present, the choice of the Hash Algorithm to use when producing deterministic requests is left to the Group Manager.

5.1.2. Status Properties

The CBOR map includes the following status parameters. Unless specified otherwise, these are defined in this document and their CBOR abbreviations are defined in Section 7.

* 'rt', with value the resource type "core.osc.gconf" associated with group-configuration resources, encoded as a CBOR text string.

* 'active', encoding the CBOR simple value "true" (0xf5) if the OSCORE group is currently active, or the CBOR simple value "false" (0xf4) otherwise.

* 'group_name', with value the group name of the OSCORE group encoded as a CBOR text string.

* 'group_title', with value either a human-readable description of the OSCORE group encoded as a CBOR text string, or the CBOR simple value "null" (0xf6) if no description is specified.

* 'ace_groupcomm_profile', defined in Section 4.3.1 of [I-D.ietf-ace-key-groupcomm], with value "coap_group_oscore_app"

defined in Section 16.5 of [I-D.ietf-ace-key-groupcomm-oscore] encoded as a CBOR integer.

* 'max_stale_sets', encoding a CBOR unsigned integer with value strictly greater than 1. With reference to Section 7.1 of [I-D.ietf-ace-key-groupcomm-oscore], this parameter specifies N, i.e., the maximum number of sets of stale OSCORE Sender IDs that the Group Manager stores for the group.

* 'exp', defined in Section 4.3.1 of [I-D.ietf-ace-key-groupcomm].

* 'gid_reuse', encoding the CBOR simple value "true" (0xf5) if, upon rekeying the OSCORE group, the Group Manager can reassign the values of the OSCORE Group ID used as OSCORE ID Context, as per Section 3.2.1.1 of [I-D.ietf-core-oscore-groupcomm] and Section 11 of [I-D.ietf-ace-key-groupcomm-oscore]. Otherwise, this parameter encodes the CBOR simple value "false" (0xf4).

* 'app_groups', with value a list of names of application groups, encoded as a CBOR array. Each element of the array is a CBOR text string, specifying the name of an application group using the OSCORE group as security group (see Section 2.1 of [I-D.ietf-core-groupcomm-bis]).

* 'joining_uri', with value the URI of the group-membership resource for joining the newly created OSCORE group as per Section 6.2 of [I-D.ietf-ace-key-groupcomm-oscore], encoded as a CBOR text string.

* 'group_policies', defined in Section 4.3.1 of [I-D.ietf-ace-key-groupcomm], and consistent with the format and content defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

* 'as_uri', with value the URI of the Authorization Server associated with 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 Sections 5 and 6 of [I-D.ietf-ace-key-groupcomm-oscore]).

5.2. Default Values

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

A possible reason for the Group Manager to consider default values different from those recommended in this section is to ensure that each of those are consistent with what the Group Manager supports,

e.g., in terms of signature algorithm and format of authentication credentials used in the OSCORE group.

This ensures that the Group Manager is able to perform the operations defined in [I-D.ietf-ace-key-groupcomm-oscore], as to its interactions with joining nodes and current group members for an OSCORE group (see Section 14 of [I-D.ietf-ace-key-groupcomm-oscore]).

5.2.1. Configuration Parameters

For each of the configuration parameters listed below, the Group Manager refers to the following pre-configured default value, if none is specified by the Administrator.

* For 'group_mode', the Group Manager SHOULD use the CBOR simple value "true" (0xf5).

* If 'group_mode' has value "true" (0xf5), the Group Manager SHOULD use the default values defined in Section 14.2 of [I-D.ietf-ace-key-groupcomm-oscore] as follows: the value of 'sign_enc_alg' for the parameter 'gp_enc_alg' defined in this document; the value of 'sign_alg' and 'sign_params' for the corresponding parameters defined in this document.

  Editor's note: as per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document and consistently with the naming used in the latest version of [I-D.ietf-core-oscore-groupcomm].

* If 'group_mode' has value "true" (0xf5), the Group Manager SHOULD use the CBOR simple value "false" (0xf4) for the parameter 'det_req'.

* If 'det_req' has value "true" (0xf5), the Group Manager SHOULD use SHA-256 (COSE algorithm encoding: -16) as default value for the parameter 'det_hash_alg'.

* For 'pairwise_mode', the Group Manager SHOULD use the CBOR simple value "true" (0xf5).

* If 'pairwise_mode' has value "true" (0xf5), the Group Manager SHOULD use the same default values defined in Section 14.3 of [I-D.ietf-ace-key-groupcomm-oscore] for the parameters 'alg', 'ecdh_alg', and 'ecdh_params'.

* For any other configuration parameter, the Group Manager SHOULD use the same default values defined in Section 14.1 of [I-D.ietf-ace-key-groupcomm-oscore].

5.2.2. Status Parameters

For each of the status parameters listed below, the Group Manager refers to the following pre-configured default value, if none is specified by the Administrator.

* For 'active', the Group Manager SHOULD use the CBOR simple value "false" (0xf4).

* For 'group_title', the Group Manager SHOULD use the CBOR simple value "null" (0xf6).

* For 'max_stale_sets', the Group Manager SHOULD use the CBOR unsigned integer with value 3.

* For 'gid_reuse', the Group Manager SHOULD use the CBOR simple value "false" (0xf4).

* For 'app_groups', the Group Manager SHOULD use the empty CBOR array.

* For 'group_policies', the Group Manager SHOULD use the default values defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore].

6. Interactions with the Group Manager

This section describes the operations that are possible to perform on the group-collection resource and the group-configuration resources at the Group Manager.

For each operation, it is defined whether that operation is required or optional to support for the Group Manager and an Administrator. If the Group Manager supports an operation, then the Group Manager must be able to correctly handle authorized and valid requests sent by the Administrator to carry out that operation. If the Group Manager receives an authorized and valid request to perform an operation that it does not support, then the Group Manager MUST respond with a 5.01 (Not Implemented) response.

When checking the scope claim of a stored Access Token to verify that any of the requests defined in the following is authorized, the Group Manager only considers scope entries expressing permissions for administrative operations, namely "admin scope entries" as defined in Section 3. Instead, the alternative "user scope entries" defined in [I-D.ietf-ace-key-groupcomm-oscore] are not considered.

That is, when handling any of the requests for administrative operations defined in the following, the Group Manager ignores possible "user scope entries" specified in the scope of a stored access token.

The Content-Format in messages containing a payload is set to application/ace-groupcomm+cbor, defined in Section 11.2 of [I-D.ietf-ace-key-groupcomm]. Furthermore, the entry labels defined in Section 7 of this document MUST be used, when specifying the corresponding configuration and status parameters.

6.1. Retrieve the Full List of Group Configurations

This operation MUST be supported by the Group Manager and an Administrator.

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

The Group Manager MUST prepare the list L to include in the response as follows. For each group-configuration resource R:

1. The Group Manager considers the group name GROUPNAME of the OSCORE group associated with R.

2. The Group Manager retrieves the stored Access Token for the Administrator. Then, it checks whether GROUPNAME matches with the group name pattern specified in any scope entry of the 'scope' claim in the Access Token.

3. The link to the group-configuration resource R is added to the list L only in case of a positive match.

An example of message exchange is shown below.

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

<= 2.05 Content
   Content-Format: 40 (application/link-format)

   Payload:

   <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"
```

6.2. Retrieve a List of Group Configurations by Filters

This operation MUST be supported by the Group Manager and MAY be supported by an Administrator.

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

The filter criteria are specified in the request payload as a CBOR map, whose possible entries are specified in Section 5.1 and use the same abbreviations defined in Section 7. Entry values are the ones admitted for the corresponding labels in the POST request for creating a group configuration (see Section 6.3). A valid request MUST NOT include the same entry multiple times.

The Group Manager MUST prepare the list L to include in the response as follows.

1. The Group Manager prepares a preliminary version of the list L, as specified in Section 6.1 for the processing of a GET request to the group-collection resource.

2. The Group Manager applies the filter criteria specified in the FETCH request to the list L from the previous step. The result is the list L to include in the response.

An example of message exchange is shown below.

```
=> 0.05 FETCH
   Uri-Path: manage
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
       "group_mode" : true,
       "gp_enc_alg" : 10,
             "hkdf" : 5
   }

<= 2.05 Content
   Content-Format: 40 (application/link-format)

   Payload:

   <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"
```

6.3. Create a New Group Configuration

This operation MUST be supported by the Group Manager and an Administrator.

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 MUST specify the intended group name GROUPNAME, and MAY specify the intended group title together with pieces of information concerning the group configuration.

The request payload is a CBOR map, whose possible entries are specified in Section 5.1 and use the same abbreviations defined in Section 7. In particular:

- The payload MAY include any of the configuration parameters defined in Section 5.1.1.

- The payload MUST include the status parameter 'group_name' defined in Section 5.1.2 and specifying the intended group name.

- The payload MAY include any of the status parameters 'active', 'group_title', 'max_stale_sets', 'exp', 'gid_reuse', 'app_groups', 'group_policies', and 'as_uri' defined in Section 5.1.2.

- The payload MUST NOT include any of the status parameters 'rt', 'ace_groupcomm_profile', and 'joining_uri' defined in Section 5.1.2.

Consistently with what is defined at step 4 of Section 4, the Group Manager MUST check whether the group name specified in the 'group_name' parameter matches with the group name pattern specified in any scope entry of the 'scope' claim in the stored Access Token for the Administrator. In case of a positive match, the Group Manager MUST check whether the permission set in the found scope entry specifies the permission "Create".

If the verification above fails (i.e., there are no matching scope entries specifying the "Create" permission), the Group Manager MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm].

If the group configuration to be created would include parameter values that prevent the Group Manager from performing the operations defined in [I-D.ietf-ace-key-groupcomm-oscore] (e.g., due to the Group Manager not supporting a format of authentication credentials), the Group Manager MUST respond with a 5.03 (Service Unavailable) response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 12 ("Unsupported group configuration") and the 'error_description' parameter SHOULD be included in order to provide additional context.

Otherwise, if any of the following occurs, the Group Manager MUST respond with a 4.00 (Bad Request) response.

- Any of the received parameters is specified multiple times.

- Any of the received parameters is not recognized, or not valid, or not consistent with respect to other related parameters.

- 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 POST request, the Group Manager performs the following actions.

If the 'group_name' parameter specifies the group name of an already existing OSCORE group, the Group Manager MUST find an alternative name for the new OSCORE group to create.

In addition to that, the final decision about the name assigned to the new OSCORE group is always of the Group Manager, which may have more constraints than the Administrator can be aware of, possibly beyond the availability of suggested names. For example, the Group

Manager may specifically want to use a randomized character string as the name of a newly created group.

If the Group Manager has selected a name GROUPNAME different from the name GROUPNAME* indicated in the parameter 'group_name' of the request, then the following conditions MUST hold.

- The chosen name GROUPNAME is available to assign; and

- If GROUPNAME* matches with the group name pattern of certain scope entries from the 'scope' claim in the stored Access Token for the Administrator, then the chosen group name GROUPNAME also matches with each of those group name patterns.

If the Group Manager does not find any group name for which both the above conditions hold, the Group Manager MUST respond with a 5.03 (Service Unavailable) response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 11 ("No available group names").

Otherwise, the Group Manager creates a new group-configuration resource, accessible to the Administrator at /manage/GROUPNAME, where GROUPNAME is the name of the OSCORE group as either indicated in the parameter 'group_name' of the request or uniquely assigned by the Group Manager. The group-collection resource is also accordingly updated.

The operation of creating the new group-configuration resource and accordingly updating the group-collection resource MUST be atomic.

The value of the status parameter 'rt' is set to "core.osc.gconf". The values of other parameters specified in the request are used as group configuration information for the newly created OSCORE group.

If the request specifies the parameter 'gid_reuse' encoding the CBOR simple value "true" (0xf5) and the Group Manager does not support the reassignment of OSCORE Group ID values (see Section 3.2.1.1 of [I-D.ietf-core-oscore-groupcomm] and Section 11 of [I-D.ietf-ace-key-groupcomm-oscore]), then the Group Manager sets the value of the 'gid_reuse' status parameter in the group-configuration resource to the CBOR simple value "false" (0xf4).

For each parameter not specified in the request, the Group Manager refers to the default values specified in Section 5.2.

After that, the Group Manager creates a new group-membership resource accessible at ace-group/GROUPNAME to nodes that want to join the OSCORE group, as specified in Section 6.1 of [I-D.ietf-ace-key-groupcomm-oscore]. Note that such group

membership-resource comprises a number of sub-resources intended to current group members, as defined in Section 4.1 of [I-D.ietf-ace-key-groupcomm] and Section 8 of [I-D.ietf-ace-key-groupcomm-oscore].

From then on, the Group Manager will rely on the current group configuration to build the Join Response message defined in Section 6.3 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.

*The OSCORE Master Secret.

*The OSCORE Master Salt (optionally).

*The Group ID, used as OSCORE ID Context, 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 specifies the parameters 'group_name', 'joining_uri', and 'as_uri', from the status properties of the newly created OSCORE group (see Section 5.1), as detailed below.

The response payload is a CBOR map, where entries use the same abbreviations defined in Section 7.

*'group_name', with value the group name of the OSCORE group. 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. This parameter MUST be included.

*'joining_uri', with value the URI of the group-membership resource for joining the newly created OSCORE group. This parameter MUST be included.

*'as_uri', with value the URI of the Authorization Server associated with the Group Manager for the newly created OSCORE group. This parameter MUST be included. Its 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.

If the POST request specified the parameter 'gid_reuse' encoding the CBOR simple value "true" (0xf5) but the Group Manager has set the value of the 'gid_reuse' status parameter in the group-configuration resource to the CBOR simple value "false" (0xf4), then the response payload MUST include also the parameter 'gid_reuse' encoding the CBOR simple value "false" (0xf4).

If the POST request did not specify certain parameters and the Group Manager used default values different from the ones recommended in Section 5.2, then the response payload MUST include also those parameters, specifying the values chosen by the Group Manager for the current group configuration.

The Group Manager can register the link to the group-membership resource with URI specified in 'joining_uri' to a Resource Directory [RFC9176], as defined in Section 2 of [I-D.tiloca-core-oscore-discovery]. The Group Manager considers the current group configuration when specifying additional information for the link to register.

Alternatively, the Administrator can perform the registration in 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.

* The name of the OSCORE group MUST take the value specified in 'group_name' from the 2.01 (Created) response.

* The names of the application groups using the OSCORE group MUST take the values possibly specified by the elements of the 'app_groups' parameter in the POST request.

* If also registering a related link to the Authorization Server associated with the OSCORE group, the related link MUST have as link target the URI in 'as_uri' from the 2.01 (Created) response.

* As to every other information element describing the current group configuration, the following applies.

  - If a certain parameter was specified in the POST request, the Administrator MUST use either the value specified in the 2.01 (Created) response, if the Group Manager specified one, or the value specified in the POST request otherwise.

  - If a certain parameter was not specified in the POST request, the Administrator MUST use either the value specified in the 2.01 (Created) response, if the Group Manager specified one, or the corresponding default value recommended in Section 5.2.1 otherwise.

Note that, compared to the Group Manager, the Administrator is less likely to remain closely aligned with possible changes and updates that would require a prompt update to the registration in the Resource Directory. This applies especially to the address of the Group Manager, as well as the URI of the group-membership resource or of the Authorization Server associated with the Group Manager.

Therefore, it is RECOMMENDED that registrations of links to group-membership resources in the Resource Directory are made (and possibly updated) directly by the Group Manager, rather than by the Administrator.

An example of message exchange is shown below.

```
=> 0.02 POST
   Uri-Path: manage
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
        "gp_enc_alg" : 10,
             "hkdf" : 5,
     "pairwise_mode" : true,
           "active" : true,
       "group_name" : "gp4",
      "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: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
      "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
         "as_uri" : "coap://as.example.com/token"
   }
```

6.4. Retrieve a Group Configuration

This operation MUST be supported by the Group Manager and an Administrator.

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

Consistently with what is defined at step 4 of Section 4, the Group Manager MUST check whether GROUPNAME matches with the group name pattern specified in any scope entry of the 'scope' claim in the stored Access Token for the Administrator. In case of a positive match, the Group Manager MUST check whether the permission set in the found scope entry specifies the permission "Read".

If the verification above fails (i.e., there are no matching scope entries specifying the "Read" permission), the Group Manager MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm].

Otherwise, after a successful processing of the GET request, 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 5.1. The exact content of the payload reflects the current configuration of the OSCORE group. This includes both configuration properties and status properties.

The response payload is a CBOR map, whose possible entries are specified in Section 5.1 and use the same abbreviations defined in Section 7.

An example of message exchange is shown below.

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

<= 2.05 Content
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
                      "hkdf" : 5,
                  "cred_fmt" : 33,
                "group_mode" : true,
                "gp_enc_alg" : 10,
                  "sign_alg" : -8,
              "sign_params" : [[1], [1, 6]],
            "pairwise_mode" : true,
                      "alg" : 10,
                 "ecdh_alg" : -27,
              "ecdh_params" : [[1], [1, 6]],
                  "det_req" : false,
                       "rt" : "core.osc.gconf",
                   "active" : true,
                "group_name" : "gp4",
              "group_title" : "rooms 1 and 2",
    "ace_groupcomm_profile" : "coap_group_oscore_app",
          "max_stale_sets" : 3,
                      "exp" : 1360289224,
               "gid_reuse" : false,
                "app_groups" : ["room1", "room2"],
              "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
                  "as_uri" : "coap://as.example.com/token"
   }
```

6.5. Retrieve Part of a Group Configuration by Filters

This operation MUST be supported by the Group Manager and MAY be supported by an Administrator.

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

The request payload is a CBOR map, which contains the following field:

* 'conf_filter', encoded as a CBOR array. Each element of the array specifies one requested configuration parameter or status parameter of the current group configuration (see Section 5.1),

encoded with the corresponding CBOR abbreviation defined in Section 7.

The Group Manager MUST perform the same authorization checks defined for the processing of a GET request to a group-configuration resource in Section 6.4. That is, the Group Manager MUST verify that the Administrator has been granted a "Read" permission applicable to the targeted group-configuration resource.

After a successful processing of the FETCH request, the Group Manager replies to the Administrator with a 2.05 (Content) response. The response has as payload a partial representation of the group configuration (see Section 5.1). The exact content of the payload reflects the current configuration of the OSCORE group, and is limited to the configuration properties and status properties requested by the Administrator in the FETCH request.

The response payload includes the requested configuration parameters and status parameters, and is formatted as in the response payload of a GET request to a group-configuration resource (see Section 6.4). If the request payload specifies a parameter that is not included in the group configuration, then the response payload MUST NOT include a corresponding parameter.

An example of message exchange is shown below.

```
=> 0.05 FETCH
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
     "conf_filter" : ["gp_enc_alg",
                      "hkdf",
                      "pairwise_mode",
                      "active",
                      "group_title",
                      "app_groups"]
   }

<= 2.05 Content
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
        "gp_enc_alg" : 10,
              "hkdf" : 5,
     "pairwise_mode" : true,
           "active" : true,
       "group_title" : "rooms 1 and 2",
        "app_groups" : ["room1", "room2"]
   }
```

6.6. Overwrite a Group Configuration

This operation MAY be supported by the Group Manager and an Administrator.

The Administrator can send a PUT request to the group-configuration resource manage/GROUPNAME associated with an OSCORE group with group name GROUPNAME, in order to overwrite the current configuration of that group with a new one.

The payload of the request has the same format of the POST request defined in Section 6.3, with the exception that the configuration parameters 'group_mode' and 'pairwise_mode' as well as the status parameters 'group_name' and 'gid_reuse' MUST NOT be included.

The error handling for the PUT request is the same as for the POST request defined in Section 6.3, with the following difference in terms of authorization checks.

Consistently with what is defined at step 4 of Section 4, the Group Manager MUST check whether GROUPNAME matches with the group name pattern specified in any scope entry of the 'scope' claim in the stored Access Token for the Administrator. In case of a positive match, the Group Manager MUST check whether the permission set in the found scope entry specifies the permission "Write".

If the verification above fails (i.e., there are no matching scope entries specifying the "Write" permission), the Group Manager MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm].

If the updated group configuration would include parameter values that prevent the Group Manager from performing the operations defined in [I-D.ietf-ace-key-groupcomm-oscore] (e.g., due to the Group Manager not supporting a format of authentication credentials), the Group Manager MUST respond with a 5.03 (Service Unavailable) response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 12 ("Unsupported group configuration") and the 'error_description' parameter SHOULD be included in order to provide additional context.

If no error occurs and the PUT request is successfully processed, the Group Manager performs the following actions.

First, the Group Manager updates the group-configuration resource, consistently with the values indicated in the PUT request from the Administrator. For each parameter not specified in the PUT request, the Group Manager MUST use default values as specified in Section 5.2. The corresponding group-membership resource is also accordingly updated.

The operation of overwriting the group-configuration resource and accordingly updating the group-membership resource MUST be atomic.

If a new value N' is specified for the 'max_stale_sets' status parameter and N' is smaller than the current value N, the Group Manager preserves the (up to) N' most recent sets of stale OSCORE Sender IDs associated with the group, and deletes any possible older set (see Section 7.1 of [I-D.ietf-ace-key-groupcomm-oscore]).

From then on, the Group Manager relies on the latest updated configuration to build the Join Response message defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore], when handling the joining of a new group member. Similarly, the Group Manager

relies on the new group configuration when building responses specifying (part of) the group configuration to a current group member. For instance, this applies when a group member retrieves from the Group Manager the updated group keying material (see Section 9.1 of [I-D.ietf-ace-key-groupcomm-oscore]) or the current group status (see Section 9.9 of [I-D.ietf-ace-key-groupcomm-oscore]).

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 6.3.

If the PUT request did not specify certain parameters and the Group Manager used default values different from the ones recommended in Section 5.2, then the response payload MUST include also those parameters, specifying the values chosen by the Group Manager for the current group configuration.

If the link to the group-membership resource was registered in the Resource Directory [RFC9176], the Group Manager 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 in 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.

* The name of the OSCORE group MUST take the value specified in 'group_name' from the 2.04 (Changed) response.

* The names of the application groups using the OSCORE group MUST take the values possibly specified by the elements of the 'app_groups' parameter in the PUT request.

* If also registering a related link to the Authorization Server associated with the OSCORE group, the related link MUST have as link target the URI in 'as_uri' from the 2.04 (Changed) response.

* As to every other information element describing the current group configuration, the following applies.

  - If a certain parameter was specified in the PUT request, the Administrator MUST use either the value specified in the 2.04 (Changed) response, if the Group Manager specified one, or the value specified in the PUT request otherwise.

  - If a certain parameter was not specified in the PUT request, the Administrator MUST use either the value specified in the 2.04 (Changed) response, if the Group Manager specified one,

or the corresponding default value recommended in Section 5.2.1 otherwise.

As discussed in Section 6.3, it is RECOMMENDED that registrations of links to group-membership resources in the Resource Directory are made (and possibly updated) directly by the Group Manager, rather than by the Administrator.

An example of message exchange is shown below.

```
=> 0.03 PUT
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
       "gp_enc_alg" : 11,
            "hkdf" : 5
   }

<= 2.04 Changed
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
      "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
         "as_uri" : "coap://as.example.com/token"
   }
```

6.6.1. Effects on Joining Nodes

After having overwritten a group configuration, if the value of the status parameter 'active' is changed from "true" (0xf5) to "false" (0xf4), the Group Manager MUST stop admitting new members in the OSCORE group. In particular, until the status parameter 'active' is changed back to "true" (0xf5), the Group Manager MUST respond to a Join Request with a 5.03 (Service Unavailable) response, as defined in Section 6.2 of [I-D.ietf-ace-key-groupcomm-oscore].

If the value of the status parameter 'active' is changed from "false" (0xf4) to "true" (0xf5), the Group Manager resumes admitting new members in the OSCORE group, by processing their Join Requests (see Section 6.2 of [I-D.ietf-ace-key-groupcomm-oscore]).

6.6.2. Effects on the Group Members

After having overwritten a group configuration, the Group Manager informs the members of the OSCORE group, over the pairwise secure communication channels established when joining the group (see Section 6 of [I-D.ietf-ace-key-groupcomm-oscore]).

To this end, the Group Manager can individually target the 'control_uri' URI of each group member (see Section 4.3.1 of [I-D.ietf-ace-key-groupcomm]), if provided by the intended recipient upon joining the OSCORE group (see Section 6.1 of [I-D.ietf-ace-key-groupcomm-oscore]). Such messages sent by the Group Manager to each group member MUST have Content-Format set to application/ace-groupcomm+cbor, and MUST be formatted as the Join Response defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore], with the following differences.

* Only the parameters 'gkty', 'key', 'num', 'exp' and 'ace_groupcomm_profile' are present.

* The 'key' parameter includes only the following parameters, with values reflecting the new configuration of the OSCORE group.

  - 'hkdf' and 'cred_fmt'.

  - 'sign_enc_alg', 'sign_alg', and 'sign_params', only in case the configuration parameter 'group_mode' in the group-configuration resource has value "true" (0xf5), i.e., the OSCORE group uses the group mode of Group OSCORE.

    Editor's note: as per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document and consistently with the naming used in the latest version of [I-D.ietf-core-oscore-groupcomm].

  - 'alg', 'ecdh_alg', and 'ecdh_params', only in case the configuration parameter 'pairwise_mode' in the group-configuration resource has value "true" (0xf5), i.e., the OSCORE group uses the pairwise mode of Group OSCORE.

  - 'det_hash_alg' defined in Section 4 of [I-D.amsuess-core-cachable-oscore], only in case the configuration parameter 'det_req' is present with value "true" (0xf5), and specifying the Hash Algorithm used in the OSCORE group when producing deterministic requests, as defined in [I-D.amsuess-core-cachable-oscore].

Alternatively, group members can obtain the information above by accessing the group-membership resource associated with the OSCORE group (see Section 9.1 of [I-D.ietf-ace-key-groupcomm-oscore]), optionally by subscribing for updates to such a resource, e.g., by using CoAP Observe [RFC7641].

When receiving such information, each group member uses it to update the corresponding parameters in the Group OSCORE Security Context of the group in question (see Section 2 of [I-D.ietf-core-oscore-groupcomm]. If any of 'sign_enc_alg', 'sign_alg', 'alg', and 'ecdh_alg' has as value the CBOR simple value "null" (0xf6), then the corresponding parameter in the Group OSCORE Security Context becomes unset if it is not already. According to the new parameter values, each group member derives new Sender/ Recipient Keys, a new Common IV, and new Pairwise Keys. When doing so, a group member MUST NOT reset the Sender Sequence Number in its Sender Context or reset the Replay Window in its Recipient Contexts.

Editor's note: as per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document and consistently with the naming used in the latest version of [I-D.ietf-core-oscore-groupcomm].

The following holds when the value of specific parameters is updated.

* If the value of the status parameter 'active' is changed from "true" (0xf5) to "false" (0xf4):

  - The Group Manager MUST stop accepting requests for new individual keying material from current group members (see Section 9.2 of [I-D.ietf-ace-key-groupcomm-oscore]), until the status parameter 'active' is changed back to "true" (0xf5). Until then, the Group Manager MUST respond to a Key Renewal Request with a 5.03 (Service Unavailable) response, as defined in Section 9.2 of [I-D.ietf-ace-key-groupcomm-oscore].

  - The Group Manager MUST stop accepting updated authentication credentials uploaded by current group members (see Section 9.4 of [I-D.ietf-ace-key-groupcomm-oscore]), until the status parameter 'active' is changed back to "true" (0xf5). Until then, the Group Manager MUST respond to an Authentication Credential Update Request with a 5.03 (Service Unavailable) response, as defined in Section 9.4 of [I-D.ietf-ace-key-groupcomm-oscore].

*Every group member, upon learning that the OSCORE group has been deactivated (i.e., 'active' has value "false" (0xf4)), SHOULD stop communicating in the group.

Every group member, upon learning that the OSCORE group has been reactivated (i.e., 'active' has value "true" (0xf5) again), can resume communicating in the group.

*If the value of 'gp_enc_alg' and/or 'alg' is changed, the Group Manager determines the new maximum size NEW_MAX_SIZE that can be used for the OSCORE Sender IDs of the group members, based on the size of the AEAD nonce of such algorithms (see Section 2.2 of [I-D.ietf-core-oscore-groupcomm]). In case NEW_MAX_SIZE is strictly smaller than the old, maximum size of the OSCORE Sender IDs used in the OSCORE group, the Group Manager MUST proceed as follows.

  -The Group Manager checks if any of the current group members has an OSCORE Sender ID whose size is strictly larger than NEW_MAX_SIZE.

  -If any of such group members is found, the Group Manager MUST evict them from the OSCORE group. That is, the Group Manager MUST terminate their membership and MUST rekey the group in such a way that the new keying material is not provided to those evicted members. This also includes adding their relinquished Sender IDs to the most recent set of stale Sender IDs for the OSCORE group (see Section 7.1 of [I-D.ietf-ace-key-groupcomm-oscore]), before rekeying the group. Such evicted group members can rejoin the OSCORE group, thus obtaining the new group keying material together with a new, valid OSCORE Sender ID.

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

  -Leave the OSCORE group (see Section 9.11 of [I-D.ietf-ace-key-groupcomm-oscore]), e.g., if not supporting the indicated new algorithms; or

  -Remain in the OSCORE group and use the Group OSCORE Security Context after having updated it as defined above.

Editor's note: as per the text above, the referred version of [I-D.ietf-ace-key-groupcomm-oscore] still uses 'sign_enc_alg' as parameter name. The next version of [I-D.ietf-ace-key-groupcomm-oscore] will be updated in order to use 'gp_enc_alg' instead, as already done for this document and consistently with the naming used in the latest version of [I-D.ietf-core-oscore-groupcomm].

*Every group member, upon receiving updated values for 'cred_fmt', 'sign_alg', 'sign_params', 'ecdh_alg', and 'ecdh_params' MUST either:

- Leave the OSCORE group, e.g., if not supporting the indicated new format, algorithms, parameters and encoding; or

- Leave the OSCORE group and rejoin it (see Section 6 of [I-D.ietf-ace-key-groupcomm-oscore]). When rejoining the group, an authentication credential in the indicated format used in the OSCORE group MUST be provided to the Group Manager. The authentication credential as well as the included public key MUST be compatible with the indicated algorithms and parameters.

- Remain in the OSCORE group and use the Group OSCORE Security Context after having updated it as defined above, and, if required, perform the following actions.

  - Provide the Group Manager with a new authentication credential to use in the OSCORE group (see Section 9.4 of [I-D.ietf-ace-key-groupcomm-oscore]). The new authentication credential MUST be in the indicated format used in the OSCORE group. The new authentication credential as well as the included public key MUST be compatible with the indicated algorithms and parameters.

    Consistently, the group member has to retrieve the new authentication credentials of other group members as they are uploaded to the Group Manager (see Section 9.3 of [I-D.ietf-ace-key-groupcomm-oscore]). In order to ensure the retrieval of latest authentication credentials that are consistent with the new group configuration, it is preferable that the group member retrieves such authentication credentials after a pre-configured time interval has elapsed since uploading its own authentication credential. Later on, the group member will need to retrieve other group members' authentication credentials that it is still missing and that it needs for processing messages exchanged in the OSCORE group.

  - Retrieve from the Group Manager the new Group Manager's authentication credential (see Section 9.5 of [I-D.ietf-ace-key-groupcomm-oscore]). The new Group Manager's authentication credential is in the indicated format used in the OSCORE group. The new authentication credential as well as the included public key are compatible with the indicated algorithms and parameters.

6.7. Selective Update of a Group Configuration

This operation MAY be supported by the Group Manager and an Administrator.

The Administrator can send a PATCH/iPATCH request [RFC8132] to the group-configuration resource manage/GROUPNAME associated with an OSCORE group with group name GROUPNAME, in order to update the value of only part of the group configuration.

The request payload has the same format of the PUT request defined in Section 6.6, with the difference that it MAY also specify names of application groups to be removed from or added to the 'app_groups' status parameter. The names of such application groups are provided as defined below.

The CBOR map in the request payload includes the field 'app_groups_diff', whose CBOR abbreviation is defined in Section 7. This field is encoded as a CBOR array including the following two elements.

- The first element is a CBOR array, namely 'app_groups_del'. Each of its elements is a CBOR text string, with value the name of an application group to remove from the 'app_groups' status parameter.

- The second element is a CBOR array, namely 'app_groups_add'. Each of its elements is a CBOR text string, with value the name of an application group to add to the 'app_groups' status parameter.

The CDDL definition [RFC8610] of the CBOR array 'app_groups_diff' formatted as in the response from the Group Manager is provided below.

```
app-group-name = tstr
name-patch = [* app-group-name]
app_groups_diff = [app_groups_del: name-patch,
                   app_groups_add: name-patch]
```

Figure 3: CDDL definition of the 'app_groups_diff' field

The Group Manager MUST respond with a 4.00 (Bad Request) response in case: both the inner CBOR arrays 'app_groups_del' and 'app_groups_add' are empty; or the CBOR map in the request payload includes both the 'app_groups' field and the 'app_groups_diff' field.

The error handling for the PATCH/iPATCH request is the same as for the PUT request defined in Section 6.6, with the following additions.

- The set of group configuration parameters to update MUST NOT be empty. That is, the Group Manager MUST respond with a 4.00 (Bad Request) response, if the request payload includes an empty CBOR map.

- If the Request-URI does not point to an existing group-configuration resource, the Group Manager MUST NOT create a new resource, and MUST respond with a 4.04 (Not Found) response.

- When applying the specified updated values would yield an inconsistent group configuration, the Group Manager MUST respond with a 4.09 (Conflict) response.

  The response, MAY include the current representation of the group configuration resource, like when responding to a GET request as defined in Section 6.4. Otherwise, the response SHOULD include a diagnostic payload with additional information for the Administrator to recognize the source of the conflict.

- When the request uses specifically the iPATCH method, the Group Manager MUST respond with a 4.00 (Bad Request) response, in case the CBOR map includes the parameter 'app_groups_diff'.

Furthermore, the Group Manager MUST perform the same authorization checks defined for the processing of a PUT request to a group-configuration resource in Section 6.6. That is, the Group Manager MUST verify that the Administrator has been granted a "Write" permission applicable to the targeted group-configuration resource.

If the updated group configuration would include parameter values that prevent the Group Manager from performing the operations defined in [I-D.ietf-ace-key-groupcomm-oscore] (e.g., due to the Group Manager not supporting a format of authentication credentials), the Group Manager MUST respond with a 5.03 (Service Unavailable) response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 12 ("Unsupported group configuration") and the 'error_description' parameter SHOULD be included in order to provide additional context.

If no error occurs and the PATCH/iPATCH request is successfully processed, the Group Manager performs the following actions.

First, the Group Manager updates the group-configuration resource, consistently with the values indicated in the PATCH/iPATCH request

from the Administrator. The corresponding group-membership resource is also accordingly updated.

The operation of updating the group-configuration resource and accordingly updating the group-membership resource MUST be atomic.

Unlike for the PUT request defined in Section 6.6, the Group Manager does not alter the value of configuration parameters and status parameters for which updated values are not specified in the request payload. In particular, the Group Manager does not assign possible default values to those parameters.

Special processing occurs when updating the 'app_groups' status parameter by difference, as defined below. The Administrator should not expect the Group Manager to add or delete names of application group names according to any particular order.

- If the name of an application group to add (delete) is specified multiple times, the Group Manager considers it only once for addition to (deletion from) the 'app_groups' status parameter.

- If the name of an application group to delete is not present in the 'app_groups' status parameter before any change is applied, the Group Manager ignores that name.

- If the name of an application group to add is already present in the 'app_groups' status parameter before any change is applied, the Group Manager ignores that name.

- The Group Manager deletes from the 'app_groups' status parameter the names of the application groups specified in the inner 'app_groups_del' CBOR array of the 'app_groups_diff' field.

- The Group Manager adds to the 'app_groups' status parameter the names of the application groups specified in the inner 'app_groups_add' CBOR array of the 'app_groups_diff' field.

After having updated the group-configuration resource, from then on the Group Manager relies on the new group configuration to build the Join Response message defined in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore], when handling the joining of a new group member. Similarly, the Group Manager relies on the new group configuration when building responses specifying (part of) the group configuration to a current group member. For instance, this applies when a group member retrieves from the Group Manager the updated group keying material (see Section 9.1 of [I-D.ietf-ace-key-groupcomm-oscore]) or the current group status (see Section 9.9 of [I-D.ietf-ace-key-groupcomm-oscore]).

Finally, 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 6.3.

The same considerations as for the PUT request defined in Section 6.6 hold also in this case, with respect to refreshing a possible registration of the link to the group-membership resource in the Resource Directory [RFC9176].

An example of message exchange is shown below.

```
=> 0.06 PATCH
   Uri-Path: manage
   Uri-Path: gp4
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
          "gp_enc_alg" : 10,
     "app_groups_diff" : [["room1"],
                          ["room3", "room4"]]
   }

<= 2.04 Changed
   Content-Format: CT_TBD (application/ace-groupcomm+cbor)

   Payload:

   {
      "group_name" : "gp4",
     "joining_uri" : "coap://[2001:db8::ab]/ace-group/gp4/",
          "as_uri" : "coap://as.example.com/token"
   }
```

6.7.1. Effects on Joining Nodes

After having selectively updated part of a group configuration, the effects on candidate joining nodes are the same as defined in Section 6.6.1 for the case of group configuration overwriting.

6.7.2. Effects on the Group Members

After having selectively updated part of a group configuration, the effects on the current group members are the same as defined in Section 6.6.2 for the case of group configuration overwriting.

6.8. Delete a Group Configuration

This operation MUST be supported by the Group Manager and an Administrator.

The Administrator can send a DELETE request to the group-configuration resource manage/GROUPNAME associated with an OSCORE group with group name GROUPNAME, in order to delete that OSCORE group.

Consistently with what is defined at step 4 of Section 4, the Group Manager MUST check whether GROUPNAME matches with the group name pattern specified in any scope entry of the 'scope' claim in the stored Access Token for the Administrator. In case of a positive match, the Group Manager MUST check whether the permission set in the found scope entry specifies the permission "Delete".

If the verification above fails (i.e., there are no matching scope entries specifying the "Delete" permission), the Group Manager MUST reply with a 4.03 (Forbidden) error response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm].

Otherwise, the Group Manager continues processing the request, which would be successful only on an inactive OSCORE group. That is, the DELETE request actually yields a successful deletion of the OSCORE group, only if the corresponding status parameter 'active' has current value "false" (0xf4). The Administrator can ensure that, by first performing an update of the group-configuration resource associated with the OSCORE group (see Section 6.6), and setting the corresponding status parameter 'active' to "false" (0xf4).

If, upon receiving the DELETE request, the current value of the status parameter 'active' is "true" (0xf5), the Group Manager MUST respond with a 4.09 (Conflict) response. The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 10 ("Group currently active").

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

First, the Group Manager deletes the OSCORE group, deallocates both the group-configuration resource as well as the group-membership resource associated with that group, and accordingly updates the group-collection resource.

The operation of deleting the group-configuration resource and the corresponding group-membership resource, as well as of accordingly updating the group-collection resource MUST be atomic.

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

An example of message exchange is shown below.

```
=> 0.04 DELETE
   Uri-Path: manage
   Uri-Path: gp4

<= 2.02 Deleted
```

6.8.1. Effects on the Group Members

After having deleted an OSCORE 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 association established with that member during its joining process (see Section 6 of [I-D.ietf-ace-key-groupcomm-oscore]).

- 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 11.1 of [I-D.ietf-ace-key-groupcomm-oscore]). The Group Manager uses the same format of the Join Response message in Section 6.3 of [I-D.ietf-ace-key-groupcomm-oscore], where only the parameters 'gkty', 'key' and 'ace_groupcomm_profile' are present, and the 'key' parameter is the empty CBOR map.

- A group member may subscribe for updates to the group-membership resource associated with the OSCORE 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 OSCORE group (see Section 6.1 of [I-D.ietf-ace-key-groupcomm]). The response MUST have Content-Format set to application/ace-groupcomm+cbor and is formatted as defined in Section 4.1.2 of [I-D.ietf-ace-key-groupcomm]. The value of the 'error' field MUST be set to 5 ("Group deleted").

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

7. ACE Groupcomm Parameters

In addition to what is defined in Section 8 of [I-D.ietf-ace-key-groupcomm], this document defines additional parameters used in the messages exchanged between the Administrator and the Group Manager (see Section 6). The table below summarizes them and specifies the CBOR key to use instead of the full descriptive name.

Note that the media type application/ace-groupcomm+cbor MUST be used when these parameters are transported in the respective message fields.

Name	CBOR Key	CBOR Type	Reference
hkdf	TBD	tstr / int	[RFC-XXXX]
cred_fmt	TBD	int	[RFC-XXXX]
group_mode	TBD	simple value	[RFC-XXXX]
gp_enc_alg	TBD	tstr / int / simple value	[RFC-XXXX]
sign_alg	TBD	tstr / int / simple value	[RFC-XXXX]
sign_params	TBD	array / simple value	[RFC-XXXX]
pairwise_mode	TBD	simple value	[RFC-XXXX]
alg	TBD	tstr / int / simple value	[RFC-XXXX]
ecdh_alg	TBD	tstr / int / simple value	[RFC-XXXX]
ecdh_params	TBD	array / simple value	[RFC-XXXX]
det_req	TBD	simple value	[RFC-XXXX]
det_hash_alg	TBD	tstr / int	[RFC-XXXX]
rt	TBD	tstr	[RFC-XXXX]
active	TBD	simple value	[RFC-XXXX]
group_name	TBD	tstr	[RFC-XXXX]
group_title	TBD	tstr / simple value	[RFC-XXXX]
max_stale_sets	TBD	uint	[RFC-XXXX]
gid_reuse	TBD	simple value	[RFC-XXXX]
app_groups	TBD	array	[RFC-XXXX]
joining_uri	TBD	tstr	[RFC-XXXX]

as_uri	TBD	tstr	[RFC-XXXX]
conf_filter	TBD	array	[RFC-XXXX]
app_groups_diff	TBD	array	[RFC-XXXX]

Figure 4: ACE Groupcomm Parameters

The following holds for the Group Manager.

* It MUST support the parameters 'error', 'error_description', 'ace_groupcomm_profile', 'exp' and 'group_policies', which are defined in Section 8 of [I-D.ietf-ace-key-groupcomm].

  This is consistent with what is defined in Section 8 of [I-D.ietf-ace-key-groupcomm] for the Key Distribution Center, of which the Group Manager defined in [I-D.ietf-ace-key-groupcomm-oscore] is a specific instance.

* It MUST support all the parameters listed in Figure 4, with the exception of the 'app_groups_diff' parameter, which MUST be supported only if the Group Manager supports the selective update of a group configuration (see Section 6.7).

The following holds for an Administrator.

* It MUST support the parameters 'error', 'error_description', 'ace_groupcomm_profile', 'exp' and 'group_policies', which are defined in Section 8 of [I-D.ietf-ace-key-groupcomm].

* It MUST support all the parameters listed in Figure 4, with the following exceptions.

  - 'conf_filter', which MUST be supported only if the Administrator supports the partial retrieval of a group configuration by filters (see Section 6.5).

  - 'app_groups_diff' parameter, which MUST be supported only if the Administrator supports the selective update of a group configuration (see Section 6.7).

8. ACE Groupcomm Error Identifiers

In addition to what is defined in Section 9 of [I-D.ietf-ace-key-groupcomm], this document defines a new value that the Group Manager can include as error identifiers, in the 'error' field of an error response with Content-Format application/ace-groupcomm+cbor.

Value	Description
10	Group currently active
11	No available group names
12	Unsupported group configuration

Figure 5: ACE Groupcomm Error Identifiers

When receiving an error response from the Group Manager, an Administrator may use the information conveyed in the 'error' parameter to determine what actions to take next. If it is included in the error response, the 'error_description' parameter may provide additional context. In particular, the following guidelines apply.

* In case of error 10, the Administrator should stop sending the DELETE request to the Group Manager (see Section 6.8), until the group becomes inactive. As per this document, this error is relevant only for the Administrator, if it tries to delete a group without having set its status to inactive first (see Section 6.8). In such a case, the Administrator should take the expected course of actions, and set the group status to inactive first (see Section 6.6 and Section 6.7), before sending a new request of group deletion to the Group Manager.

* In case of error 11, the Administrator has the following options.

  - The Administrator simply tries again later on. The new POST request to the group-collection resource specifies the same group name originally suggested in the previous request that triggered the error response (see Section 6.3). This option fundamentally relies on the Group Manager freeing up group names, hence it is not viable if considerably or indefinitely postponing the creation of the group is not acceptable.

  - The Administrator sends a new POST request to the group-collection resource right away, specifying a different group name than the one suggested in the previous request that triggered the error response. The new group name suggested by the Administrator should be such that the following holds.

    Let us define: i) S, as the set of all the scope entries in the Administrator's Access Token, such that the old group name matched with each of those scope entries; ii) S', as the set of all the scope entries in the Administrator's Access Token,

such that the new group name matches with each of those scope entries. Then, S' is neither equal to S nor a subset of S.

- The Administrator requests a new Access Token to the Authorization Server, in order to update its access rights, and have a new granted scope whose scope entries specify more and/or different group name patterns than the old Access Token.

  After uploading the new Access Token to the Group Manager, the Administrator can send a new POST request to the group-collection resource. When doing so, the Administrator suggests a new group name to the Group Manager, according to the same criteria discussed for the previous option.

* In case of error 12, the Administrator has the following options.

- If the Administrator has attempted to create a new group configuration (see Section 6.3), the Administrator can take into account what the Group Manager specifies in the 'error_description' parameter of the error response, and send a new request to the Group Manager for accordingly creating the group configuration.

  This requires that the Administrator finds acceptable to create a group configuration different from the originally intended one.

- If the Administrator has attempted to overwrite (see Section 6.6) or selectively update (see Section 6.7) an existing group configuration, the Administrator can take into account what the Group Manager specifies in the 'error_description' parameter of the error response, and send a new request to the Group Manager for accordingly overwriting or selectively updating the group configuration.

  This requires that the Administrator finds acceptable to overwrite or update the current group configuration differently than how it was originally intended. If this is not attainable, the Administrator may decide to not take further actions and keep the current group configuration as is, or instead to delete the group configuration altogether (see Section 6.8).

9. Security Considerations

Security considerations are inherited from the ACE framework for Authentication and Authorization [RFC9200], and from the specific transport profile of ACE used between the Administrator and the Group Manager, such as [RFC9202] and [RFC9203].

The same security considerations from [I-D.ietf-ace-key-groupcomm] and [I-D.ietf-ace-key-groupcomm-oscore] also apply, with particular reference to the process of rekeying OSCORE groups.

Further security considerations are compiled below.

9.1. Change of Group Configuration

With respect to changing group configurations, the following security considerations hold.

* A change of the current group configuration (see Section 6.6 and Section 6.7) might result in generating and distributing new group keying material, consistently with the newly enforced algorithms and related parameters. In such a case, the Group Manager can perform a group rekeying as per Section 11 of [I-D.ietf-ace-key-groupcomm-oscore], or provide the new group keying material together with the new group configuration as per Section 6.6 and Section 6.7 of this document.

  After gaining knowledge of the new group configuration, current group members may also leave the OSCORE group and rejoin it, hence obtaining the new group configuration parameters and the up-to-date group keying material. When this happens, the Group Manager SHOULD NOT repeatedly rekey the group upon the re-join of every current group member, each of which is identifiable by means of the secure association that it has with the Group Manager.

  Shortly following an update of group configuration, the Group Manager SHOULD prioritize the re-join of such current group members before processing Join Requests from new group members.

* Following the enforcement of a new group configuration, a group member might support it while not deeming it conducive to a sufficient security level (e.g., in terms of security algorithms and related parameters). In such a case, it is RECOMMENDED that the group member leaves the group.

* A change of the current group configuration, possibly also requiring a group rekeying, might result in temporarily preventing communications among some group members altogether, until they have aligned themselves to the new group configuration. This is especially the case for a change of group configuration affecting the security algorithms and related parameters used in the group.

  Furthermore, a change of group configuration might interfere with ongoing, extended exchanges between group members, especially

Block-Wise transfers [RFC7959][RFC9177] and the transmission of Observe notifications for ongoing Observations [RFC7641].

A group configuration (possibly together with the group keying material) may have been updated while a Block-Wise transfer is ongoing between two group members. This will result in blocks being resent, if the block sender and recipient are not yet both aligned with the new group configuration (and group keying material), in which case the block recipient would reply with an error message.

After a change of group configuration, a group member MUST terminate an ongoing Observation if the new group configuration would not have allowed to compute exactly the Observe request associated with the ongoing Observation. This occurs, for example, when the new group configuration specifies a signature algorithm different than the one used in the group when the Observe request was protected.

9.2. Group Manager

In addition to what is discussed in Section 10.1 of [I-D.ietf-ace-key-groupcomm], a compromised Group Manager would allow an adversary to also monitor the group configurations specified by an Administrator, or to enforce group configurations different than the specified ones, which can result in communications in the OSCORE groups not attaining the originally intended security level.

Although this is undesirable, it is not worse than the control that the adversary would gain on the group keying material through the compromised Group Manager (see Section 10.1 of [I-D.ietf-ace-key-groupcomm]).

Unlike what is defined in Section 10.2 of [I-D.ietf-ace-key-groupcomm] with respect to renewing the group keying material, the Group Manager does not have to change the group configurations of the OSCORE groups it is responsible for, after having experienced a reboot.

9.3. Administrators

If multiple Administrators are responsible for the same OSCORE group, they are expected to be aware of each other and of their shared responsibility, as well as to be aligned on what is in the best interest of the OSCORE group and its secure operation. It is out of the scope of this document to define how different Administrators are appointed as responsible for an OSCORE group and how they achieve and maintain such an alignment with each other.

A compromised Administrator may collude with unauthorized parties. Within the extent of the granted access rights, the compromised Administrator may leak group configurations, change them in such a way that communications in the OSCORE groups do not attain the originally intended security level, or delete OSCORE groups altogether thus impeding their secure operation.

When an Administrator is found compromised, the pertaining Access Tokens MUST be revoked by the Authorization Server. A possible way for the Authorization Server to notify the affected Group Managers about such revoked Access Tokens is defined in [I-D.ietf-ace-revoked-token-notification].

10. IANA Considerations

This document has the following actions for IANA.

Note to RFC Editor: Please replace all occurrences of "[RFC-XXXX]" with the RFC number of this specification and delete this paragraph.

10.1. ACE Groupcomm Parameters

IANA is asked to register the following entries in the "ACE Groupcomm Parameters" registry defined in Section 11.6 of [I-D.ietf-ace-key-groupcomm].

Name: hkdf
CBOR Key: TBD
CBOR Type: tstr / int
Reference: [RFC-XXXX]

Name: cred_fmt
CBOR Key: TBD
CBOR Type: int
Reference: [RFC-XXXX]

Name: group_mode
CBOR Key: TBD
CBOR Type: simple value
Reference: [RFC-XXXX]

Name: gp_enc_alg
CBOR Key: TBD
CBOR Type: tstr / int / simple value
Reference: [RFC-XXXX]

Name: sign_alg
CBOR Key: TBD
CBOR Type: tstr / int / simple value
Reference: [RFC-XXXX]

Name: sign_params
CBOR Key: TBD
CBOR Type: array / simple value
Reference: [RFC-XXXX]

Name: pairwise_mode
CBOR Key: TBD
CBOR Type: simple value
Reference: [RFC-XXXX]

Name: alg
CBOR Key: TBD
CBOR Type: tstr / int / simple value
Reference: [RFC-XXXX]

Name: ecdh_alg
CBOR Key: TBD
CBOR Type: tstr / int / simple value
Reference: [RFC-XXXX]

Name: ecdh_params
CBOR Key: TBD
CBOR Type: array / simple value
Reference: [RFC-XXXX]

Name: det_req
CBOR Key: TBD
CBOR Type: simple value
Reference: [RFC-XXXX]

Name: det_hash_alg
CBOR Key: TBD
CBOR Type: tstr / int
Reference: [RFC-XXXX]

Name: rt
CBOR Key: TBD
CBOR Type: tstr
Reference: [RFC-XXXX]

Name: active
CBOR Key: TBD
CBOR Type: simple value
Reference: [RFC-XXXX]

Name: group_name
CBOR Key: TBD
CBOR Type: tstr
Reference: [RFC-XXXX]

Name: group_title
CBOR Key: TBD
CBOR Type: tstr / simple value
Reference: [RFC-XXXX]

Name: max_stale_sets
CBOR Key: TBD
CBOR Type: uint
Reference: [RFC-XXXX]

Name: gid_reuse
CBOR Key: TBD
CBOR Type: simple value
Reference: [RFC-XXXX]

Name: app_groups
CBOR Key: TBD
CBOR Type: array
Reference: [RFC-XXXX]

Name: joining_uri
CBOR Key: TBD
CBOR Type: tstr
Reference: [RFC-XXXX]

Name: as_uri
CBOR Key: TBD
CBOR Type: tstr
Reference: [RFC-XXXX]

Name: conf_filter
CBOR Key: TBD
CBOR Type: array
Reference: [RFC-XXXX]

Name: app_groups_diff
CBOR Key: TBD
CBOR Type: array
Reference: [RFC-XXXX]

10.2. ACE Groupcomm Errors

IANA is asked to register the following entry in the "ACE Groupcomm Errors" registry defined in Section 11.11 of [I-D.ietf-ace-key-groupcomm].

Value: 10
Description: Group currently active
Reference: [RFC-XXXX]

Value: 11
Description: No available group names
Reference: [RFC-XXXX]

Value: 12
Description: Unsupported group configuration
Reference: [RFC-XXXX]

10.3. Resource Types

IANA is asked to enter the following values in the "Resource Type (rt=) Link Target Attribute Values" registry within the "Constrained Restful Environments (CoRE) Parameters" registry group.

Value: core.osc.gcoll
Description: Group-collection resource of an OSCORE Group Manager
Reference: [RFC-XXXX]

Value: core.osc.gconf
Description: Group-configuration resource of an OSCORE Group Manager
Reference: [RFC-XXXX]

10.4. Group OSCORE Admin Permissions

This document establishes the IANA "Group OSCORE Admin Permissions" registry. The registry has been created to use the "Expert Review" registration procedure [RFC8126]. Expert review guidelines are provided in Section 10.5.

This registry includes the possible permissions that Administrators can have to perform operations on an OSCORE Group Manager, each in combination with a numeric identifier. These numeric identifiers are used to express authorization information about performing administrative operations concerning OSCORE groups under the control of the Group Manager, as specified in Section 3 of [RFC-XXXX].

The columns of this registry are:

- Name: A value that can be used in documents for easier comprehension, to identify a possible permission that

Administrators can perform when interacting with an OSCORE Group Manager.

* Value: The numeric identifier for this permission. Integer values greater than 65535 are marked as "Private Use", all other values use the registration policy "Expert Review" [RFC8126].

  Note that, in general, a single permission can be associated with multiple different operations that are possible to be performed when interacting with the Group Manager.

* Description: This field contains a brief description of the permission.

* Reference: This contains a pointer to the public specification for the permission.

This registry will be initially populated by the values in Figure 2.

The Reference column for all of these entries will be [RFC-XXXX].

10.5. Expert Review Instructions

The IANA registry established in this document is defined as "Expert Review". This section gives some general guidelines for what the experts should be looking for, but they are being designated as experts for a reason so they should be given substantial latitude.

Expert reviewers should take into consideration the following points:

* Clarity and correctness of registrations. Experts are expected to check the clarity of purpose and use of the requested entries. Experts should inspect the entry for the considered permission, to verify the correctness of its description against the permission as intended in the specification that defined it. Expert should consider requesting an opinion on the correctness of registered parameters from the Authentication and Authorization for Constrained Environments (ACE) Working Group and the Constrained RESTful Environments (CoRE) Working Group.

  Entries that do not meet these objective of clarity and completeness should not be registered.

* Duplicated registration and point squatting should be discouraged. Reviewers are encouraged to get sufficient information for registration requests to ensure that the usage is not going to duplicate one that is already registered and that the point is likely to be used in deployments.

* Experts should take into account the expected usage of permissions when approving point assignment. Given a 'Value' V as code point, the length of the encoding of (2^(V+1) - 1) should be weighed against the usage of the entry, considering the resources and capabilities of devices it will be used on. Additionally, given a 'Value' V as code point, the length of the encoding of (2^(V+1) - 1) should be weighed against how many code points resulting in that encoding length are left, and the resources and capabilities of devices it will be used on.

* Specifications are recommended. When specifications are not provided, the description provided needs to have sufficient information to verify the points above.

11. References

11.1. Normative References

[COSE.Algorithms] IANA, "COSE Algorithms", <https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[I-D.ietf-ace-key-groupcomm] Palombini, F. and M. Tiloca, "Key Provisioning for Group Communication using ACE", Work in Progress, Internet-Draft, draft-ietf-ace-key-groupcomm-16, 5 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-key-groupcomm-16>.

[I-D.ietf-ace-key-groupcomm-oscore] Tiloca, M., Park, J., and F. Palombini, "Key Management for OSCORE Groups in ACE", Work in Progress, Internet-Draft, draft-ietf-ace-key-groupcomm-oscore-16, 6 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-key-groupcomm-oscore-16>.

[I-D.ietf-core-groupcomm-bis] Dijk, E., Wang, C., and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, draft-ietf-core-groupcomm-bis-08, 11 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-core-groupcomm-bis-08>.

[I-D.ietf-core-oscore-groupcomm] Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and J. Park, "Group Object Security for Constrained RESTful Environments (Group OSCORE)", Work in Progress, Internet-Draft, draft-ietf-core-oscore-groupcomm-18, 22 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-groupcomm-18>.

[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/rfc/rfc2119>.

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

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

[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/rfc/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/rfc/rfc7641>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[RFC8132] van der Stok, P., Bormann, C., and A. Sehgal, "PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)", RFC 8132, DOI 10.17487/RFC8132, April 2017, <https://www.rfc-editor.org/rfc/rfc8132>.

[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/rfc/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[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/rfc/rfc8613>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[RFC9200] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)", RFC 9200, DOI 10.17487/RFC9200, August 2022, <https://www.rfc-editor.org/rfc/rfc9200>.

[RFC9202] 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)", RFC 9202, DOI 10.17487/RFC9202, August 2022, <https://www.rfc-editor.org/rfc/rfc9202>.

[RFC9203] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "The Object Security for Constrained RESTful Environments (OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", RFC 9203, DOI 10.17487/RFC9203, August 2022, <https://www.rfc-editor.org/rfc/rfc9203>.

[RFC9237] Bormann, C., "An Authorization Information Format (AIF) for Authentication and Authorization for Constrained Environments (ACE)", RFC 9237, DOI 10.17487/RFC9237, August 2022, <https://www.rfc-editor.org/rfc/rfc9237>.

[RFC9277] Richardson, M. and C. Bormann, "On Stable Storage for Items in Concise Binary Object Representation (CBOR)", RFC 9277, DOI 10.17487/RFC9277, August 2022, <https://www.rfc-editor.org/rfc/rfc9277>.

11.2. Informative References

[I-D.amsuess-core-cachable-oscore]

Amsüss, C. and M. Tiloca, "Cacheable OSCORE", Work in Progress, Internet-Draft, draft-amsuess-core-cachable-oscore-06, 11 January 2023, <https://datatracker.ietf.org/doc/html/draft-amsuess-core-cachable-oscore-06>.

[I-D.ietf-ace-revoked-token-notification]
Tiloca, M., Palombini, F., Echeverria, S., and G. Lewis, "Notification of Revoked Access Tokens in the Authentication and Authorization for Constrained Environments (ACE) Framework", Work in Progress, Internet-Draft, draft-ietf-ace-revoked-token-notification-06, 2 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-revoked-token-notification-06>.

[I-D.ietf-cose-cbor-encoded-cert]
Mattsson, J. P., Selander, G., Raza, S., Höglund, J., and M. Furuhed, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-05, 10 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-05>.

[I-D.tiloca-core-oscore-discovery] Tiloca, M., Amsüss, C., and P. Van der Stok, "Discovery of OSCORE Groups with the CoRE Resource Directory", Work in Progress, Internet-Draft, draft-tiloca-core-oscore-discovery-13, 8 March 2023, <https://datatracker.ietf.org/doc/html/draft-tiloca-core-oscore-discovery-13>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/rfc/rfc7959>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/rfc/rfc8392>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version

1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[RFC9176] Amsüss, C., Ed., Shelby, Z., Koster, M., Bormann, C., and P. van der Stok, "Constrained RESTful Environments (CoRE) Resource Directory", RFC 9176, DOI 10.17487/RFC9176, April 2022, <https://www.rfc-editor.org/rfc/rfc9176>.

[RFC9177] Boucadair, M. and J. Shallow, "Constrained Application Protocol (CoAP) Block-Wise Transfer Options Supporting Robust Transmission", RFC 9177, DOI 10.17487/RFC9177, March 2022, <https://www.rfc-editor.org/rfc/rfc9177>.

Appendix A. Processing of Group Name Patterns at the AS

When processing an Authorization Request from an Administrator (see Section 4), the AS builds the authorization information expressing granted permissions as scope entries, according to the AIF specific data model AIF-OSCORE-GROUPCOMM and to its extension specified in Section 3. These scope entries are in turn specified as value of the 'scope' claim to include in the Access Token.

In order to evaluate the requested permissions against the access policies pertaining to the Administrator for the Group Manager in question, the AS can perform the following steps.

The following specifically refers only to "admin scope entries", i.e., scope entries that express authorization information for Administrators of OSCORE groups.

1. The AS initializes three empty sets of scope entries, namely S1, S2 and S3.

2. For each scope entry E in the 'scope' parameter of the Authorization Request, the AS performs the following actions.

   * In its access policies related to administrative operations at the Group Manager for the Administrator, the AS determines every group name superpattern P*, such that every group name matching with the pattern P of the scope entry E matches also with P*.

   * If no superpatterns are found, the AS proceeds with the next scope entry, if any. Otherwise, the AS computes Tperm* as the union of the permission sets associated with the superpatterns found at the previous step. That is, Tperm* is the inclusive OR of the binary representations of the Tperm values associated with the found superpatterns and encoding the corresponding permission sets as per Section 3.

* The AS adds to the set S1 a scope entry, such that its Toid is the same as in the scope entry E, while its Tperm is the AND of Tperm* with the Tperm in the scope entry E.

3. For each scope entry E in the 'scope' parameter of the Authorization Request, the AS performs the following actions.

   * In its access policies related to administrative operations at the Group Manager for the Administrator, the AS determines every group name subpattern P*, such that: i) the pattern P of the scope entry E is different from P*; and ii) every group name matching with P* also matches with P.

   * If no subpatterns are found, the AS proceeds with the next scope entry, if any. Otherwise, for each found subpattern P*, the AS adds to the set S2 a scope entry, such that its Toid is the same as in the subpattern P*, while its Tperm is the AND of the Tperm from the subpattern P* with the Tperm in the scope entry E.

4. For each scope entry E in the 'scope' parameter of the Authorization Request, the AS performs the following actions.

   * For each group name pattern P* in its access policies related to administrative operations at the Group Manager for the Administrator, the AS performs the following actions.

     - The AS attempts to determine a crosspattern P** such that: i) in the previous steps, P** was not identified as a superpattern or subpattern for the pattern P of the scope entry E; ii) every group name matching with P** also matches with both P and P*.

     - If no crosspattern is built, the AS proceeds with the next pattern in its access policies related to administrative operations at the Group Manager for the Administrator, if any. Otherwise, the AS adds to the set S3 a scope entry, such that its Toid is the same as in the crosspattern P**, while its Tperm is the AND of the Tperm from the pattern P* and the Tperm in the scope entry E.

5. If the sets S1, S2 and S3 are all empty, the Authorization Request has not been successfully verified, and the AS returns an error response as per Section 5.8.3 of [RFC9200]. Otherwise, the AS uses the scope entries in the sets S1, S2 and S3 as the scope entries for the 'scope' claim to include in the Access Token, as per the format defined in Section 3.

Appendix B. Document Updates

RFC EDITOR: PLEASE REMOVE THIS SECTION.

B.1. Version -08 to -09

* Removed use of CoRAL.

* Use of the pairwise mode changed to "true" by default.

* Clarified effects on group members after a group configuration change.

* Renamed "Signature Encryption Algorithm" to "Group Encryption Algorithm".

* Renamed "sign_enc_alg" to "gp_enc_alg".

* Fixes and editorial improvements.

B.2. Version -07 to -08

* Consistency of parameter names.

* More details on consistency of message payload.

* New section on multiple, concurrent Administrators.

* Specified atomicity of write operations.

* Clarified effects of configuration overwriting on group members.

* New ACE Groupcomm Error on unsupported configuration.

* Possible reason to deviate from default parameter values.

* Added security considerations.

* CoRAL examples use CBOR diagnostic notation and Packed CBOR.

* Various clarifications and editorial improvements.

B.3. Version -06 to -07

* Alignment with renaming in draft-ietf-ace-key-groupcomm.

* Updated signaling of semantics for binary encoded scopes.

* Split between parameter registration and their CBOR abbreviations.

*Classified parameters as must/should/may be supported.

*New error code "No available group names" and related guidelines.

*Fixes in the examples.

*Editorial improvements.

B.4. Version -05 to -06

*Use and extend the same AIF specific data model AIF-OSCORE-GROUPCOMM defined in [I-D.ietf-ace-key-groupcomm-oscore].

*Revised Client-AS interaction, based on the used AIF specific data model.

*Categorized operations at the Group Manager as required and optional to support.

*Added status parameter 'gid_reuse', on reassigning OSCORE Group IDs upon group rekeying.

*Clarifications on the group name ultimately chosen by the Group Manager.

*Moved the detailed processing of group name patterns at the AS to an Appendix, as an example.

*Editorial improvements.

B.5. Version -04 to -05

*Defined format of scope based on a new AIF data model.

*Specified authorization checks at the Group Manager.

*Revised resource handlers based on the new scope format.

*Renamed 'pub_key_enc' to 'cred_fmt'.

*Mandatory to include 'group_name' in the group creation request.

*Suggesting a used 'group_name' results in a new name, not in an error.

*Distinction between authentication credentials and public keys.

*More details on informing group members about changes in the group configuration.

*Revised order of sections; editorial improvements.

B.6. Version -03 to -04

* Clarifications on what to do in case of enhanced error responses.

* Clarifications on handling default values for group parameters.

* New configuration parameters to support OSCORE deterministic requests.

* IANA considerations - Use RFC8126 terminology.

* Author's change of address.

* Editorial improvements.

B.7. Version -02 to -03

* Aligned new and old parameters to core-groupcomm-oscore and ace-key-groupcomm-oscore.

* Removed 'cs_key_params' and 'ecdh_key_params' to avoid redundant COSE capabilities of key types, consistently with draft-ietf-ace-key-groupcomm-oscore.

* Revised examples and side effects due to parameter changes.

* New error type "Group currently active".

B.8. Version -01 to -02

* Admit multiple Administrators and limited access to admin resources.

* Early design considerations for defining the format of scope.

* Additional error handling, using also error types.

* Selective update of group-configuration resources with PATCH/iPATCH.

* Editorial improvements.

B.9. Version -00 to -01

* Names of application groups as status parameter.

* Parameters related to the pairwise mode of Group OSCORE.

* Defined FETCH for group-configuration resources.

* Policies on registration of links to the Resource Directory.

*Added resource type for group-configuration resources.

*Fixes, clarifications and editorial improvements.

Acknowledgments

Klaus Hartke provided substantial contribution in defining the resource model based on group collection and group configurations.

The authors sincerely thank Christian Amsüss, 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; and by the H2020 project SIFIS-Home (Grant agreement 952652).

Authors' Addresses

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

Email: marco.tiloca@ri.se

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

Email: rikard.hoglund@ri.se

Peter van der Stok
Consultant

Phone: +31-492474673 (Netherlands), +33-966015248 (France)
Email: stokcons@bbhmail.nl

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

Email: francesca.palombini@ericsson.com