

ACE Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 12 July 2025

M. Tiloca  
R. Högglund  
RISE AB  
P. van der Stok

F. Palombini  
Ericsson AB  
8 January 2025

Admin Interface for the OSCORE Group Manager  
draft-ietf-ace-oscore-gm-admin-13

## Abstract

Group communication for CoAP can be secured using Group Object Security for Constrained RESTful Environments (Group OSCORE). A Group Manager is responsible for handling the joining of new group members, as well as managing and distributing 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](mailto: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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

This Internet-Draft will expire on 12 July 2025.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

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

## Table of Contents

1. Introduction . . . . .	4
1.1. Terminology . . . . .	5
2. Group Administration . . . . .	7
2.1. Managing OSCORE Groups . . . . .	8
2.2. Collection Representation . . . . .	9
2.3. Discovery . . . . .	9
3. Format of Scope . . . . .	10
3.1. On Using Group Name Patterns . . . . .	14
4. Getting Access to the Group Manager . . . . .	14
4.1. Multiple Administrators for the Same OSCORE Group . . . . .	18
5. Group Configurations . . . . .	20
5.1. Group Configuration Representation . . . . .	20
5.1.1. Configuration Parameters . . . . .	20
5.1.2. Status Parameters . . . . .	23
5.2. Default Values . . . . .	24
5.2.1. Configuration Parameters . . . . .	25
5.2.2. Status Parameters . . . . .	26
6. Interactions with the Group Manager . . . . .	26
6.1. Retrieve the Full List of Group Configurations . . . . .	28
6.2. Retrieve a List of Group Configurations by Filters . . . . .	28

6.3.	Create a New Group Configuration . . . . .	31
6.4.	Retrieve a Group Configuration . . . . .	37
6.5.	Retrieve Part of a Group Configuration by Filters . . . . .	39
6.6.	Overwrite a Group Configuration . . . . .	40
6.6.1.	Effects on Joining Nodes . . . . .	44
6.6.2.	Effects on the Group Members . . . . .	44
6.7.	Selective Update of a Group Configuration . . . . .	49
6.7.1.	Effects on Joining Nodes . . . . .	53
6.7.2.	Effects on the Group Members . . . . .	53
6.8.	Delete a Group Configuration . . . . .	53
6.8.1.	Effects on the Group Members . . . . .	55
7.	ACE Groupcomm Parameters . . . . .	56
8.	ACE Groupcomm Error Identifiers . . . . .	58
9.	Security Considerations . . . . .	60
9.1.	Change of Group Configuration . . . . .	61
9.2.	Group Manager . . . . .	62
9.3.	Administrators . . . . .	62
10.	IANA Considerations . . . . .	63
10.1.	ACE Groupcomm Parameters . . . . .	63
10.2.	ACE Groupcomm Errors . . . . .	68
10.3.	Resource Types . . . . .	68
10.4.	Group OSCORE Admin Permissions . . . . .	69
10.5.	Expert Review Instructions . . . . .	69
11.	References . . . . .	70
11.1.	Normative References . . . . .	70
11.2.	Informative References . . . . .	73
Appendix A.	Processing of Group Name Patterns at the AS . . . . .	75
Appendix B.	CDDL Model . . . . .	77
Appendix C.	Document Updates . . . . .	78
C.1.	Version -12 to -13 . . . . .	78
C.2.	Version -11 to -12 . . . . .	79
C.3.	Version -10 to -11 . . . . .	79
C.4.	Version -09 to -10 . . . . .	80
C.5.	Version -08 to -09 . . . . .	80
C.6.	Version -07 to -08 . . . . .	81
C.7.	Version -06 to -07 . . . . .	81
C.8.	Version -05 to -06 . . . . .	81
C.9.	Version -04 to -05 . . . . .	82
C.10.	Version -03 to -04 . . . . .	82
C.11.	Version -02 to -03 . . . . .	83
C.12.	Version -01 to -02 . . . . .	83
C.13.	Version -00 to -01 . . . . .	83
Acknowledgments	. . . . .	83
Authors' Addresses	. . . . .	84

## 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 join the correct OSCORE group explicitly. 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. That method builds on the ACE framework for Authentication and Authorization [RFC9200], 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 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 may lead 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.

Throughout this document, examples for CBOR data items are expressed in CBOR extended diagnostic notation as defined in Section 8 of [RFC8949] and Appendix G of [RFC8610] ("diagnostic notation"). Diagnostic notation comments are often used to provide a textual representation of the numeric parameter names and values.

In the CBOR diagnostic notation used in this document, constructs of the form `e'SOME_NAME'` are replaced by the value assigned to `SOME_NAME` in the CDDL model shown in Figure 3 of Appendix B. For example, `{e'group_name': "gpl", e'gp_enc_alg': 10}` stands for `{-13: "gpl", -4: 10}`.

Note to RFC Editor: Please delete the paragraph immediately preceding this note. Also, in the CBOR diagnostic notation used in this document, please replace the constructs of the form `e'SOME_NAME'` with the value assigned to `SOME_NAME` in the CDDL model shown in Figure 3 of Appendix B. Finally, please delete this note.

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.

- \* CDDL [RFC8610], 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 a 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 [RFC9594] 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, and that current members can access to retrieve updated keying material.

Note that the term "endpoint" is used here following its OAuth definition [RFC6749], 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 for creating, configuring, and deleting 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 be consistent with the ABNF rule "segment = \*pchar" defined in Section 3.3 of [RFC3986].
- \* 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.

When defining operations at the Group Manager and providing examples, this document uses /manage as the url-path of the group-collection resource; implementations can use a different url-path.

- \* 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 same construct, and can define their own instead.

- \* Admin resource: a group-collection resource or a group-configuration resource hosted by the Group Manager.
- \* Secure communication association: a security association established between any two of the Administrator, the AS, and the Group Manager and used for protecting their message exchanges. For example, depending on the used transport profile of ACE, this can rely on DTLS [RFC9147] as per [RFC9202], or on OSCORE [RFC8613] as per [RFC9203].

## 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). The Group Manager 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 issue Access Tokens to the Administrator for other purposes than accessing admin resources of registered Group Managers. For example, an Access Token can specify authorization information for joining OSCORE groups at a Group Manager (see [I-D.ietf-ace-key-groupcomm-oscure]), possibly combined with authorization information for accessing admin resources at the same Group Manager (see Section 3). Also, an AS can of course issue an Access Token that specifies authorization information unrelated to OSCORE groups, but instead pertaining to the access of other resources hosted by the Group Manager or other Resource Servers.

## 2.1. Managing OSCORE Groups

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

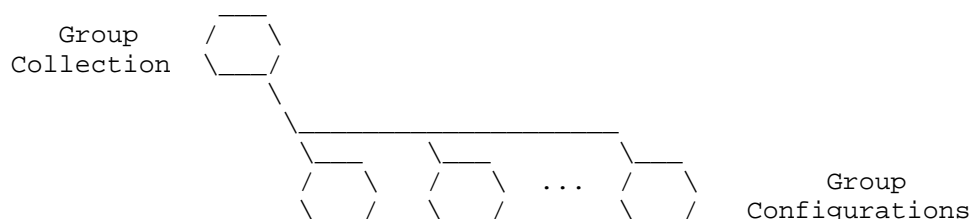


Figure 1: Admin Resources of a Group Manager



The Group Manager exports a single group-collection resource, with resource type "core.osc.gcoll" registered in Section 10.3 of this document. The interface for the group-collection resource defined in Section 6 allows the Administrator, if permitted, to:

- \* Retrieve the list of existing OSCORE groups.
- \* Retrieve a 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" registered 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, if permitted, 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".

## 2.3. Discovery

The Administrator can discover group-collection resources from a Resource Directory [RFC9176] or from .well-known/core, by using the resource type "core.osc.gcoll".

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

Building on the definition in Section 3.3 of [RFC6749] considered in the ACE framework [RFC9200], scope denotes: the permissions that the Client (i.e., the Administrator) seeks to obtain from the AS for accessing resources at a Resource Server (i.e., the Group Manager); and the permissions that the AS actually issues to the Client following its request. This process is detailed in Sections 5.8.1 and 5.8.2 of [RFC9200].

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 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 into scope entries, which express authorization information for users of an OSCORE group, i.e., actual group members or external signature verifiers. Hereafter, these are referred to as "user scope entries".

This document extends the same AIF 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. Hereafter, these are referred to as "admin scope entries", or simply as "scope entries" unless otherwise indicated.

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

$$\text{AIF-Generic}\langle\text{Toid}, \text{Tperm}\rangle = [* [\text{Toid}, \text{Tperm}]]$$

the value of the CBOR byte string used as scope encodes the CBOR array  $[* [\text{Toid}, \text{Tperm}]]$ , where each  $[\text{Toid}, \text{Tperm}]$  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 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 21065. This indicates that the group name pattern specified as value of the CBOR text string is a regular expression in the I-Regexp flavor [RFC9485].

In case the AIF 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 with respect to performing 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 Table 1.

- The set of N numbers is converted into the single value Q, by taking two to the power of each numeric identifier X<sub>1</sub>, X<sub>2</sub>, ..., X<sub>N</sub>, 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

Table 1: 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 Table 1.

```

;# include rfc9237

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

oscore-gname = true / tstr / #6.<uint>(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]

```

The following example in CBOR diagnostic notation shows a CBOR array including five scope entries as its elements.

```

[[true,      / Toid (wildcard pattern) /
  5          / Tperm (List + Read) /
],
["gp1",     / Toid (literal pattern) /
  31        / Tperm (List + Create +
                Read + Write + Delete) /
],
["gp2",     / Toid (literal pattern) /
  31        / Tperm (List + Create +
                Read + Write + Delete) /
],
[21065("^[A-K][0-9][-a-z0-9]*$"), / Toid (complex pattern) /
  31          / Tperm (List + Create +
                Read + Write + Delete) /
],
[21065("^[J-Z][0-9][-a-z0-9]*$"), / Toid (complex pattern) /
  13          / Tperm (List + Read + Write) /
]
]

```

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.

### 3.1. On Using Group Name Patterns

Having the object identifier ("Toid") specialized as a pattern confers 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 the 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).

## 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 transport profile of ACE in use, 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 and 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]).

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. Also, in the 'scope' claim of the Access Token issued by the AS, that semantics MUST be used for all the scope entries that specify a complex pattern.

Furthermore, the AS MAY use the extended format of scope defined in Section 7 of [RFC9594] 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-oscure].

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-oscure]. 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 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].

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

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.

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, with respect to performing 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-collection resource or a group-configuration resource, the Group Manager MUST check that it is storing a valid Access Token for that Administrator, and that the Access Token includes at least one admin scope entry. If this is not the case, the Group Manager MUST reply with a 4.01 (Unauthorized) error response.

If the request targets the group-collection resource for creating a new group with name GROUPNAME or it targets the group-configuration resource associated with an existing group with name GROUPNAME, then 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 (i.e., ID: 19).

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

It is possible that multiple Administrators are authorized to operate on the same Group Manager in the interest of the same OSCORE group, while also taking different responsibilities.

For example, 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 fewer permissions to perform administrative operations related to the OSCORE group at the Group Manager. For example, they may not be authorized to create an OSCORE group, or to delete an 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 regularly obtains 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.

In order to avoid race conditions due to possible concurrent updates of the group-configuration resource (i.e., the "lost update" problem), the Group Manager can include the ETag Option in the responses to the GET requests sent to the group-configuration resource (see Section 5.10.6 of [RFC7252]). Then, when sending to the Group Manager a request for overwriting or updating the group-configuration resource, the Administrator includes an If-Match Option with value the most recent ETag that the Administrator knows for that resource (see Section 5.10.8.1 of [RFC7252]).

## 5. Group Configurations

A group configuration consists of information related to an OSCORE group, as organized into configuration parameters and status parameters.

In particular, configuration parameters specify how members of the OSCORE group use the Group OSCORE protocol to protect their communications (e.g., by using which algorithms). Instead, status parameters specify information concerning the management of the OSCORE group and its current setting at the Group Manager (e.g., for handling identifiers and the joining of group members).

### 5.1. Group Configuration Representation

The group configuration representation is a CBOR map, which includes the configuration parameters specified in Section 5.1.1 and the status parameters specified in Section 5.1.2.

Unless stated otherwise, these parameters are defined in this document and their CBOR abbreviations are defined in Section 7.

#### 5.1.1. Configuration Parameters

The CBOR map includes the following configuration parameters.

- \* '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. This parameter can take the same values as 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. This parameter can take the same values as 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 7 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. This parameter can take the same values as 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. This parameter can take the same values as 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. This parameter can take the same values as 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 8 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. This parameter can take the same values as 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. This parameter can take the same values as 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. This parameter can take the same values as 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 can be present only if both the configuration parameters 'group\_mode' and 'pairwise\_mode' have value true (0xf5), and MUST NOT be present otherwise.
- \* '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 Parameters

The CBOR map includes the following status parameters.

- \* 'rt', which specifies the resource type "core.osc.gconf" associated with group-configuration resources, encoded as a CBOR text string.
- \* 'active', which specifies whether the OSCORE group is currently active, encoded as the CBOR simple value true (0xf5) or false (0xf4).
- \* 'group\_name', which specifies the group name of the OSCORE group encoded as a CBOR text string.
- \* 'group\_description', which specifies 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 [RFC9594], with value "coap\_group\_oscore\_app" registered 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 [RFC9594].
- \* '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 12.2.1.1 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 [RFC9594], 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 uses for the configuration and status parameters.

The Group Manager MAY choose different default values instead of those recommended in this section. A possible reason 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 uses the following pre-configured default value, if that parameter is not specified by the Administrator.

- \* 'group\_mode' - The Group Manager SHOULD use the CBOR simple value true (0xf5).
- \* 'pairwise\_mode' - The Group Manager SHOULD use the CBOR simple value true (0xf5).
- \* 'gp\_enc\_alg', 'sign\_alg', and 'sign\_params' - If the value of 'group\_mode' is determined to be the CBOR simple 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].

- \* 'alg', 'ecdh\_alg', and 'ecdh\_params' - If the value of 'pairwise\_mode' is determined to be the CBOR simple 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'.
- \* 'det\_req' - If the value of both 'group\_mode' and 'pairwise\_mode' is determined to be the CBOR simple value true (0xf5), the Group Manager SHOULD add the parameter 'det\_req' to the group configuration and SHOULD set its value to the CBOR simple value false (0xf4).

- \* 'det\_hash\_alg' - If the value of 'det\_req' is determined to be the CBOR simple value true (0xf5), the Group Manager SHOULD add the parameter 'det\_hash\_alg' to the group configuration and SHOULD set its value to -16 (COSE algorithm encoding for SHA-256).

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 uses the following pre-configured default value, if that parameter is not specified by the Administrator.

- \* 'active' - The Group Manager SHOULD use the CBOR simple value false (0xf4).
- \* 'group\_description' - The Group Manager SHOULD use the CBOR simple value null (0xf6).
- \* 'max\_stale\_sets' - The Group Manager SHOULD use the CBOR unsigned integer with value 3, consistent with what is defined in Section 14.1 of [I-D.ietf-ace-key-groupcomm-oscore].
- \* 'gid\_reuse' - The Group Manager SHOULD use the CBOR simple value false (0xf4).
- \* 'app\_groups' - The Group Manager SHOULD use the empty CBOR array.
- \* '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 an Administrator and for the Group Manager. If an Administrator supports an operation, then the Administrator is able to produce and send the request associated with that operation. 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. 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.

Upon receiving from the Administrator a POST request to the group-collection resource or a request to a group-configuration resource, the Group Manager performs the following authorization checks, consistently with what is defined at step 4 of Section 4.

- \* The Group Manager MUST check whether the group name TARGETNAME pertaining to the request 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 PERMISSION required to perform the requested administrative operation.

If there are no matching scope entries specifying the permission PERMISSION, the Group Manager MUST reply with a 4.03 (Forbidden) error response. Further details on TARGETNAME and PERMISSION are defined separately for each operation at the Group Manager.

The Content-Format in messages containing a payload is set to application/ace-groupcomm+cbor, defined in Section 11.2 of [RFC9594]. Furthermore, the CBOR abbreviations 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.

Entry values are the ones admitted for the corresponding labels in the POST request for creating a group configuration (see Section 6.3), with the exception that the parameter 'group\_name' (if present) can also be encoded as a tagged CBOR data item, specifying a group name pattern with the semantics signaled by the CBOR tag.

In such a case, the parameter 'group\_name' expresses a group name pattern in the same way as a complex pattern Toid does in a scope entry (see Section 3). In particular, the filter criterion is satisfied by any group name that matches with the group name pattern specified by the parameter 'group\_name' in the payload of the FETCH request.

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: 261 (application/ace-groupcomm+cbor)
```

Payload:

```
{
  e'group_mode' : true,
  e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
  e'hkdf' : 5 / HMAC-256-256 /
}
```

```
<= 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"
```

The following, additional example considers a request payload that uses both configuration parameters and status parameters as filter criteria. In particular, the following is assumed.

- \* In the URI of every group-configuration resource, the path component is /manage/GROUPNAME, where GROUPNAME is the group name of the associated OSCORE group.
- \* The Group Manager hosts four group-configuration resources, for the OSCORE groups with names "gp4", "gp5", "gp6", and "foo". All the OSCORE groups use the AEAD Algorithm AES-CCM-16-64-128 (COSE algorithm encoding: 10). Also, all the OSCORE groups are currently active, except for "gp6".

```
=> 0.05 FETCH
  Uri-Path: "manage"
  Content-Format: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
    e'group_name' : 21065("gp[0-9]*"),
    e'active' : true
  }

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

  Payload:

  <coap://[2001:db8::ab]/manage/gp4>;rt="core.osc.gconf",
  <coap://[2001:db8::ab]/manage/gp5>;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. 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 encoded as a CBOR text string. As defined later in this section, the group name specified in this parameter is simply a suggestion to the Group Manager, which makes the final decision about the name to assign to the new group.
- \* The payload MAY include any of the status parameters 'active', 'group\_description', '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.

When performing the authorization checks, the Group Manager uses the value of the 'group\_name' parameter from the request as TARGETNAME, and "Create" as PERMISSION.

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/concise-problem-details+cbor [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry 'ace-groupcomm-error', the value of the 'error-id' field MUST be set to 12 ("Unsupported group configuration"), and the 'detail' field 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 not recognized, or not valid, or not consistent with respect to other related parameters. In particular, the value of the status parameter 'exp' (if present) is not valid if the indicated expiration date is not in the future.
- \* The Group Manager does not trust or deem acceptable 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 try to determine 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
- \* With reference to the `'scope'` claim in the stored Access Token for the Administrator, let us define `PERM*` as the union of the permission sets associated with the scope entries such that `GROUPNAME*` matches with the specified group name pattern. Also, let us define `PERM` as the union of the permission sets associated with the scope entries such that `GROUPNAME` matches with the specified group name pattern. Then, `PERM` and `PERM*` **MUST** be equal.

If the Group Manager does not manage to determine a 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/concise-problem-details+cbor` [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry `'ace-groupcomm-error'`, the value of the `'error-id'` field **MUST** be set to 11 ("Unable to determine a group name").

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. That is, until the request processing fails, or the group-configuration resource is fully created and the values of its parameters set, the following applies.

- \* The group-configuration resource **MUST NOT** be accessible through other operations.
- \* The group-collection resource **MUST NOT** be updated to reflect the presence of the new group-configuration resource.

When the group-collection resource is eventually updated to reflect the presence of the new group-configuration resource, this update **MUST NOT** be interrupted by other updates to the group-collection resource due to the creation or deletion of group-configuration resources.

In the newly created group-configuration resource, 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 12.2.1.1 of [I-D.ietf-core-oscgroupcomm] and Section 11 of [I-D.ietf-ace-key-groupcomm-osc]), 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-osc]. Note that such group membership-resource comprises a number of sub-resources intended to current group members, as defined in Section 4.1 of [RFC9594] and Section 8 of [I-D.ietf-ace-key-groupcomm-osc].

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-osc], 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. One or more Location-Path options 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 parameters of the newly created OSCORE group (see Section 5.1), as detailed below.

The response payload is a CBOR map, whose possible entries are specified in Section 5.1. In particular, the following applies.

- \* 'group\_name', which specifies 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 value of the 'group\_name' status parameter for the OSCORE group. This parameter MUST be included.
- \* 'joining\_uri', which specifies the URI of the group-membership resource for joining the newly created OSCORE group. This parameter MUST be included.
- \* 'as\_uri', which specifies 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 value of the 'as\_uri' status parameter 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 also include 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.

It is also possible that the Administrator performs 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: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
    e'hkdf' : 5 / HMAC-256-256 /,
    e'pairwise_mode' : true,
    e'active' : true,
    e'group_name' : "gp4",
    e'group_description' : "rooms 1 and 2",
    e'app_groups' : ["room1", "room2"],
    e'as_uri' : "coap://as.example.com/token"
  }
```

```
<= 2.01 Created
  Location-Path: "manage"
  Location-Path: "gp4"
  Content-Format: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'group_name' : "gp4",
    e'joining_uri' : "coap://[2001:db8::ab]/ace-group/gp4/",
    e'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.

When performing the authorization checks, the Group Manager uses `GROUPNAME` as `TARGETNAME`, and `"Read"` as `PERMISSION`.

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 parameters and status parameters.

The response payload is a CBOR map, whose possible entries are specified in Section 5.1.

An example of message exchange is shown below.

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

<= 2.05 Content
    Content-Format: 261 (application/ace-groupcomm+cbor)

    Payload:

    {
        e'hkdf' : 5 / HMAC-256-256 /,
        e'cred_fmt' : 33 / x5chain /,
        e'group_mode' : true,
        e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
        e'sign_alg' : -8 / EdDSA /,
        e'sign_params' : [[1], [1, 6]]
                        / [[OKP], [OKP, Ed25519]] /,
        e'pairwise_mode' : true,
        e'alg' : 10 / AES-CCM-16-64-128 /,
        e'ecdh_alg' : -27 / ECDH-SS-HKDF-256 /,
        e'ecdh_params' : [[1], [1, 4]]
                        / [[OKP], [OKP, X25519]] /,
        e'det_req' : false,
        e'rt' : "core.osc.gconf",
        e'active' : true,
        e'group_name' : "gp4",
        e'group_description' : "rooms 1 and 2",
        e'ace_groupcomm_profile' : "coap_group_oscore_app",
        e'max_stale_sets' : 3,
        e'exp' : 1360289224,
        e'gid_reuse' : false,
        e'app_groups' : ["room1", "room2"],
        e'joining_uri' : "coap://[2001:db8::ab]/ace-group/gp4/",
        e'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.

When performing the authorization checks, the Group Manager uses `GROUPNAME` as `TARGETNAME`, and `"Read"` as `PERMISSION`.

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 parameters and status parameters 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: 261 (application/ace-groupcomm+cbor)
```

Payload:

```
{
  e'conf_filter' : [e'gp_enc_alg',
                    e'hkdf',
                    e'pairwise_mode',
                    e'active',
                    e'group_description',
                    e'app_groups']
}
```

```
<= 2.05 Content
  Content-Format: 261 (application/ace-groupcomm+cbor)
```

Payload:

```
{
  e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
  e'hkdf'       : 5 / HMAC-256-256 /,
  e'pairwise_mode' : true,
  e'active'       : true,
  e'group_description' : "rooms 1 and 2",
  e'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 POST 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 POST request is the same as for the POST request defined in Section 6.3, with the following difference in terms of authorization checks.



When performing the authorization checks, the Group Manager uses GROUPNAME as TARGETNAME, and "Write" as PERMISSION.

If the group-configuration resource targeted by the POST request does not currently exist, then the Group Manager MUST NOT create the resource and MUST reply with a 4.04 (Not Found) error response.

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/concise-problem-details+cbor [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry 'ace-groupcomm-error', the value of the 'error-id' field MUST be set to 12 ("Unsupported group configuration"), and the 'detail' field SHOULD be included in order to provide additional context.

If no error occurs and the POST 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 POST request from the Administrator. When doing so, the configuration parameters 'group\_mode' and 'pairwise\_mode' as well as the status parameters 'group\_name' and 'gid\_reuse' MUST remain unchanged.

For each other parameter not specified in the POST request, the Group Manager MUST use default values as specified in Section 5.2. Note that the default value recommended for the status parameter 'active' is the CBOR simple value false (0xf4). Therefore, if the Administrator intends to preserve the current status of the group as active, then the payload of the POST request has to include the parameter 'active' specifying the CBOR simple value true (0xf5).

When updating the group-configuration resource, the corresponding group-membership resource is also accordingly updated. The operation of overwriting such two resources MUST be atomic. That is, until the request processing fails, or the group-configuration resource has been fully updated and the values of its parameters set, the following applies.

- \* The group-configuration resource MUST NOT be accessible through other operations.
- \* The group-membership resource MUST NOT be updated to reflect the new group configuration.

- \* The filter criteria specified in a FETCH request to the group-collection resource (see Section 6.2) MUST be compared against the representation that the group-configuration resource had before its update started.

When the group-membership resource is eventually updated to reflect the new group configuration, this update MUST NOT be interrupted by other operations performed on the group-membership resource.

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 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.

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].

It is also possible that the Administrator updates 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 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 2.04 (Changed) response.
- \* As to every other information element describing the current group configuration, the following applies.
  - If a certain parameter was specified in the POST 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 POST request otherwise.
  - If a certain parameter was not specified in the POST request, the Administrator MUST use either the value specified in the 2.04 (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.

```
=> 0.02 POST
  Uri-Path: "manage"
  Uri-Path: "gp4"
  Content-Format: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'gp_enc_alg' : 11 / AES-CCM-16-64-256 /,
    e'hkdf' : 5 / HMAC-256-256 /
  }

<= 2.04 Changed
  Content-Format: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'group_name' : "gp4",
    e'joining_uri' : "coap://[2001:db8::ab]/ace-group/gp4/",
    e'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 [RFC9594]), 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.
  - o 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.

- o Retrieve from the Group Manager the Group Manager's new 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.



As discussed above, after the group configuration has been updated, some group members may leave the OSCORE group and rejoin it. 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 other, new group members.

### 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 POST 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'. 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 request from the Administrator 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 2: 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 POST 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.

As an example, this is the case if the resulting group configuration would include the parameter 'sign\_alg' specifying the signature algorithm EdDSA (COSE algorithm encoding: -8) and, at the same time, the parameter 'sign\_params' specifying EC2 as COSE key type and P-256 as COSE elliptic curve (i.e., as the CBOR array [[2], [2, 1]]).

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' and the name of an application group is specified both in the 'app\_groups\_del' and 'app\_groups\_add' inner arrays.

When performing the authorization checks, the Group Manager uses GROUPNAME as TARGETNAME, and "Write" as PERMISSION.

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/concise-problem-details+cbor [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry 'ace-groupcomm-error', the value of the 'error-id' field MUST be set to 12 ("Unsupported group configuration"), and the 'detail' field 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. That is, the same as defined in Section 6.6 when atomically overwriting a group-configuration resource applies.

Unlike for the POST 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 POST 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: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'gp_enc_alg' : 10 / AES-CCM-16-64-128 /,
    e'app_groups_diff' : [["room1"], ["room3", "room4"]]
  }

<= 2.04 Changed
  Content-Format: 261 (application/ace-groupcomm+cbor)

  Payload:

  {
    e'group_name' : "gp4",
    e'joining_uri' : "coap://[2001:db8::ab]/ace-group/gp4/",
    e'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.

When performing the authorization checks, the Group Manager uses `GROUPNAME` as `TARGETNAME`, and "Delete" as `PERMISSION`.

Otherwise, the Group Manager continues processing the request, which MUST fail if the OSCORE group is active. That is, the DELETE request MUST yield the 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 Section 6.7), 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/concise-problem-details+cbor [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry 'ace-groupcomm-error', the value of the 'error-id' 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. That is, until the request processing fails, or the group-configuration resource is deleted, the following applies.

- \* The group-configuration resource MUST NOT be accessible through other operations.
- \* The group-membership resource MUST NOT be deleted.
- \* The group-collection resource MUST NOT be updated to reflect the deletion of the group-configuration resource.

When the group-membership resource is eventually deleted, this deletion MUST NOT be interrupted by other operations performed on the group-membership resource.

When the group-collection resource is eventually updated to reflect the deletion of the group-configuration resource, this update MUST NOT be interrupted by other updates to the group-collection resource due to the creation or deletion of group-configuration resources, or to other operations performed on those.

After deleting the group-configuration resource, 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 [RFC9594]). The response MUST have Content-Format set to application/concise-problem-details+cbor [RFC9290] and is formatted as defined in Section 4.1.2 of [RFC9594]. Within the Custom Problem Detail entry 'ace-groupcomm-error', the value of the 'error-id' field MUST be set to 6 ("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 [RFC9594], 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	-1	tstr or int	[RFC-XXXX]
cred_fmt	-2	int	[RFC-XXXX]
group_mode	-3	True or False	[RFC-XXXX]
gp_enc_alg	-4	Null or tstr or int	[RFC-XXXX]
sign_alg	-5	Null or tstr or int	[RFC-XXXX]
sign_params	-6	Null or array	[RFC-XXXX]
pairwise_mode	-7	True or False	[RFC-XXXX]
alg	-8	Null or tstr or int	[RFC-XXXX]
ecdh_alg	-9	Null or tstr or int	[RFC-XXXX]
ecdh_params	-10	Null or array	[RFC-XXXX]
det_req	-25	True or False	[RFC-XXXX]
det_hash_alg	-26	tstr or int	[RFC-XXXX]
rt	-11	tstr	[RFC-XXXX]
active	-12	True or False	[RFC-XXXX]



group_name	-13	tstr or #6.<uint>(any)	[RFC-XXXX]
group_description	-14	Null or tstr	[RFC-XXXX]
max_stale_sets	-15	uint	[RFC-XXXX]
gid_reuse	-16	True or False	[RFC-XXXX]
app_groups	-17	array	[RFC-XXXX]
joining_uri	-18	tstr	[RFC-XXXX]
as_uri	-19	tstr	[RFC-XXXX]
conf_filter	-27	array	[RFC-XXXX]
app_groups_diff	-28	array	[RFC-XXXX]

Table 2: ACE Groupcomm Parameters

The following holds for the Group Manager.

- \* It MUST support the parameters 'ace\_groupcomm\_profile', 'exp', and 'group\_policies', which are defined in Section 8 of [RFC9594].

This is consistent with what is defined in Section 8 of [RFC9594] 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 Table 2, 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 'ace\_groupcomm\_profile', 'exp', and 'group\_policies', which are defined in Section 8 of [RFC9594].
- \* It MUST support all the parameters listed in Table 2, 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 [RFC9594], this document defines new values that the Group Manager can use as error identifiers. These are used in error responses with Content-Format application/concise-problem-details+cbor [RFC9290], as values of the 'error-id' field within the Custom Problem Detail entry 'ace-groupcomm-error' (see Section 4.1.2 of [RFC9594]).

Value	Description	Reference
10	Group currently active	[RFC-XXXX]
11	Unable to determine a group name	[RFC-XXXX]
12	Unsupported group configuration	[RFC-XXXX]

Table 3: ACE Groupcomm Error Identifiers

If the Administrator supports the problem-details format [RFC9290] and the Custom Problem Detail entry 'ace-groupcomm-error' defined in Section 4.1.2 of [RFC9594], and is able to understand the error specified in the 'error-id' field therein, then the Administrator may use that information to determine what actions to take next. If the Concise Problem Details data item specified in the error response includes the 'detail' entry and the Administrator supports it, such an entry 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 making the group name available again before the Administrator sends the new POST request. Hence, this option is not viable if it is unacceptable for the Administrator to considerably or indefinitely postpone the creation of the new group.
  - 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.

In order to not inadvertently suggest a new group name that is already assigned to an existing OSCORE group, the Administrator can first retrieve the list of existing groups from the Group Manager, as defined in Section 6.1. In the payload of the response from the Group Manager, each specified link indicates the name of an existing OSCORE group as the last segment of its url-path.

The Administrator should choose the new group name `GROUPNAME` to suggest, in such a way that it does not renounce permissions that were granted per the old group name `GROUPNAME*`. This is the case if the following holds.

With reference to the 'scope' claim of the Administrator's Access Token, let us define `PERM*` as the union of the permission sets associated with the scope entries such that `GROUPNAME*` matches with the specified group name pattern. Also, let us define `PERM` as the union of the permission sets associated with the scope entries such that `GROUPNAME` matches with the specified group name pattern. Then, `PERM` specifies no fewer permissions than `PERM*`.

- 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 'detail' entry of the Concise Problem Details data item [RFC9290] specified in 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 'detail' entry of the Concise Problem Details data item [RFC9290] specified in 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 [RFC9594] and [I-D.ietf-ace-key-groupcomm-oscure] 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-oscure], 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.

- \* Following the enforcement of a new group configuration, a group member might not deem 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 from 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 [RFC9594], a compromised Group Manager would allow an adversary to also monitor the group configurations specified by an Administrator, or to enforce group configurations different from 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 [RFC9594]).

Unlike what is defined in Section 10.2 of [RFC9594] 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 within the "Authentication and Authorization for Constrained Environments (ACE)" registry group.

- \* Name: hkdf
- \* CBOR Key: -1 (suggested)
- \* CBOR Type: tstr or int
- \* Reference: [RFC-XXXX]
  
- \* Name: cred\_fmt
- \* CBOR Key: -2 (suggested)
- \* CBOR Type: int
- \* Reference: [RFC-XXXX]
  
- \* Name: group\_mode
- \* CBOR Key: -3 (suggested)
- \* CBOR Type: True or False
- \* Reference: [RFC-XXXX]
  
- \* Name: gp\_enc\_alg
- \* CBOR Key: -4 (suggested)
- \* CBOR Type: Null or tstr or int

- \* Reference: [RFC-XXXX]
  
- \* Name: sign\_alg
- \* CBOR Key: -5 (suggested)
- \* CBOR Type: Null or tstr or int
- \* Reference: [RFC-XXXX]
  
- \* Name: sign\_params
- \* CBOR Key: -6 (suggested)
- \* CBOR Type: Null or array
- \* Reference: [RFC-XXXX]
  
- \* Name: pairwise\_mode
- \* CBOR Key: -7 (suggested)
- \* CBOR Type: True or False
- \* Reference: [RFC-XXXX]
  
- \* Name: alg
- \* CBOR Key: -8 (suggested)
- \* CBOR Type: Null or tstr or int
- \* Reference: [RFC-XXXX]
  
- \* Name: ecdh\_alg
- \* CBOR Key: -9 (suggested)



- \* CBOR Type: Null or tstr or int

- \* Reference: [RFC-XXXX]

- \* Name: ecdh\_params

- \* CBOR Key: -10 (suggested)

- \* CBOR Type: Null or array

- \* Reference: [RFC-XXXX]

- \* Name: det\_req

- \* CBOR Key: -25 (suggested)

- \* CBOR Type: True or False

- \* Reference: [RFC-XXXX]

- \* Name: det\_hash\_alg

- \* CBOR Key: -26 (suggested)

- \* CBOR Type: tstr or int

- \* Reference: [RFC-XXXX]

- \* Name: rt

- \* CBOR Key: -11 (suggested)

- \* CBOR Type: tstr

- \* Reference: [RFC-XXXX]

- \* Name: active

- \* CBOR Key: -12 (suggested)
- \* CBOR Type: True or False
- \* Reference: [RFC-XXXX]
  
- \* Name: group\_name
- \* CBOR Key: -13 (suggested)
- \* CBOR Type: tstr or #6.<uint>(any)
- \* Reference: [RFC-XXXX]
  
- \* Name: group\_description
- \* CBOR Key: -14 (suggested)
- \* CBOR Type: Null or tstr
- \* Reference: [RFC-XXXX]
  
- \* Name: max\_stale\_sets
- \* CBOR Key: -15 (suggested)
- \* CBOR Type: uint
- \* Reference: [RFC-XXXX]
  
- \* Name: gid\_reuse
- \* CBOR Key: -16 (suggested)
- \* CBOR Type: True or False
- \* Reference: [RFC-XXXX]

- \* Name: app\_groups
- \* CBOR Key: -17 (suggested)
- \* CBOR Type: array
- \* Reference: [RFC-XXXX]

- \* Name: joining\_uri
- \* CBOR Key: -18 (suggested)
- \* CBOR Type: tstr
- \* Reference: [RFC-XXXX]

- \* Name: as\_uri
- \* CBOR Key: -19 (suggested)
- \* CBOR Type: tstr
- \* Reference: [RFC-XXXX]

- \* Name: conf\_filter
- \* CBOR Key: -27 (suggested)
- \* CBOR Type: array
- \* Reference: [RFC-XXXX]

- \* Name: app\_groups\_diff
- \* CBOR Key: -28 (suggested)
- \* CBOR Type: array
- \* Reference: [RFC-XXXX]

## 10.2. ACE Groupcomm Errors

IANA is asked to register the following entries in the "ACE Groupcomm Errors" registry within the "Authentication and Authorization for Constrained Environments (ACE)" registry group.

- \* Value: 10 (suggested)
- \* Description: Group currently active
- \* Reference: [RFC-XXXX]
  
- \* Value: 11 (suggested)
- \* Description: Unable to determine a group name
- \* Reference: [RFC-XXXX]
  
- \* Value: 12 (suggested)
- \* Description: Unsupported group configuration
- \* Reference: [RFC-XXXX]

## 10.3. Resource Types

IANA is asked to enter the following entries 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" (see Section 4.5 of [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 Table 1. 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-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-12, 21 October 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-core-groupcomm-bis-12>>.

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

Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and R. Hglund, "Group Object Security for Constrained RESTful Environments (Group OSCORE)", Work in Progress, Internet-Draft, draft-ietf-core-oscore-groupcomm-23, 26 September 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-groupcomm-23>>.

[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>>.

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

[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>>.
- [RFC9290] Fossati, T. and C. Bormann, "Concise Problem Details for Constrained Application Protocol (CoAP) APIs", RFC 9290, DOI 10.17487/RFC9290, October 2022, <<https://www.rfc-editor.org/rfc/rfc9290>>.
- [RFC9485] Bormann, C. and T. Bray, "I-Regexp: An Interoperable Regular Expression Format", RFC 9485, DOI 10.17487/RFC9485, October 2023, <<https://www.rfc-editor.org/rfc/rfc9485>>.
- [RFC9594] Palombini, F. and M. Tiloca, "Key Provisioning for Group Communication Using Authentication and Authorization for Constrained Environments (ACE)", RFC 9594, DOI 10.17487/RFC9594, September 2024, <<https://www.rfc-editor.org/rfc/rfc9594>>.

## 11.2. Informative References

- [I-D.amsuess-core-cachable-oscore]  
Amsuess, C. and M. Tiloca, "Cacheable OSCORE", Work in Progress, Internet-Draft, draft-amsuess-core-cachable-oscore-09, 8 July 2024, <<https://datatracker.ietf.org/doc/html/draft-amsuess-core-cachable-oscore-09>>.

[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-09, 22 September 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-ace-revoked-token-notification-09>>.

[I-D.ietf-cose-cbor-encoded-cert]

Mattsson, J. P., Selander, G., Raza, S., Hglund, J., and M. Furuheid, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-11, 8 July 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-11>>.

[I-D.tiloca-core-oscore-discovery]

Tiloca, M., Ams端ss, 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-16, 4 September 2024, <<https://datatracker.ietf.org/doc/html/draft-tiloca-core-oscore-discovery-16>>.

[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] Ams端ss, 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 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.

This appendix provides an example of how the AS can evaluate the requested permissions against the access policies pertaining to the Administrator for the Group Manager in question.

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

Also, it is assumed that the AS stores the access policies as a set of "admin policy entries", which have the same format of the scope entries according to the AIF data model AIF-OSCORE-GROUPCOMM (see Section 3). The following specifically considers only "admin policy entries", i.e., policy entries for Administrators of OSCORE groups hereafter shortly referred to as "policy entries".

The AS performs the following steps.

1. The AS initializes three empty sets of scope entries, namely S\_OUT.
2. For each scope entry E\_S in the 'scope' parameter of the Authorization Request, the AS performs the following actions.
  - a. The AS initializes an empty set of policy entries, namely S\_AUX.
  - b. The AS considers all the policy entries related to the Administrator and the Group Manager in question. For each policy entry E\_P among those policy entries, the AS determines whether

every group name matching with the Toid of E\_S would also match with the Toid of E\_P. If that is the case, then the AS adds E\_P to the set S\_AUX. The particular way that the AS uses to make a determination is implementation specific.

c. If the set S\_AUX is empty, the AS proceeds with the next scope entry, if any. Otherwise, the AS computes TPERM\_AUX as the union of the permission sets associated with the policy entries in the set S\_AUX. That is, TPERM\_AUX is the inclusive OR of the binary representation of the Tperm values in the policy entries within the set S\_AUX.

d. The AS adds to the set S\_OUT one scope entry, such that its Toid is the same as in the scope entry E\_S, while its Tperm is the AND of TPERM\_AUX with the Tperm in the scope entry E\_S.

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

a. The AS initializes an empty set of policy entries, namely S\_AUX.

b. The AS considers all the policy entries related to the Administrator and the Group Manager in question. For each policy entry E\_P among those policy entries, and such that the Toid of E\_P is different from the Toid of E\_S, the AS determines whether every group name matching with the Toid of E\_P would also match with the Toid of E\_S. If that is the case, then the AS adds E\_S to the set S\_AUX. The particular way that the AS uses to make a determination is implementation specific.

c. If the set S\_AUX is empty, the AS proceeds with the next scope entry, if any. Otherwise, the AS adds to the set S\_OUT one scope entry, such that its Toid is the same as in the policy entry E\_P, while its Tperm is the AND of the Tperm in the policy entry E\_P with the Tperm in the scope entry E\_S.

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

- a. The AS considers all the policy entries related to the Administrator and the Group Manager in question, such that they were never added to the set `S_AUX` during the previous steps 2 and 3. For each policy entry `E_P` among those policy entries, the AS attempts to determine a group name pattern `TOID_AUX` such that every group name matching with `TOID_AUX` would also match with the Toid of `E_P` as well as with the Toid of `E_S`. The particular way that the AS uses to make a determination is implementation specific.
  - b. If the AS could not determine a group name pattern `TOID_AUX`, then the AS proceeds with the next policy entry `E_P`, if any. Otherwise, the AS adds to the set `S_OUT` one scope entry, such that its Toid is `TOID_AUX`, while its Tperm is the AND of the Tperm in the policy entry `E_P` with the Tperm in the scope entry `E_S`.
5. If the set `S_OUT` is 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 set `S_OUT` as the scope entries for the 'scope' claim to include in the Access Token, as per the format defined in Section 3.

#### Appendix B. CDDL Model

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

```
hkdf = -1
cred_fmt = -2
group_mode = -3
gp_enc_alg = -4
sign_alg = -5
sign_params = -6
pairwise_mode = -7
alg = -8
ecdh_alg = -9
ecdh_params = -10
det_req = -25
det_hash_alg = -26
rt = -11
active = -12
group_name = -13
group_description = -14
max_stale_sets = -15
gid_reuse = -16
app_groups = -17
joining_uri = -18
as_uri = -19
conf_filter = -27
app_groups_diff = -28

ace_groupcomm_profile = 10
exp = 11
```

Figure 3: CDDL model

## Appendix C. Document Updates

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

### C.1. Version -12 to -13

- \* Uri-Path and Location-Path as text strings in examples.
- \* Removed moot reference to Section 3.4.5.3 of RFC 8949.
- \* Fixed example to correctly use the I-Regexp flavor from RFC 9485.
- \* Highlighted that values to register for IANA are suggested.
- \* Updated references.
- \* Editorial fixes.

## C.2. Version -11 to -12

- \* CBOR diagnostic notation uses placeholders from a CDDL model.
- \* Clarified relation between group name and URI path segment.
- \* /manage is a url-path chosen as an example, but not a default one.
- \* Recapped concepts of scope and secure communication association.
- \* Main/optional Administrator is presented more as an example.
- \* The use of CBOR Tag 35 is not mentioned anymore.
- \* Added considerations on race conditions with multiple Administrators.
- \* Clarified requirement for some operations to be atomic.
- \* Early centralization of what it means to have permissions.
- \* Improved presentation of default values for the parameters.
- \* POST (instead of PUT) for overwriting a group-configuration resource.
- \* Example of inconsistent configuration following a PATCH request.
- \* Clarified invalid semantics of an iPATCH request.
- \* Repositioned text from security to operational considerations.
- \* Revised appendix with an example of name pattern processing at the AS.
- \* Minor clarifications and editorial improvements.

## C.3. Version -10 to -11

- \* Early mentioned that issued Access Tokens can have other purposes.
- \* Added example of array of scope entries.
- \* Removed moot paragraph about the benefits of group name patterns.
- \* Use of CBOR tag 21065 to indicate a regular expression.
- \* Renamed 'group\_title' as 'group\_description'.

- \* Added a second example of FETCH to the group-collection resource.
- \* Avoiding accidental deactivation of a group when updating it.
- \* Avoid alternative ways to create a group configuration resource.
- \* RFC 9290 is used instead of the custom format for error responses.
- \* Added integer abbreviations for the new entries in the "ACE Groupcomm Parameters" registry.
- \* Editorial fixes and improvements.

#### C.4. Version -09 to -10

- \* Consistent use of 4.03 (Forbidden) error responses.
- \* Removed moot, remnant statements from when CoRAL was used.
- \* Clarified how the Group Manager may attempt to determine an alternative group name upon creating a new group.
- \* Made explicit what parameters cannot change when overwriting a group configuration.
- \* Improved guidelines to the Group Manager on selecting an alternative group name.
- \* Improved guidelines to Administrators receiving an error after trying to create a new group.
- \* Changed description of error 11 from "No available group names" to "Unable to determine a group name".
- \* Editorial fixes and improvements.

#### C.5. 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.

#### C.6. 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.

#### C.7. 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.

#### C.8. Version -05 to -06

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

- \* Revised Client-AS interaction, based on the used AIF 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.

#### C.9. 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.

#### C.10. 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.

#### C.11. 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".

#### C.12. 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.

#### C.13. 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 Ams<sup>端</sup>ss, Carsten Bormann, Jim Schaad, G<sup>端</sup>ran Selander, and Cigdem Sengul for their comments and feedback.

The work on this document has been partly supported by the Sweden's Innovation Agency VINNOVA and the Celtic-Next projects CRITISEC and CYPRESS; 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 H<sup>端</sup>glund  
RISE AB  
Isafjordsgatan 22  
SE-16440 Stockholm Kista  
Sweden  
Email: rikard.hoglund@ri.se

Peter van der Stok  
Email: stokcons@kpnmail.nl

Francesca Palombini  
Ericsson AB  
Torshamnsgatan 23  
SE-16440 Stockholm Kista  
Sweden  
Email: francesca.palombini@ericsson.com