ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 11 July 2026

M. Tiloca
R. H旦glund
RISE AB

7 January 2026

Using the Constrained RESTful Application Language (CoRAL) with the Admin Interface for the OSCORE Group Manager
draft-ietf-ace-oscore-gm-admin-coral-05

Abstract

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

Discussion Venues

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

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

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

Status of This Memo

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

This Internet-Draft will expire on 11 July 2026.

Copyright Notice

Table of Contents

1. Introduction

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

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

The method in [I-D.ietf-ace-key-groupcomm-oscore] specifies how nodes can join an OSCORE group through the respective Group Manager. Such a method builds on the ACE framework for Authentication and Authorization [RFC9200], so ensuring a secure joining process as well as authentication and authorization of joining nodes (clients) at the Group Manager (resource server).

Furthermore, [I-D.ietf-ace-oscore-gm-admin] specifies a RESTful admin interface at the Group Manager, which is intended for an Administrator as a separate entity external to the Group Manager and its application. The interface allows the Administrator to create and delete OSCORE groups, as well as to configure and update their configuration.

This document builds on [I-D.ietf-ace-oscore-gm-admin] and specifies how an Administrator interacts with the same RESTful admin interface by using the Constrained RESTful Application Language (CoRAL) [I-D.ietf-core-coral]. Compared to [I-D.ietf-ace-oscore-gm-admin], there is no change in the admin interface and its operations, nor in the way the group configurations are organized and represented.

Interaction examples using Packed CBOR [I-D.ietf-cbor-packed] are provided and are expressed in CBOR diagnostic notation as defined in Section 8 of [RFC8949] and Appendix G of [RFC8610]. Section 1.2 provides the notation and assumptions used in the examples.

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] or [RFC9203]. These also include 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.

* Concise Binary Object Representation (CBOR) [RFC8949], Packed CBOR [I-D.ietf-cbor-packed], and CBOR Object Signing and Encryption (COSE) [RFC9052][RFC9053].

* The Constrained RESTful Application Language (CoRAL) [I-D.ietf-core-coral] and Constrained Resource Identifiers (CRIs) [I-D.ietf-core-href].

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

  - "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 security protocols OSCORE [RFC8613] and Group OSCORE [I-D.ietf-core-oscore-groupcomm]. These especially include the concepts below:

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

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

* The ACE framework for Authentication and Authorization [RFC9200]. The terminology for entities in the considered architecture is defined in OAuth 2.0 [RFC6749]. In particular, this includes client (C), resource server (RS), and authorization server (AS).

* The management of keying material for groups in ACE [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. Candidate group members access such a resource to join the OSCORE group, while current group members can access it to retrieve updated keying material.

Readers are also expected to be familiar with the terms and concepts used in [I-D.ietf-ace-oscore-gm-admin], with particular reference to "Administrator", "group name", "group-collection resource", and "group-configuration resource".

Like in [I-D.ietf-ace-oscore-gm-admin], this document uses /manage as the url-path of the group-collection resource at the Group Manager when providing examples; implementations can use a different url-path. Building on that, this document uses /manage/GROUPNAME as the url-path of a group-configuration resource; implementations are not required to use this name and can define their own instead.

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. The CoAP definition, which is "[a]n entity participating in the CoAP protocol" [RFC7252], is not used in this document.

1.2. Notation and Assumptions Used in the Examples

As per Section 2.4 of [I-D.ietf-core-coral], CoRAL expresses Uniform Resource Identifiers (URIs) [RFC3986] as Constrained Resource Identifier (CRI) references [I-D.ietf-core-href].

Examples in this document use the following notation.

When using the CURIE syntax [CURIE-20101216], the following applies.

* 'core.osc.gcoll' stands for http://coreapps.org/core.osc.gcoll

* 'core.osc.gconf' stands for http://coreapps.org/core.osc.gconf

* 'linkformat' stands for http://www.iana.org/assignments/linkformat/

  This URI is to be defined with IANA, together with other URIs that build on it through further path segments, e.g., http://www.iana.org/assignments/linkformat/rt

When using a URI http://www.iana.org/assignments/linkformat/SEG1/SEG2

* The path segment SEG1 is the name of a web link target attribute.

  Names of target attributes used in Link Format [RFC6690] are expected to be coordinated through the "Target Attributes" registry defined in [RFC9423].

* The path segment SEG2 is the value of the target attribute.

The application-extension identifier "cri" defined in Section 3.4 of [I-D.ietf-cbor-edn-literals] is used to notate a CBOR Extended Diagnostic Notation (EDN) literal for a CRI or CRI reference. This format is not expected to be sent over the network.

Packed CBOR [I-D.ietf-cbor-packed] is also used, thus reducing representation size. Examples in this document especially refer to the values from the two shared item tables in Appendix A.

Finally, examples in this document consider a Group Manager with address [2001:db8::ab] and use the CoAP Content-Format ID 65087 for the media type "application/coral+cbor".

2. Group Administration

The group administration is enforced as defined in Section 2 of [I-D.ietf-ace-oscore-gm-admin].

2.1. Managing OSCORE Groups

This document uses the same resource model defined in Section 2.1 of [I-D.ietf-ace-oscore-gm-admin], which is based on a group-collection resource and multiple group-configuration resources.

When accessing such resources, the Administrator relies on the same interface defined in Section 6 of [I-D.ietf-ace-oscore-gm-admin], for which differences that apply when using CoRAL are compiled in Section 6 of this document.

2.2. Collection Representation

A collection of group configurations is represented as a CoRAL document containing the list of corresponding group-configuration resources.

Each group configuration is represented as a top-level link element, with the URI of the group-configuration resource as link target and with http://coreapps.org/core.osc.gcoll#item as relation type.

2.3. Discovery

The Administrator can discover the group-collection resource from a Resource Directory (see, for instance, [I-D.hartke-t2trg-coral-reef]) or from /.well-known/core, by using the resource type "core.osc.gcoll" registered in Section 10.3 of [I-D.ietf-ace-oscore-gm-admin].

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

3. Format of Scope

In order to express authorization information for the Administrator (see Section 4), the same format and encoding of scope defined in Section 3 of [I-D.ietf-ace-oscore-gm-admin] is used, as relying on the Authorization Information Format (AIF) [RFC9237] and the extended AIF data model AIF-OSCORE-GROUPCOMM defined in Section 3 of [I-D.ietf-ace-key-groupcomm-oscore].

4. Getting Access to the Group Manager

All communications between the involved entities rely on CoAP 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 specifically used and are out of the scope of this document.

The Administrator requests access to the Group Manager as per Steps 1-3 in Section 4 of [I-D.ietf-ace-oscore-gm-admin].

The Administrator accesses the admin interface at the Group Manager as per Step 4 in Section 4 of [I-D.ietf-ace-oscore-gm-admin], with the difference that administrative operations are not performed as defined in Section 6 of [I-D.ietf-ace-oscore-gm-admin], but instead as defined in Section 6 of this document.

4.1. Multiple Administrators for the Same OSCORE Group

What is defined in Section 4.1 of [I-D.ietf-ace-oscore-gm-admin] also holds for this document, with the following difference.

The Administrator performs administrative operations at the Group Manager not as defined in Section 6 of [I-D.ietf-ace-oscore-gm-admin], but instead as defined in Section 6 of this document.

5. Group Configurations

A group configuration consists of a set of parameters.

5.1. Group Configuration Representation

The same group configuration representation defined in Section 5.1 of [I-D.ietf-ace-oscore-gm-admin] is used, as including configuration parameters and status parameters.

5.1.1. Configuration Parameters

The same configuration parameters defined in Section 5.1.1 of [I-D.ietf-ace-oscore-gm-admin] are used.

5.1.2. Status Parameters

The same status parameters defined in Section 5.1.2 of [I-D.ietf-ace-oscore-gm-admin] are used.

5.2. Default Values

The Group manager refers to the same default values defined in Section 5.2 of [I-D.ietf-ace-oscore-gm-admin].

6. Interactions with the Group Manager

The same as defined in Section 6 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* The Content-Format in messages containing a payload is set to application/coral+cbor, which is registered in Section 7.2 of [I-D.ietf-core-coral].

* The parameters ’sign_params’, ’ecdh_params’, ’app_groups’, and ’group_policies’ are referred to as "structured parameters".

* If a message payload specifies a link element corresponding to a structured parameter, then the following applies:

  - The payload MUST NOT include any link element corresponding to an inner information element of that structured parameter.

- The link element MUST have the link target with value the CBOR simple value false (0xf4) for indicating the structured parameter with no elements.

  Editor’s note: this should change to using an empty CBOR array or an empty CBOR map as appropriate, once this is made explicitly possible in the binary format of link items in CoRAL (see Section 3.1.4 of [I-D.ietf-core-coral]).

* If a message payload specifies an information element of a structured parameter from the group configuration, then that information element MUST be specified by means of the corresponding link element.

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.

The same as defined in Section 6.1 of [I-D.ietf-ace-oscore-gm-admin] holds.

An example of message exchange is shown below.

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

   <= 2.05 Content
      Content-Format: 65087 (application/coral+cbor)

      Payload:

      [
        [1, cri'coap://[2001:db8::ab]/manage'],
        [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp1', [
          [2, simple(6) / item 6 for linkformat:rt /,
           6(-200) / item 415 for cri'http://www.iana.org/assignments
                                    /linkformat/rt/core.osc.gconf' /]]
        ],
        [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp2', [
          [2, simple(6) / item 6 for linkformat:rt /,
           6(-200) / item 415 for cri'http://www.iana.org/assignments
                                    /linkformat/rt/core.osc.gconf' /]]
        ],
        [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp3', [
          [2, simple(6) / item 6 for linkformat:rt /,
           6(-200) / item 415 for cri'http://www.iana.org/assignments
                                    /linkformat/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.

The same as defined in Section 6.2 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* The filter criteria are specified in the request payload with top-level link elements, each of which corresponds to an entry of the group configuration (see Section 5.1), with the exception of non-empty structured parameters.

* If names of application groups are used as filter criteria, each element of the 'app_groups' array from the status parameters is included as a separate link element with name 'app_group'.

* With the exception of the 'app_group' element, a valid request MUST NOT include the same element multiple times. Element values are the ones admitted for the corresponding labels in the POST request for creating a group configuration (see Section 6.3).

An example of message exchange is shown below.

```
=> 0.05 FETCH
   Uri-Path: "manage"
   Content-Format: 65087 (application/coral+cbor)

   Payload:

   [
     [2, 6(27) / item 70 for core.osc.gconf:#group_mode /, true],
     [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 10],
     [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, 5]
   ]

<= 2.05 Content
   Content-Format: 65087 (application/coral+cbor)

   Payload:

   [
    [1, cri'coap://[2001:db8::ab]/manage'],
    [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp1', [
      [2, simple(6) / item 6 for linkformat:rt /,
       6(-200) / item 415 for cri'http://www.iana.org/assignments
                                 /linkformat/rt/core.osc.gconf' /]]
    ],
    [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp2', [
      [2, simple(6) / item 6 for linkformat:rt /,
       6(-200) / item 415 for cri'http://www.iana.org/assignments
                                 /linkformat/rt/core.osc.gconf' /]]
    ],
    [2, 6(17) / item 50 for core.osc.gcoll:#item /, cri'/gp3', [
      [2, simple(6) / item 6 for linkformat:rt /,
       6(-200) / item 415 for cri'http://www.iana.org/assignments
                                 /linkformat/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 same as defined in Section 6.3 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* In the request payload, each link element corresponds to an entry of the group configuration (see Section 5.1), with the exception of non-empty structured parameters.

* In the request payload, each element of the 'app_groups' array from the status parameters is included as a separate element with name 'app_group'.

* The Group Manager MUST respond with a 4.00 (Bad Request) response if any link element is specified multiple times in the payload of the POST request, with the exception of the 'app_group' link element.

* The response payload includes one link element for each specified parameter, with the exception of non-empty structured parameters.

* In the response payload, each element of the 'app_groups' array from the status parameters is included as a separate element with name 'app_group'.

* If the Administrator performs the registration of the group-membership resource to a Resource Directory on behalf of the Group Manager, then the names of the application groups using the OSCORE group MUST take the values possibly specified by the different 'app_group' link elements in the POST request.

An example of message exchange is shown below.

```
   => 0.02 POST
      Uri-Path: "manage"
      Content-Format: 65087 (application/coral+cbor)

      Payload:

      [
        [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 10],
        [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, 5],
        [2, 6(-31) / item 77 for core.osc.gconf:#pairwise_mode /, true],
        [2, 6(-36) / item 87 for core.osc.gconf:#active /, true],
        [2, 6(36) / item 88 for core.osc.gconf:#group_name /, "gp4"],
        [2, 6(-37) / item 89 for core.osc.gconf:#group_description /,
         "rooms 1 and 2"],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 1"],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 2"],
        [2, 6(43) / item 102 for core.osc.gconf:#as_uri /,
         cri'coap://as.example.com/token']
      ]

   <= 2.01 Created
      Location-Path: "manage"
      Location-Path: "gp4"
      Content-Format: 65087 (application/coral+cbor)

      Payload:

      [
        [2, 6(36) / item 88 for core.osc.gconf:#group_name /, "gp4"],
        [2, 6(-41) / item 97 for core.osc.gconf:#joining_uri /,
         cri'coap://[2001:db8::ab]/ace-group/gp4/'],
        [2, 6(43) / item 102 for core.osc.gconf:#as_uri /,
         cri'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.

The same as defined in Section 6.4 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* The response payload includes one link element for each entry of the group configuration (see Section 5.1), with the exception of non-empty status parameters.

* Each element of the 'app_groups' array from the status parameters is included as a separate link element with name 'app_group'.

An example of message exchange is shown below.

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

<= 2.05 Content
   Content-Format: 65087 (application/coral+cbor)

   Payload:

   [
     [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, 5],
     [2, 6(-27) / item 69 for core.osc.gconf:#cred_fmt /, 33],
     [2, 6(27) / item 70 for core.osc.gconf:#group_mode /, true],
     [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 10],
     [2, 6(28) / item 72 for core.osc.gconf:#sign_alg /, -8],
     [2, 6(29) / item 74 for
      core.osc.gconf:#sign_params.alg_capab.key_type /, 1],
     [2, 6(-30) / item 75 for
      core.osc.gconf:#sign_params.key_type_capab.key_type /, 1],
     [2, 6(30) / item 76 for
      core.osc.gconf:#sign_params.key_type_capab.curve /, 6],
     [2, 6(-31) / item 77 for core.osc.gconf:#pairwise_mode /, true],
     [2, 6(31) / item 78 for core.osc.gconf:#alg /, 10],
     [2, 6(-32) / item 79 for core.osc.gconf:#ecdh_alg /, -27],
     [2, 6(-33) / item 81 for
      core.osc.gconf:#ecdh_params.alg_capab.key_type /, 1],
     [2, 6(33) / item 82 for
      core.osc.gconf:#ecdh_params.key_type_capab.key_type /, 1],
     [2, 6(-34) / item 83 for
      core.osc.gconf:#ecdh_params.key_type_capab.curve /, 6],
     [2, 6(34) / item 84 for core.osc.gconf:#det_req /, false],
     [2, 6(35) / item 86 for core.osc.gconf:#rt /, "core.osc.gconf"],
     [2, 6(-36) / item 87 for core.osc.gconf:#active /, true],
     [2, 6(36) / item 88 for core.osc.gconf:#group_name /, "gp4"],
     [2, 6(-37) / item 89 for core.osc.gconf:#group_description /,
      "rooms 1 and 2"],
     [2, 6(37) / item 90 for core.osc.gconf:#ace_groupcomm_profile /,
      "coap_group_oscore_app"],
     [2, 6(-38) / item 91 for core.osc.gconf:#max_stale_sets /, 3],
```

```
        [2, 6(38) / item 92 for core.osc.gconf:#exp /, 1360289224],
        [2, 6(-39) / item 93 for core.osc.gconf:#gid_reuse /, false],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 1"],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 2"],
        [2, 6(-41) / item 97 for core.osc.gconf:#joining_uri /,
         cri'coap://[2001:db8::ab]/ace-group/gp4/'],
        [2, 6(43) / item 102 for core.osc.gconf:#as_uri /,
         cri'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 same as defined in Section 6.5 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* The request payload includes one link element for each requested configuration parameter or status parameter of the current group configuration (see Section 5.1). All the specified link elements MUST have the link target with value the CBOR simple value null (0xf6).

* The request payload MUST NOT include any link element corresponding to an inner information element of a structured parameter.

* The response payload includes the requested configuration parameters and status parameters, and is formatted like 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 link element.

An example of message exchange is shown below.

```
   => 0.05 FETCH
      Uri-Path: "manage"
      Uri-Path: "gp4"
      Content-Format: 65087 (application/coral+cbor)

      Payload:

      [
        [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, null],
        [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, null],
        [2, 6(-31) / item 77 for core.osc.gconf:#pairwise_mode /, null],
        [2, 6(-36) / item 87 for core.osc.gconf:#active /, null],
        [2, 6(-37) / item 89 for core.osc.gconf:#group_description /,
         null],
        [2, 6(41) / item 98 for core.osc.gconf:#app_groups /, null]
      ]

   <= 2.05 Content
      Content-Format: 65087 (application/coral+cbor)

      Payload:

      [
        [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 10],
        [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, 5],
        [2, 6(-31) / item 77 for core.osc.gconf:#pairwise_mode /, true],
        [2, 6(-36) / item 87 for core.osc.gconf:#active /, true],
        [2, 6(-37) / item 89 for core.osc.gconf:#group_description /,
         "rooms 1 and 2"],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 1"],
        [2, 6(39) / item 94 for core.osc.gconf:#app_group /, "room 2"]
      ]
```

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 same as defined in Section 6.6 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following difference.

* If the Administrator updates the registration of the group-membership resource in the Resource Directory on behalf of the Group Manager, then the names of the application groups using the OSCORE group MUST take the values possibly specified by the different 'app_group' link elements in the POST request.

An example of message exchange is shown below.

```
=> 0.02 POST
   Uri-Path: "manage"
   Uri-Path: "gp4"
   Content-Format: 65087 (application/coral+cbor)

   Payload:

   [
     [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 11],
     [2, 6(26) / item 68 for core.osc.gconf:#hkdf /, 5]
   ]

<= 2.04 Changed
   Content-Format: 65087 (application/coral+cbor)

   Payload:

   [
     [2, 6(36) / item 88 for core.osc.gconf:#group_name /, "gp4"],
     [2, 6(-41) / item 97 for core.osc.gconf:#joining_uri /,
      cri'coap://[2001:db8::ab]/ace-group/gp4/'],
     [2, 6(43) / item 102 for core.osc.gconf:#as_uri /,
      cri'coap://as.example.com/token']
   ]
```

6.6.1. Effects on Joining Nodes

The same as defined in Section 6.6.1 of [I-D.ietf-ace-oscore-gm-admin] holds.

6.6.2. Effects on the Group Members

The same as defined in Section 6.6.2 of [I-D.ietf-ace-oscore-gm-admin] holds.

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 same as defined in Section 6.7 of [I-D.ietf-ace-oscore-gm-admin] holds, with the following differences.

* If the request payload specifies names of application groups to be removed from or added to the 'app_groups' status parameter, then such names are specified by means of the following top-level link elements.

  - 'app_group_del', with value a text string specifying the name of an application group to remove from the 'app_groups' status parameter. This link element can be included multiple times.

  - 'app_group_add', with value a text string specifying the name of an application group to add to the 'app_groups' status parameter. This link element can be included multiple times.

  The Group Manager MUST respond with a 4.00 (Bad Request) response, if the request payload includes any 'app_group' link element together with any 'app_group_del' and/or 'app_group_add' link element.

* The Group Manager MUST respond with a 4.00 (Bad Request) response, if the request payload includes no link elements.

* When the request uses specifically the iPATCH method, the Group Manager MUST respond with a 4.00 (Bad Request) response, if any link element 'app_group_del' and/or 'app_group_add' is included.

* When updating the 'app_groups' status parameter by difference, the Group Manager:

  - Deletes from the 'app_groups' status parameter the names of the application groups specified in the different 'app_group_del' link elements.

  - Adds to the 'app_groups' status parameter the names of the application groups specified in the different 'app_group_add' link elements.

An example of message exchange is shown below.

```
 => 0.06 PATCH
    Uri-Path: "manage"
    Uri-Path: "gp4"
    Content-Format: 65087 (application/coral+cbor)

    Payload:

    [
      [2, 6(-28) / item 71 for core.osc.gconf:#gp_enc_alg /, 10],
      [2, 6(-40) / item 95 for core.osc.gconf:#app_group_del /,
       "room1"],
      [2, 6(40) / item 96 for core.osc.gconf:#app_group_add /, "room3"],
      [2, 6(40) / item 96 for core.osc.gconf:#app_group_add /, "room4"]
    ]

 <= 2.04 Changed
    Content-Format: 65087 (application/coral+cbor)

    Payload:

    [
      [2, 6(36) / item 88 for core.osc.gconf:#group_name /, "gp4"],
      [2, 6(-41) / item 97 for core.osc.gconf:#joining_uri /,
       cri'coap://[2001:db8::ab]/ace-group/gp4/'],
      [2, 6(43) / item 102 for core.osc.gconf:#as_uri /,
       cri'coap://as.example.com/token']
    ]
```

6.7.1. Effects on Joining Nodes

The same as defined in Section 6.7.1 of [I-D.ietf-ace-oscore-gm-admin] holds.

6.7.2. Effects on the Group Members

The same as defined in Section 6.7.2 of [I-D.ietf-ace-oscore-gm-admin] holds.

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.

The same as defined in Section 6.8 of [I-D.ietf-ace-oscore-gm-admin] holds.

6.8.1. Effects on the Group Members

The same as defined in Section 6.8.1 of [I-D.ietf-ace-oscore-gm-admin] holds.

7. Support of Top-Level Link Elements

Consistently with Section 7 of [I-D.ietf-ace-oscore-gm-admin], the following holds for the Group Manager.

* It MUST support the top-level link elements 'ace_groupcomm_profile', 'exp', and 'group_policies' corresponding to the ACE Groupcomm Parameters defined in Section 8 of [RFC9594].

  This is consistent with what is defined in Section 8 of [RFC9594] for the Key Distribution Center (KDC), of which the Group Manager defined in [I-D.ietf-ace-key-groupcomm-oscore] is a specific instance.

* It MUST support the top-level link elements corresponding to all the parameters listed in Section 7 of [I-D.ietf-ace-oscore-gm-admin], with the exception of 'app_groups_diff' that 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 top-level link elements 'ace_groupcomm_profile', 'exp', and 'group_policies' corresponding to the ACE Groupcomm Parameters defined in Section 8 of [RFC9594].

* It MUST support the top-level link elements corresponding to all the parameters listed in Section 7 of [I-D.ietf-ace-oscore-gm-admin], 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', which MUST be supported only if the Administrator supports the selective update of a group configuration (see Section 6.7).

8. Error Identifiers

If the Group Manager sends an error response with Content-Format application/concise-problem-details+cbor [RFC9290] as defined in Section 4.1.2 of [RFC9594], then the 'error-id' field within the Custom Problem Detail entry 'ace-groupcomm-error' takes value from those defined in Section 9 of [RFC9594] and in Section 8 of [I-D.ietf-ace-oscore-gm-admin].

The same guidelines in Section 8 of [I-D.ietf-ace-oscore-gm-admin] for the Administrator to handle such error identifiers hold.

9. Security Considerations

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

The same security considerations from [RFC9594] and [I-D.ietf-ace-key-groupcomm-oscore] also apply, with particular reference to the process of rekeying OSCORE groups.

The same security considerations from [I-D.ietf-ace-oscore-gm-admin] also apply, as well as the security considerations for CoRAL [I-D.ietf-core-coral] and Packed CBOR [I-D.ietf-cbor-packed].

10. IANA Considerations

This document has no actions for IANA.

11. References

11.1. Normative References

[CURIE-20101216]
Birbeck, M. and S. McCarron, "CURIE Syntax 1.0 - A syntax for expressing Compact URIs - W3C Working Group Note", 16 December 2010, <http://www.w3.org/TR/2010/NOTE-curie-20101216>.

[I-D.ietf-ace-key-groupcomm-oscore]
Tiloca, M. and F. Palombini, "Key Management for Group Object Security for Constrained RESTful Environments (Group OSCORE) Using Authentication and Authorization for Constrained Environments (ACE)", Work in Progress, Internet-Draft, draft-ietf-ace-key-groupcomm-oscore-18, 28 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-key-groupcomm-oscore-18>.

[I-D.ietf-ace-oscore-gm-admin]
Tiloca, M., H旦glund, R., Van der Stok, P., and F. Palombini, "Admin Interface for the OSCORE Group Manager", Work in Progress, Internet-Draft, draft-ietf-ace-oscore-gm-admin-13, 8 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-oscore-gm-admin-13>.

[I-D.ietf-cbor-edn-literals]
Bormann, C., "CBOR Extended Diagnostic Notation (EDN)", Work in Progress, Internet-Draft, draft-ietf-cbor-edn-literals-19, 16 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cbor-edn-literals-19>.

[I-D.ietf-cbor-packed]
Bormann, C. and M. G端tschow, "Packed CBOR", Work in Progress, Internet-Draft, draft-ietf-cbor-packed-17, 15 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cbor-packed-17>.

[I-D.ietf-core-coral]
Ams端ss, C. and T. Fossati, "The Constrained RESTful Application Language (CoRAL)", Work in Progress, Internet-Draft, draft-ietf-core-coral-06, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-core-coral-06>.

[I-D.ietf-core-groupcomm-bis]
Dijk, E. and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, draft-ietf-core-groupcomm-bis-15, 25 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-groupcomm-bis-15>.

[I-D.ietf-core-href]
Bormann, C. and H. Birkholz, "Constrained Resource Identifiers", Work in Progress, Internet-Draft, draft-

ietf-core-href-30, 21 November 2025,
<https://datatracker.ietf.org/doc/html/draft-ietf-core-href-30>.

[I-D.ietf-core-oscore-groupcomm]
Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and R. H旦glund, "Group Object Security for Constrained RESTful Environments (Group OSCORE)", Work in Progress, Internet-Draft, draft-ietf-core-oscore-groupcomm-28, 23 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-groupcomm-28>.

[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>.

[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>.

[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>.

[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.hartke-t2trg-coral-reef] Hartke, K., "Resource Discovery in Constrained RESTful Environments (CoRE) using the Constrained RESTful Application Language (CoRAL)", Work in Progress, Internet-Draft, draft-hartke-t2trg-coral-reef-04, 9 May 2020, <https://datatracker.ietf.org/doc/html/draft-hartke-t2trg-coral-reef-04>.

[I-D.ietf-cose-cbor-encoded-cert] Mattsson, J. P., Selander, G., Raza, S., H旦glund, J., and M. Furuhed, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-15, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-15>.

[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>.

[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>.

[RFC9423] Bormann, C., "Constrained RESTful Environments (CoRE) Target Attributes Registry", RFC 9423, DOI 10.17487/RFC9423, April 2024, <https://www.rfc-editor.org/rfc/rfc9423>.

Appendix A. Shared Item Tables for Packed CBOR

This appendix defines the two shared item tables that the examples in this document refer to for using Packed CBOR [I-D.ietf-cbor-packed].

The application-extension identifier "cri" defined in Section 3.4 of [I-D.ietf-cbor-edn-literals] is used to notate a CBOR Extended Diagnostic Notation (EDN) literal for a CRI.

A.1. Compacting CoRAL Predicates with Packed CBOR

The following shared item table is used for compacting CoRAL predicates, as per Section 2.2 of [I-D.ietf-cbor-packed].

Index	Item
6	cri'http://www.iana.org/assignments/linkformat/rt'
50	cri'http://coreapps.org/core.osc.gcoll#item'
68	cri'http://coreapps.org/core.osc.gconf#hkdf'
69	cri'http://coreapps.org/core.osc.gconf#cred_fmt'
70	cri'http://coreapps.org/core.osc.gconf#group_mode'
71	cri'http://coreapps.org/core.osc.gconf#gp_enc_alg'
72	cri'http://coreapps.org/core.osc.gconf#sign_alg'
73	cri'http://coreapps.org/core.osc.gconf#sign_params'
74	cri'http://coreapps.org/core.osc.gconf#sign_params .alg_capab.key_type'
75	cri'http://coreapps.org/core.osc.gconf#sign_params .key_type_capab.key_type'
76	cri'http://coreapps.org/core.osc.gconf#sign_params .key_type_capab.curve'
77	cri'http://coreapps.org/core.osc.gconf#pairwise_mode'

78	cri'http://coreapps.org/core.osc.gconf#alg'
79	cri'http://coreapps.org/core.osc.gconf#ecdh_alg'
80	cri'http://coreapps.org/core.osc.gconf#ecdh_params'
81	cri'http://coreapps.org/core.osc.gconf#ecdh_params .alg_capab.key_type'
82	cri'http://coreapps.org/core.osc.gconf#ecdh_params .key_type_capab.key_type'
83	cri'http://coreapps.org/core.osc.gconf#ecdh_params .key_type_capab.curve'
84	cri'http://coreapps.org/core.osc.gconf#det_req'
85	cri'http://coreapps.org/core.osc.gconf#det_hash_alg'
86	cri'http://coreapps.org/core.osc.gconf#rt'
87	cri'http://coreapps.org/core.osc.gconf#active'
88	cri'http://coreapps.org/core.osc.gconf#group_name'
89	cri'http://coreapps.org/ core.osc.gconf#group_description'
90	cri'http://coreapps.org/core.osc.gconf #ace_groupcomm_profile'
91	cri'http://coreapps.org/ core.osc.gconf#max_stale_sets'
92	cri'http://coreapps.org/core.osc.gconf#exp'
93	cri'http://coreapps.org/core.osc.gconf#gid_reuse'
94	cri'http://coreapps.org/core.osc.gconf#app_group'
95	cri'http://coreapps.org/core.osc.gconf#app_group_del'
96	cri'http://coreapps.org/core.osc.gconf#app_group_add'
97	cri'http://coreapps.org/core.osc.gconf#joining_uri'
98	cri'http://coreapps.org/core.osc.gconf#app_groups'

99	cri'http://coreapps.org/ core.osc.gconf#group_policies'
100	cri'http://coreapps.org/core.osc.gconf#group_policies .key_update_check_interval'
101	cri'http://coreapps.org/core.osc.gconf#group_policies .exp_delta'
102	cri'http://coreapps.org/core.osc.gconf#as_uri'

Table 1: Shared Item Table for Compacting CoRAL Predicates.

A.2. Compacting Values of the rt= Target Attribute with Packed CBOR

The following shared item table is used for compacting values of the rt= target attribute, as per Section 2.2 of [I-D.ietf-cbor-packed].

Index	Item
415	cri'http://www.iana.org/assignments/linkformat/rt /core.osc.gconf'

Table 2: Shared Item Table for Compacting Values of the rt= Target Attribute.

Appendix B. Document Updates

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

B.1. Version -04 to -05

* Use "compacting" instead of "compressing" when referring to Packed CBOR.
* Updated references.
* Editorial fixes and improvements.

B.2. Version -03 to -04

* Updated references.
* Editorial improvements and fixes.

B.3. Version -02 to -03

* Uri-Path and Location-Path as text strings in examples.
* Updated references.
* Editorial fixes.

B.4. Version -01 to -02

* Avoid quotation marks for CBOR simple values.
* Fixed use of ’linkformat’ in the CURIE syntax.
* Fixed use of CURIEs that result in a URI with the fragment component.
* Renamed ’group_title’ as ’group_description’.
* Status/Configuration "properties" renamed as "parameters".
* POST (instead of PUT) for overwriting a group-configuration resource.
* Remove reference to the abandoned, custom format for error messages.
* Editorial improvements.

B.5. Version -00 to -01

* Updated reference and introductory text for the CBOR EDN application-extension identifier "cri".

B.6. Version -00

* CoRAL content taken out from draft-ietf-ace-oscore-gm-admin-08.

Acknowledgments

Most of the content in this document was originally specified in draft-ietf-ace-oscore-gm-admin, which is co-authored also by Peter van der Stok and Francesca Palombini, and where Klaus Hartke contributed in the initial definition of the resource model and interactions using CoRAL.

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

This work was supported by the Sweden's Innovation Agency VINNOVA within the EUREKA 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旦glund
RISE AB
Isafjordsgatan 22
SE-16440 Stockholm Kista
Sweden
Email: rikard.hoglund@ri.se