CoRE Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2020

M. Tiloca
RISE AB
C. Amsuess

P. van der Stok
Consultant

November 04, 2019

Discovery of OSCORE Groups with the CoRE Resource Directory
draft-tiloca-core-oscore-discovery-04

Abstract

Group communication over the Constrained Application Protocol (CoAP) can be secured by means of Group Object Security for Constrained RESTful Environments (Group OSCORE). At deployment time, devices may not know the exact OSCORE groups to join, the respective Group Manager, or other information required to perform the joining process. This document describes how a CoAP endpoint can use descriptions and links of resources registered at the CoRE Resource Directory to discover OSCORE groups and to acquire information for joining them through the respective Group Manager. A given OSCORE group may protect multiple application groups, which are separately announced in the Resource Directory as sets of endpoints sharing a pool of resources. This approach is consistent with, but not limited to, the joining of OSCORE groups based on the ACE framework for Authentication and Authorization in constrained environments.

Table of Contents

1. Introduction

A set of CoAP endpoints constitutes an application group by sharing a common pool of resources. The members of an application group may be members of a given security group, by sharing a common set of keying material to secure group communication.

The Constrained Application Protocol (CoAP) [RFC7252] supports group communication over IP multicast [RFC7390][I-D.dijk-core-groupcomm-bis] to improve efficiency and latency of communication and reduce bandwidth requirements. The document Object Security for Constrained RESTful Environments (OSCORE) [RFC8613] describes how to achieve end-to-end security for

CoAP messages through CBOR Object Signing and Encryption (COSE) [RFC8152].

In particular, [I-D.ietf-core-oscore-groupcomm] specifies how Group OSCORE protects CoAP messages in group communication contexts, so enabling OSCORE groups as security groups. Typically, one application group relies on exactly one OSCORE group, while a same OSCORE group may be used by multiple application groups at the same time.

A CoAP endpoint joins an OSCORE group via a Group Manager (GM), in order to get the necessary group keying material. As in [I-D.ietf-ace-key-groupcomm-oscore], the joining process can be based on the ACE framework for Authentication and Authorization in constrained environments [I-D.ietf-ace-oauth-authz], with the joining endpoint and the GM acting as ACE Client and Resource Server, respectively. That is, the joining endpoint accesses the group-membership resource associated with the OSCORE group to join and exported by the GM.

Typically, devices are equipped with a static X509 IDevID certificate installed at manufacturing time. This certificate is used at deployment time during an enrollment process that provides the device with an Operational Certificate, possibly updated during the device lifetime. In the presence of secure group communication for CoAP, such an Operational Certificate may be accompanied by information required to join OSCORE groups. This especially includes a reference to the group-membership resources to access at the respective GMs.

However, it is usually impossible to provide such precise information to freshly deployed devices as part of their (early) Operational Certificate. This can be due to a number of reasons: (1) the OSCORE group(s) to join and the responsible GM(s) are generally unknown at manufacturing time; (2) an OSCORE group of interest is created, or the responsible GM is deployed, only after the device is enrolled and fully operative in the network; and (3) information related to existing OSCORE groups or to their GMs has been changed. This requires a method for CoAP endpoints to dynamically discover OSCORE groups and their GM, and to retrieve relevant information about deployed groups.

To this end, CoAP endpoints can use descriptions and links of group-membership resources at GMs, in order to discover OSCORE groups and to retrieve the information required for joining them. With the discovery process of OSCORE groups expressed in terms of links to resources, the remaining problem is thus the discovery of those links. The CoRE Resource Directory (RD) [I-D.ietf-core-resource-directory] provides such discovery in an

efficient way, and it is expected to be used in many setups that would benefit of OSCORE group discovery.

This specification builds on this approach and describes how CoAP endpoints can use the RD to carry out the necessary link discovery steps, in order to discover OSCORE groups of interest and retrieve the information required to join them through their GM. In principle, the GM registers as an endpoint with the RD. The corresponding registration resource includes one link for each OSCORE group under that GM, specifying the path to the related group-membership resource to access for joining that group.

More information about the OSCORE group is stored in the target attributes of the respective link. This especially includes the identifiers of the application groups which use that OSCORE group. This enables a lookup of those application groups at the Resource Directory, where they are separately announced by a Commissioning Tool (see Appendix A of [I-D.ietf-core-resource-directory]).

When querying the RD for OSCORE groups, a CoAP endpoint can further benefit of the CoAP Observe Option [RFC7641]. This enables the reception of notifications about the creation of new OSCORE groups or the updates concerning existing groups. Thus, it facilitates the early deployment of CoAP endpoints, i.e. even before the GM is deployed and OSCORE groups are created.

The approach in this document is consistent with, but not limited to, the joining of OSCORE groups in [I-D.ietf-ace-key-groupcomm-oscore].

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.

This specification requires readers to be familiar with the terms and concepts discussed in [I-D.ietf-core-resource-directory] and [RFC6690]. Readers should also be familiar with the terms and concepts discussed in [RFC7252], [I-D.ietf-core-oscore-groupcomm] and [I-D.ietf-ace-key-groupcomm-oscore].

Terminology for constrained environments, such as "constrained device" and "constrained-node network", is defined in [RFC7228].

This document also refers to the following terminology.

- OSCORE group: a set of CoAP endpoints that share one OSCORE Common Security Context to protect group communication as described in [I-D.ietf-core-oscore-groupcomm]. Consequently, an OSCORE group acts as security group for all its members.

- Application group: a set of CoAP endpoints that share a set of common resources. Application groups are announced in the RD by a Commissioning Tool, according to the RD-Groups usage pattern (see Appendix A of [I-D.ietf-core-resource-directory]). An application group can be associated with a single OSCORE group, while multiple application groups can use the same OSCORE group. Application groups share resources by definition. Any two application groups associated to the same OSCORE group do not share any same resource.

2. Registration Resource for Group Managers

With reference to Figure 3 of [I-D.ietf-core-resource-directory], a Group Manager (GM) registers as an endpoint with the CoRE Resource Directory (RD). The registration includes the links to the group-membership resources located at the GM, and associated to the OSCORE groups administrated by that GM.

In particular, each link to a group-membership resource includes:

- "target": URI of the group-membership resource at the GM.

- target attributes, including:

  * Resource Type (rt) with the value "core.osc.mbr" defined in Section 8.1 of this specification.

  * The name of the OSCORE group, as defined in [I-D.ietf-ace-key-groupcomm-oscore].

  * One target attribute for each application group associated with the OSCORE group, specifying the name of that application group.

  * The algorithm used to countersign messages in the OSCORE group.

  * The elliptic curve (if applicable) for the algorithm used to countersign messages in the OSCORE group.

  * The key type of countersignature keys used to countersign messages in the OSCORE group.

  * The encoding of public keys used in the OSCORE group.

* The AEAD algorithm used in the OSCORE group.

* The HKDF algorithm used in the OSCORE group.

3. Registration of Group Manager Endpoints

During deployment, a GM finds the RD as described in Section 4 of [I-D.ietf-core-resource-directory]. Afterwards, the GM registers as an endpoint with the RD, as described in Section 5 of [I-D.ietf-core-resource-directory].

When doing so, the GM also registers all the group-membership resources it has at that point in time, i.e. one for each of its OSCORE groups.

For each registered group-membership resource, the GM includes the following parameters in the payload of the registration request.

- 'rt' = "core.osc.mbr" (see Section 8.1).

- 'sec-gp', specifying the name of the OSCORE group of interest. This parameter MUST specify a single value.

- 'app-gp', specifying the name(s) of the application group(s) associated to the OSCORE group of interest indicated by 'sec-gp'. This parameter MAY be included multiple times, and each occurrence MUST specify the name of one application group. A same application group MUST NOT be specified multiple times.

Also, for each registered group-membership resource, the GM may additionally include the following parameters in the payload of the registration request.

- 'cs_alg', specifying the algorithm used to countersign messages in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string, which is taken from the 'Value' column of the "COSE Algorithms" Registry defined in [RFC8152].

- 'cs_crv', specifying the elliptic curve (if applicable) for the algorithm used to countersign messages in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string, which is taken from the 'Value' column of the "COSE Elliptic Curve" Registry defined in [RFC8152].

- 'cs_kty', specifying the key type of countersignature keys used to countersign messages in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string,

which is taken from the 'Value' column of the "COSE Key Types" Registry defined in [RFC8152].

- 'cs_kenc', specifying the encoding of the public keys used in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string. This specification explicitly admits the signaling of COSE Keys [RFC8152] as encoding for public keys, which is indicated with "1", as taken from the 'Confirmation Key' column of the "CWT Confirmation Method" Registry defined in [I-D.ietf-ace-cwt-proof-of-possession]. Future specifications may define additional values for this parameter.

- 'alg', specifying the AEAD algorithm used in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string, which is taken from the 'Value' column of the "COSE Algorithms" Registry defined in [RFC8152].

- 'hkdf', specifying the HKDF algorithm used in the OSCORE group. If present, this parameter MUST specify a single value encoded as a text string, which is taken from the 'Value' column of the "COSE Algorithms" Registry defined in [RFC8152].

Values registered as a string that looks like an integer are not supported by this approach. Therefore, they MUST NOT be advertised through the corresponding parameters above.

A CoAP endpoint that queries the RD to discover OSCORE groups and their group-membership resource to access (see Section 5) would benefit from the information above as follows.

- The values of 'cs_alg', 'cs_crv', 'cs_kty' and 'cs_kenc' related to a group-membership resource provide an early knowledge of the format and encoding of public keys used in the OSCORE group. Thus, the CoAP endpoint does not need to ask the GM for this information as a preliminary step before the joining process, or to perform a trial-and-error exchange with the GM. Hence, the CoAP endpoint is able to provide the GM with its own public key in the correct expected format and encoding at the very first step of the joining process.

- The values of 'cs_alg', 'alg' and 'hkdf' related to a group-membership resource provide an early knowledge of the algorithms used in the OSCORE group. Thus, the CoAP endpoint is able to decide whether to actually proceed with the joining process, depending on its support for the indicated algorithms.

The GM SHOULD NOT use the Simple Registration approach described in Section 5.1 of [I-D.ietf-core-resource-directory].

The example below shows a GM with endpoint name "gm1" and address 2001:db8::ab that registers with the RD. The GM specifies the value of the 'sec-gp' parameter for accessing the OSCORE group with name "feedca570000" and used by the application group with name "group1" specified with the value of the 'app-gp' parameter. The countersignature algorithm used in the OSCORE group is EdDSA, with elliptic curve Ed25519 and keys of type OKP. Public keys used in the OSCORE group are encoded as COSE Keys [RFC8152].

Request: GM -> RD

```
Req: POST coap://rd.example.com/rd?ep=gm1
Content-Format: 40
Payload:
</group-oscore/feedca570000>;ct=41;rt="core.osc.mbr";
                              sec-gp="feedca570000";app-gp="group1";
                              cs_alg="-8";cs_crv="6";cs_kty="1";
                              cs_kenc="1"
```

Response: RD -> GM

```
Res: 2.01 Created
Location-Path: /rd/4521
```

4. Addition and Update of OSCORE Groups

The GM is responsible to refresh the registration of all its group-membership resources in the RD. This means that the GM has to update the registration within its lifetime as per Section 5.3.1 of [I-D.ietf-core-resource-directory], and has to change the content of the registration when a group-membership resource is added/removed or if its target attributes have to be changed, such as in the following cases.

- The GM creates a new OSCORE group and starts exporting the related group-membership resource.

- The GM dismisses an OSCORE group and stops exporting the related group-membership resource.

- Information related to an existing OSCORE group changes, e.g. the list of associated application groups.

To perform an update of its registrations, the GM can re-register with the RD and fully specify all links to its group-membership resources with their target attributes.

The example below shows how the GM from Section 3 re-registers with the RD. When doing so, it specifies:

- The same previous group-membership resource associated to the OSCORE group with name "feedca570000".
- An additional group-membership resource associated to the OSCORE group with name "ech0ech00000" and used by the application group "group2".
- A third group-membership resource associated with the OSCORE group with name "abcdef120000" and used by two application groups, namely "group3" and "group4".

Request: GM -> RD

```
Req: POST coap://rd.example.com/rd?ep=gm1
Content-Format: 40
Payload:
</group-oscore/feedca570000>;ct=41;rt="core.osc.mbr";
                             sec-gp="feedca570000";app-gp="group1";
                             cs_alg="-8";cs_crv="6";cs_kty="1";
                             cs_kenc="1",
</group-oscore/ech0ech00000>;ct=41;rt="core.osc.mbr";
                             sec-gp="ech0ech00000";app-gp="group2";
                             cs_alg="-8";cs_crv="6";cs_kty="1";
                             cs_kenc="1",
</group-oscore/abcdef120000>;ct=41;rt="core.osc.mbr";
                             sec-gp="abcdef120000";app-gp="group3";
                             app-gp="group4";cs_alg="-8";
                             cs_crv="6";cs_kty="1";cs_kenc="1"
```

Response: RD -> GM

```
Res: 2.04 Changed
Location-Path: /rd/4521
```

Alternatively, the GM can perform a PATCH/iPATCH [RFC8132] request to the RD, as per Section 5.3.3 of [I-D.ietf-core-resource-directory]. This requires new media-types to be defined in future standards, to apply a link-format document as a patch to an existing stored document.

5. Discovery of OSCORE Groups

A CoAP endpoint that wants to join an OSCORE group, hereafter called the joining node, might not have all the necessary information at

deployment time. Also, it might want to know about possible new OSCORE groups created afterwards by the respective Group Managers.

To this end, the joining node can perform a resource lookup at the RD as per Section 6.1 of [I-D.ietf-core-resource-directory], to retrieve the missing pieces of information needed to join the OSCORE group(s) of interest. The joining node can find the RD as described in Section 4 of [I-D.ietf-core-resource-directory].

The joining node uses the following parameter value for the lookup filtering.

- 'rt' = "core.osc.mbr" (see Section 8.1).

The joining node may additionally consider the following parameters for the lookup filtering, depending on the information it has already available.

- 'sec-gp', specifying the name of the OSCORE group of interest. This parameter MUST specify a single value.

- 'ep', specifying the registered endpoint of the GM.

- 'app-gp', specifying the name(s) of the application group(s) associated with the OSCORE group of interest. This parameter MAY be included multiple times, and each occurrence MUST specify the name of one application group. A same application group MUST NOT be specified multiple times.

Note that, with RD-based discovery, including the 'app-gp' parameter multiple times would result in finding only the group-membership resource that serves all the specified application groups, i.e. not any group-membership resource that serves either. Therefore, a joining node needs to perform N separate queries with different values for 'app-gp', in order to safely discover the (different) group-membership resource(s) serving the N application groups.

5.1. Discovery Example #1

Consistently with the examples in Section 3 and Section 4, the example below considers a joining node that wants to join the OSCORE group associated with the application group "group1", but that does not know the name of the OSCORE group, the responsible GM and the group-membership resource to access.

Request: Joining node -> RD

```
Req: GET coap://rd.example.com/rd-lookup/res
  ?rt=core.osc.mbr&app-gp=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/group-oscore/feedca570000>;rt="core.osc.mbr";
    sec-gp="feedca570000";app-gp="group1";
    cs_alg="-8";cs_crv="6";cs_kty="1";
    cs_kenc="1";anchor="coap://[2001:db8::ab]"
```

To retrieve the multicast IP address used in "group1", the joining node performs an endpoint lookup as shown below. The following assumes that the application group "group1" had been previously registered as per Appendix A of [I-D.ietf-core-resource-directory], with ff35:30:2001:db8::23 as associated multicast IP address.

```
Request: Joining node -> RD

Req: GET coap://rd.example.com/rd-lookup/ep
  ?et=core.rd-group&ep=group1

Response: RD -> Joining node

Res: 2.05 Content
Payload:
</rd/501>;ep="group1";et="core.rd-group";
          base="coap://[ff35:30:2001:db8::23]"
```

5.2. Discovery Example #2

Consistently with the examples in Section 3 and Section 4, the example below considers a joining node that wants to join the OSCORE group with name "feedca570000", but that does not know the responsible GM, the group-membership resource to access, and the associated application groups.

The example also shows how the joining node uses CoAP observation [RFC7641], in order to be notified of possible changes to the target attributes of the group-membership resource. This is also useful to handle the case where the OSCORE group of interest has not been created yet, so that the joining node can receive the requested information when it becomes available.

```
Request: Joining node -> RD
```

```
   Req: GET coap://rd.example.com/rd-lookup/res
     ?rt=core.osc.mbr&sec-gp=feedca570000
   Observe: 0

   Response: RD -> Joining node

   Res: 2.05 Content
   Observe: 24
   Payload:
   <coap://[2001:db8::ab]/group-oscore/feedca570000>;rt="core.osc.mbr";
       sec-gp="feedca570000";app-gp="group1";
       cs_alg="-8";cs_crv="6";cs_kty="1";
       cs_kenc="1";anchor="coap://[2001:db8::ab]"
```

Depending on the search criteria, the joining node performing the resource lookup can get large responses. This can happen, for instance, when the lookup request targets all the group-membership resources at a specified GM, or all the group-membership resources of all the registered GMs, as in the example below.

```
   Request: Joining node -> RD

   Req: GET coap://rd.example.com/rd-lookup/res?rt=core.osc.mbr

   Response: RD -> Joining node

   Res: 2.05 Content
   Payload:
   <coap://[2001:db8::ab]/group-oscore/feedca570000>;rt="core.osc.mbr";
       sec-gp="feedca570000";app-gp="group1";
       cs_alg="-8";cs_crv="6";cs_kty="1";
       cs_kenc="1";anchor="coap://[2001:db8::ab]",
   <coap://[2001:db8::ab]/group-oscore/ech0ech00000>;rt="core.osc.mbr";
       sec-gp="ech0ech00000";app-gp="group2";
       cs_alg="-8";cs_crv="6";cs_kty="1";
       cs_kenc="1";anchor="coap://[2001:db8::ab]",
   <coap://[2001:db8::ab]/group-oscore/abcdef120000>;rt="core.osc.mbr";
       sec-gp="abcdef120000";app-gp="group3";
       app-gp="group4";cs_alg="-8";cs_crv="6";
       cs_kty="1";cs_kenc="1";anchor="coap://[2001:db8::ab]"
```

Therefore, it is RECOMMENDED that a joining node which performs a resource lookup with the CoAP Observe option specifies the value of the parameter 'sec-gp' in its GET request sent to the RD.

6. Use Case Example With Full Discovery

In this section, the discovery of security groups is described to support the installation process of a lighting installation in an office building. The described process is a simplified version of one of many processes.

Assume the existence of four luminaires that are members of two application groups. In the first application group, the four luminaires receive presence messages and light intensity messages from sensors or their proxy. In the second application group, the four luminaires and several other pieces of equipment receive building state schedules.

Each of the two application groups is associated to a different security group and uses its own dedicated multicast IP address.

The Fairhair Alliance describes how a new device is accepted and commissioned in the network [Fairhair], by means of its certificate stored during the manufacturing process. When commissioning the new device in the installation network, the new device gets a new identity defined by a newly allocated certificate, following the BRSKI specification.

Section 7.3 of [I-D.ietf-core-resource-directory] describes how the Commissioning Tool (CT) assigns an endpoint name based on the CN field, (CN=ACME) and the serial number of the certificate (serial number = 123x, with 3 < x < 8). Corresponding ep-names ACME-1234, ACME-1235, ACME-1236 and ACME-1237 are also assumed.

It is common practice that locations in the building are specified according to a coordinate system. After the acceptance of the luminaires into the installation network, the coordinate of each device is communicated to the CT. This can be done manually or automatically.

The mapping between location and ep-name is calculated by the CT. For instance, on the basis of grouping criteria, the CT assigns: i) application group "grp_R2-4-015" to the four luminaires; and ii) application group "grp_schedule" to all schedule requiring devices. Also, the device with ep name ACME-123x has been assigned IP address: [2001:db8:4::x]. The RD is assigned IP address: [2001:db8:4:ff]. The used multicast addresses are: [ff05::5:1] and [ff05::5:2].

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***

The CT defines the application group "grp_R2-4-015", with resource /light and base address [ff05::5:1], as follows.

```
   Request: CT -> RD

   Req: POST coap://[2001:db8:4::ff]/rd
     ?ep=grp_R2-4-015&et=core.rd-group&base=coap://[ff05::5:1]
   Payload:
   </light>;rt="oic.d.light"

   Response: RD -> CT

   Res: 2.01 Created
   Location-Path: /rd/501
```

Also, the CT defines a second application group "grp_schedule", with resource /schedule and base address [ff05::5:2], as follows.

```
   Request: CT -> RD

   Req: POST coap://[2001:db8:4::ff]/rd
     ?ep=grp_schedule&et=core.rd-group&base=coap://[ff05::5:2]
   Payload:
   </schedule>;rt="oic.r.time.period"

   Response: RD -> CT

   Res: 2.01 Created
   Location-Path: /rd/502

   *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
```

Consecutively, the CT registers the four devices in the RD (IP address: 2001:db8:4::ff), with their endpoint names and application groups.

For the application group "grp_R2-4-015", four endpoints are specified as follows, with x = 4, 5, 6, 7.

```
   Request: CT -> RD

   Req: POST coap://[2001:db8:4::ff]/rd
     ?ep=ACME-123x&base=coap://[2001:db8:4::x]&app-gp=grp_R2-4-015
   Payload:
   </light>;rt="oic.d.light"

   Response: RD -> CT

   Res: 2.01 Created
   Location-Path: /rd/452x
```

For the application group "grp_schedule", four other endpoints are specified as follows, with x = 4, 5, 6, 7.

Request: CT -> RD

Req: POST coap://[2001:db8:4::ff]/rd
  ?ep=ACME-123x&base=coap://[2001:db8:4::x]&app-gp=grp_schedule
Payload:
</schedule>;rt="oic.r.time.period"

Response: RD -> CT

Res: 2.01 Created
Location-Path: /rd/456x

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***

Finally, the CT defines the corresponding security groups. In particular, assuming a Group Manager responsible for both security groups and with address [2001:db8::ab], the CT specifies:

Request: CT -> RD

```
Req: POST coap://[2001:db8:4::ff]/rd?ep=gm1&base=coap://[2001:db8::ab]
Payload:
</group-oscore/feedca570000>;ct=41;rt="core.osc.mbr";
                              sec-gp="feedca570000";app-gp="grp_R2-4-015",
</group-oscore/feedsc590000>;ct=41;rt="core.osc.mbr";
                              sec-gp="feedsc590000";app-gp="grp_schedule"
```

Response: RD -> CT

Res: 2.01 Created
Location-Path: /rd/4521

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***

The device with IP address [2001:db8:4::x] can consequently learn the groups to which it belongs. In particular, it first does an ep lookup to the RD to learn the application groups to which it belongs.

Request: Joining node -> RD

Req: GET coap://[2001:db8:4::ff]/rd-lookup/ep
  ?base=coap://[2001:db8:4::x]

Response: RD -> Joining node

```
   Res: 2.05 Content
   Payload:
   <rd/452x>;base=coap://[2001:db8:4::x]&ep=ACME-123x&\
             app-gp=grp_R2-4-015,
   <rd/456x>;base=coap://[2001:db8:4::x]&ep=ACME-123x&\
             app-gp=grp_schedule
```

To retrieve the multicast IP address used in "grp_R2-4-015", the device performs an endpoint lookup as shown below.

```
   Request: Joining node -> RD

   Req: GET coap://[2001:db8:4::ff]/rd-lookup/ep
     ?et=core.rd-group&ep=grp_R2-4-015

   Response: RD -> Joining node

   Res: 2.05 Content
   Payload:
   </rd/501>;ep="grp_R2-4-015";et="core.rd-group";
             base="coap://[ff05::5:1]"
```

Similarly, to retrieve the multicast IP address used in "grp_schedule", the device performs an endpoint lookup as shown below.

```
   Request: Joining node -> RD

   Req: GET coap://[2001:db8:4::ff]/rd-lookup/ep
     ?et=core.rd-group&ep=grp_schedule

   Response: RD -> Joining node

   Res: 2.05 Content
   Payload:
   </rd/502>;ep="grp_schedule";et="core.rd-group";
             base="coap://[ff05::5:2]"

   *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
```

Having learnt the application groups to which the device belongs, the device learns the security groups to which it belongs. In particular, it does the following for app-gp="grp_R2-4-015".

```
   Request: Joining node -> RD

   Req: GET coap://[2001:db8:4::ff]/rd-lookup/res
     ?rt=core.osc.mbr&app-gp=grp_R2-4-015
```

Response: RD -> Joining Node

```
Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/group-oscore/feedca570000>;
    rt="core.osc.mbr";sec-gp="feedca570000";
    app-gp="grp_R2-4-015";anchor="coap://[2001:db8::ab]"
```

Similarly, the device does the following for app-gp="grp_schedule".

```
Req: GET coap://[2001:db8:4::ff]/rd-lookup/res
  ?rt=core.osc.mbr&app-gp=grp_schedule
```

Response: RD -> Joining Node

```
Res: 2.05 Content
Payload:
<coap://[2001:db8::ab]/group-oscore/feedsc590000>;
    rt="core.osc.mbr";sec-gp="feedsc590000";
    app-gp="grp_schedule";anchor="coap://[2001:db8::ab]"
```

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***

After this last discovery step, the device can ask permission to join the security groups, and effectively join them through the Group Manager, e.g. according to [I-D.ietf-ace-key-groupcomm-oscore].

7. Security Considerations

The security considerations as described in Section 8 of [I-D.ietf-core-resource-directory] apply here as well.

8. IANA Considerations

This document has the following actions for IANA.

8.1. Resource Types

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

Value	Description	Reference
core.osc.mbr	Group-membership resource of an OSCORE Group Manager	[[this document]]

9. References

9.1. Normative References

[I-D.ietf-ace-cwt-proof-of-possession]
Jones, M., Seitz, L., Selander, G., Erdtman, S., and H. Tschofenig, "Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)", draft-ietf-ace-cwt-proof-of-possession-11 (work in progress), October 2019.

[I-D.ietf-ace-key-groupcomm-oscore]
Tiloca, M., Park, J., and F. Palombini, "Key Management for OSCORE Groups in ACE", draft-ietf-ace-key-groupcomm-oscore-03 (work in progress), November 2019.

[I-D.ietf-core-oscore-groupcomm]
Tiloca, M., Selander, G., Palombini, F., and J. Park, "Group OSCORE - Secure Group Communication for CoAP", draft-ietf-core-oscore-groupcomm-06 (work in progress), November 2019.

[I-D.ietf-core-resource-directory]
Shelby, Z., Koster, M., Bormann, C., Stok, P., and C. Amsuess, "CoRE Resource Directory", draft-ietf-core-resource-directory-23 (work in progress), July 2019.

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

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

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

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[Fairhair] FairHair Alliance, "Security Architecture for the Internet of Things (IoT) in Commercial Buildings", White Paper, ed. Piotr Polak , March 2018, <https://www.fairhair-alliance.org/data/downloadables/1/9/fairhair_security_wp_march-2018.pdf>.

[I-D.dijk-core-groupcomm-bis] Dijk, E., Wang, C., and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", draft-dijk-core-groupcomm-bis-01 (work in progress), July 2019.

[I-D.ietf-ace-oauth-authz] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", draft-ietf-ace-oauth-authz-25 (work in progress), October 2019.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7390] Rahman, A., Ed. and E. Dijk, Ed., "Group Communication for the Constrained Application Protocol (CoAP)", RFC 7390, DOI 10.17487/RFC7390, October 2014, <https://www.rfc-editor.org/info/rfc7390>.

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

[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/info/rfc8132>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

Acknowledgments

The authors sincerely thank Carsten Bormann, Klaus Hartke, Francesca Palombini, Dave Robin and Jim Schaad for their comments and feedback.

The work on this document has been partly supported by VINNOVA and the Celtic-Next project CRITISEC, and by the EIT-Digital High Impact Initiative ACTIVE.

Authors' Addresses

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

Email: marco.tiloca@ri.se

Christian Amsuess
Hollandstr. 12/4
Vienna 1020
Austria

Email: christian@amsuess.com

Peter van der Stok
Consultant

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