

CoRE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 12, 2019

M. Tiloca
RISE AB
C. Amsuess

P. van der Stok
Consultant
October 09, 2018

Discovery of OSCORE groups with the CoRE Resource Directory
draft-tiloca-core-oscore-discovery-00

Abstract

Group communication over the Constrained Application Protocol (CoAP) can be secured by means of Object Security for Constrained RESTful Environments (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 CoAP endpoints can use the CoRE Resource Directory to discover OSCORE groups and acquire information to join them through their respective Group Manager. This approach is consistent with, but not limited to, the joining of OSCORE groups based on the ACE framework for Authentication and Authorization.

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 April 12, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

| | | |
|----------------------|--|--------------------|
| 1. | Introduction | 2 |
| 1.1. | Terminology | 3 |
| 2. | Registration Resource for Group Managers | 4 |
| 3. | Registration of Group Manager Endpoints | 4 |
| 4. | Addition and Update of OSCORE Groups | 5 |
| 5. | Discovery of OSCORE Groups | 6 |
| 6. | Security Considerations | 8 |
| 7. | IANA Considerations | 8 |
| 7.1. | Resource Types | 8 |
| 8. | References | 8 |
| 8.1. | Normative References | 8 |
| 8.2. | Informative References | 9 |
| | Acknowledgments | 10 |
| | Authors' Addresses | 10 |

[1.](#) Introduction

The Constrained Application Protocol (CoAP) [[RFC7252](#)] supports group communication over IP multicast [[RFC7390](#)] to improve efficiency and latency of communication and reduce bandwidth requirements. The method Object Security for Constrained RESTful Environments (OSCORE) [[I-D.ietf-core-object-security](#)] enables end-to-end security of CoAP payload and options through CBOR Object Signing and Encryption (COSE) [[RFC8152](#)]. In addition, [[I-D.ietf-core-oscore-groupcomm](#)] specifies how OSCORE protects CoAP messages in group communication contexts.

A CoAP endpoint joins an OSCORE group by interacting with the responsible Group Manager (GM) to get the required keying material. As described in [[I-D.tiloca-ace-oscoap-joining](#)], 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 as ACE Client and ACE Resource Server, respectively. That is, the joining endpoint accesses the join resource associated to the OSCORE group of interest and exported by the GM.

Devices are typically equipped with a static Manufacturer Identity installed at manufacturing time. This identity is used at deployment time during an enrollment process which provides the device with an Operational Identity, possibly updated during the device lifetime. In the presence of secure group communication for CoAP, such an Operational Identity should also comprise information required for the device to join OSCORE groups. This especially includes a reference to the join resources to access at the respective GMs.

However, it can be infeasible or inconvenient to provide such precise information to freshly deployed devices as part of their (early) Operational Identity. This can be due to a number of reasons: the Manufacturer Identity has to be minimal and as small as possible in size; the OSCORE group(s) to join and the responsible GM(s) are unknown at manufacturing time; 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; information related to existing OSCORE groups or their GMs has been changed. This requires a method for CoAP endpoints to dynamically discover OSCORE groups and their GM, and to retrieve updated information about those groups.

This specification describes how CoAP endpoints use the CoRE Resource Directory (RD) [[I-D.ietf-core-resource-directory](#)] for discovering an OSCORE group and retrieving the information required to join that group through the responsible 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 join resource. More information about the OSCORE group is stored in the target attributes of the respective link.

When querying the RD for OSCORE groups, a CoAP endpoint can further benefit of observation [[RFC7641](#)]. This enables convenient notifications about the creation of new OSCORE groups or the updates of information concerning existing ones. As a consequence, it facilitates the early deployment of CoAP endpoints, i.e. even before the GM is deployed and the OSCORE groups of interest are created.

The approach described in this specification is consistent with, although not limited to, the joining of OSCORE groups described in [[I-D.tiloca-ace-oscoap-joining](#)].

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.tiloca-ace-oscoap-joining](#)].

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

This document refers also to the following terminology.

- o Zeroed-epoch Group ID: this refers to the Group ID of an OSCORE group as stored in the RD. The structure of such a stored Group ID is as per [Appendix C](#) of [[I-D.ietf-core-oscore-groupcomm](#)], with the "Group Epoch" immutable and set to zero.

2. Registration Resource for Group Managers

With reference to Figure 4 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 join resources at the GM, associated to the OSCORE groups under that GM.

In particular, each link to a join resource includes:

- o "target": URI of the join resource at the GM.
- o target attributes, including:
 - * Resource Type (rt) with the value "core.osc.j" defined in [Section 7.1](#) of this specification.
 - * The zeroed-epoch Group ID of the OSCORE group.
 - * One target attribute for each multicast IP address associated to the OSCORE group.

3. Registration of Group Manager Endpoints

Upon deployment, a GM finds the RD as described in Section 4 of [[I-D.ietf-core-resource-directory](#)]. After that, a GM registers as an endpoint with the RD, as described in Section 5.3 of [[I-D.ietf-core-resource-directory](#)]. When doing so, the GM MUST also register all the join resources it is exporting at that point in time, i.e. one for each of its OSCORE groups. The GM SHOULD NOT use the Simple Registration approach described in Section 5.3.1 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 link to one join resource for accessing the OSCORE group with zeroed-epoch Group ID "feedca570000" and one associated multicast IP address ff35:30:2001:db8::23.

Interaction: GM -> RD

```
Req: POST coap://rd.example.com/rd?ep=gm1
Content-Format: 40
Payload:
</join/feedca570000>;ct=41;rt="osc.j";
oscore-gid="feedca570000";oscore-group-ip="ff35:30:2001:db8::23"
```

Interaction: RD -> GM

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

4. Addition and Update of OSCORE Groups

The GM is responsible to keep its registration with the RD up to date with links to all its join resources. This means that the GM has to update the registration within its lifetime as per [Appendix A.1](#) of [\[I-D.ietf-core-resource-directory\]](#), and has to change the content of the registration when a join resource is added/removed or if its target attributes have to be changed, such as in the following cases.

- o The GM creates a new OSCORE group and starts exporting the related join resource.
- o The GM dismisses an OSCORE group and stops exporting the related join resource.
- o Information related to an existing OSCORE group changes, e.g. the list of associated multicast IP addresses.

In order to perform an update to the set of links in its registration, the GM can re-register with the RD and fully specify all links to its join resources and their target attributes in the payload of the POST request.

The example below shows the same GM from [Section 3](#) that re-registers with the RD, including the same join resource associated to the OSCORE group with zeroed-epoch Group ID "feedca570000", plus a second join resource associated to the OSCORE group with zeroed-epoch Group ID "ech0ech000000" and one multicast IP address ff35:30:2001:db8::45.

Interaction: GM -> RD

```
Req: POST coap://rd.example.com/rd?ep=gm1
Content-Format: 40
Payload:
</join/feedca570000>;ct=41;rt="osc.j";
oscore-gid="feedca570000";oscore-group-ip="ff35:30:2001:db8::23",
</join/ech0ech00000>;ct=41;rt="osc.j";
oscore-gid="ech0ech00000";oscore-group-ip="ff35:30:2001:db8::45"
```

Interaction: 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 [Appendix A.4](#) of [[I-D.ietf-core-resource-directory](#)]. This requires semantics to be defined in future standards, in order to apply a link-format document as a patch to a different one.

5. Discovery of OSCORE Groups

A CoAP endpoint that wants to join an OSCORE group 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 CoAP endpoint can perform a resource lookup at the RD as per Section 7.1 of [[I-D.ietf-core-resource-directory](#)], in order to retrieve the missing pieces of information needed to join the OSCORE group(s) of interest. The CoAP endpoint can find the RD as described in Section 4 of [[I-D.ietf-core-resource-directory](#)].

The lookup filtering MUST consider the following search criteria.

- o 'rt' = "osc.j" (see [Section 7.1](#)).

The lookup filtering MAY additionally consider the following search criteria, depending on the information already available to the CoAP endpoint.

- o 'oscore-gid', specifying the zeroed-epoch Group ID of the OSCORE group of interest.
- o 'ep', specifying the identifier of the GM as endpoint registered with the RD.

Consistently with the examples in [Section 3](#) and [Section 4](#), the example below shows a CoAP endpoint that wants to join the OSCORE group with zeroed-epoch Group ID "feedca570000", but that does not know the responsible GM and the join resource to access.

The example below also shows how the CoAP endpoint uses observation [[RFC7641](#)], in order to be notified of possible changes in the join resource's target attributes. This is also useful to handle the case where the OSCORE group of interest has not been created yet, so that the CoAP endpoint can receive the requested information when available at a later point in time.

Interaction: Joining node -> RD

```
Req: GET coap://rd.example.com/lookup/res?rt=osc.j&\
oscore-gid=feedca570000
Observe: 0
```

Interaction: RD -> Joining node

```
Res: 2.05 Content
Observe: 24
Payload:
<coap://[2001:db8::ab]/join/feedca570000>;rt="osc.j";
oscore-gid="feedca570000";oscore-group-ip="ff35:30:2001:db8::23";
anchor="coap://[2001:db8::ab]"
```

Depending on the used search criteria, the CoAP endpoint performing the resource lookup can get a response whose payload is quite large in size. This can happen, for instance, in case the lookup request targets all the join resources at a specified GM, or all the join resources of all the registered GMs, as in the example below.

Interaction: Joining node -> RD

```
Req: GET coap://rd.example.com/lookup/res?rt=osc.j
```

Interaction: RD -> Joining node

Res: 2.05 Content

Payload:

```
<coap://[2001:db8::ab]/join/feedca570000>;rt="osc.j";
oscore-gid="feedca570000";oscore-group-ip="ff35:30:2001:db8::23";
anchor="coap://[2001:db8::ab]",
<coap://[2001:db8::ab]/join/ech0ech000000>;rt="osc.j";
oscore-gid="ech0ech000000";oscore-group-ip="ff35:30:2001:db8::45";
anchor="coap://[2001:db8::ab]",
<coap://[2001:db8::cd]/join/abcdef120000>;rt="osc.j";
oscore-gid="abcdef120000";oscore-group-ip="ff35:30:2001:db8::67";
anchor="coap://[2001:db8::cd]"
```

Therefore, it is RECOMMENDED that a CoAP endpoint performing a resource lookup to discover OSCORE groups uses observation only when including the fine-grained search criterion 'oscore-gid' in its GET request sent to the RD.

6. Security Considerations

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

7. IANA Considerations

This document has the following actions for IANA.

7.1. 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.j | Join resource of an OSCORE Group Manager | [[this document]] |

8. References

8.1. Normative References

- [I-D.ietf-core-oscore-groupcomm]
Tiloca, M., Selander, G., Palombini, F., and J. Park,
"Secure group communication for CoAP", [draft-ietf-core-oscore-groupcomm-02](#) (work in progress), June 2018.
- [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-15](#) (work in progress), October 2018.
- [I-D.tiloca-ace-oscoap-joining]
Tiloca, M. and J. Park, "Joining OSCORE groups in ACE",
[draft-tiloca-ace-oscoap-joining-04](#) (work in progress),
June 2018.
- [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>>.
- [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>>.

8.2. Informative References

- [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-16](#)
(work in progress), October 2018.
- [I-D.ietf-core-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz,
"Object Security for Constrained RESTful Environments
(OSCORE)", [draft-ietf-core-object-security-15](#) (work in
progress), August 2018.

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

Acknowledgments

The work on this document has been partly supported 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