Discovery of OSCORE Groups with the CoRE Resource Directory

draft-tiloca-core-oscore-discovery-06

Marco Tiloca, RISE
Christian Amsüss
Peter van der Stok

IETF 108, CoRE WG, July 31st, 2020

Recap

- A newly deployed device:
  - May not know the OSCORE groups and their Group Manager (GM)
  - May have to wait GMs to be deployed or OSCORE groups to be created

- Use web links for discovery – typically through the Resource Directory (RD)
  - Discover an OSCORE group and retrieve information to join it
  - Practically, discover the links to join the OSCORE group at its GM
  - CoAP Observe supports early discovery and changes in group information

- Use resource lookup, to retrieve:
  - The name of the OSCORE group
  - A link to the resource at the GM for joining the group

Updates overview

- Addressed review of -05 from Jim – Thanks!
  - https://mailarchive.ietf.org/arch/msg/core/h62d2c2mYmG43ykz52KvbbEpgDc/
  - Some new open points (later slides)

- Revised terminology about groups
  - Now better aligned with *draft-ietf-core-groupcomm-bis*

- Clarified limitation of Link-Format as non typed
  - We can't signal an algorithm that has string value "-10" in the COSE registry
  - No such problem if we use CoRAL

Updates overview

- Fairhair/BACnet example
  - Removed the double registration
  - Removed registration of membership to application groups
    - Feature not defined in the RD document; we don't want to introduce it here
    - Common practice in some deployments; it can be in a separate document
  - Clarified that it's just an example, with no prescriptive intentions

- Added some text on one application group using many security groups
  - As of now, general reference to application policies
  - To be refined, based on the outcome of [1] related to *draft-ietf-core-groupcomm-bis*
  - Further discussion required: Which security groups must a participant join?

[1] https://mailarchive.ietf.org/arch/msg/core/4JtUVaB-XG_g0i_8v8CEMGyNdO8/

Updates overview

- Examples in CoRAL
  - Now moved to the document body
  - Next to the Link-Format examples
    - Registration
    - Update with re-registration
    - Lookup #1, Lookup #2

- New Appendix A
  - Full Fairhair/BACnet example in CoRAL

- This version -06 has now full support for both Link-Format and CoRAL RD

```
Request: Joining node -> RD

Req: GET coap://rd.example.com/rd-lookup/res
  ?rt=core.osc.mbr&sec-gp=feedca570000
Accept: TBD123456 (application/coral+cbor)
Observe: 0

Response: RD -> Joining node

Res: 2.05 Content
Observe: 24
Content-Format: TBD123456 (application/coral+cbor)

Payload:
#using <http://coreapps.org/core.oscore-discovery#>
#using reef = <http://coreapps.org/reef#>
#using iana = <http://www.iana.org/assignments/relation/>

#base <coap://[2001:db8::ab]/>
reef:rd-item </group-oscore/feedca570000> {
    reef:rt "core.osc.mbr"
    sec-gp "feedca570000"
    app-gp "group1"
    cs_alg -8
    cs_alg_crv 6
    cs_key_kty 1
    cs_key_crv 6
    cs_kenc 1
    iana:authorization-server <coap://as.example.com/token>
}
```

Open points

- When registering an OSCORE group to the RD
  - Possible to register related link to an Authorization Server (AS)
  - The AS is associated to the GM of the OSCORE group

```
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_alg_crv="6";
                              cs_key_kty="1";cs_key_crv=6";
                              cs_kenc="1",
<coap://as.example.com/token>;
      rel="authorization-server";
      anchor="coap://[2001:db8::ab]/group-oscore/feedca570000"

Response: RD -> GM

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

- Jim: not sure it should be the GM to register the “rel” link to the AS
- Who else can that be? It’s about accessing resources at the GM.
  - The GM also knows about that AS already when the group is created

Open points

- When registering an OSCORE group to the RD
  - The GM indicates the names of the application groups using the OSCORE group
  - Now we don't say how the GM knows the application groups

```
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_alg_crv="6";
                              cs_key_kty="1";cs_key_crv=6";
                              cs_kenc="1",
<coap://as.example.com/token>;
      rel="authorization-server";
      anchor="coap://[2001:db8::ab]/group-oscore/feedca570000"

Response: RD -> GM

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

- Suggestion from Jim in the "CoRAL and forms" discussion [2].
  - Related to the GM admin interface in *draft-tiloca-ace-oscore-gm-admin*
  - When creating the OSCORE group at the GM, indicate also the application groups

[2] https://mailarchive.ietf.org/arch/msg/core/BoYGYmEpJMUS8bk4PNHOEaFFcdU/

Open points

- We now use a resource type
  - rt = “core.osc.mbr”
  - Group-membership resource of an OSCORE Group Manager
- Should we have also an if= ?

```
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_alg_crv="6";
                              cs_key_kty="1";cs_key_crv=6";
                              cs_kenc="1",
<coap://as.example.com/token>;
      rel="authorization-server";
      anchor="coap://[2001:db8::ab]/group-oscore/feedca570000"

Response: RD -> GM

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

- Probably it does not matter that much, but …
- Compare *draft-ietf-ace-key-groupcomm*:
  - The group’s parent uses `if=ace.group`

Summary and next steps

- Addressed Jim’s review
- Revised CoRAL examples in the document body
- Next steps
  - Close open points from Jim’s review
  - Bridge with *ace-oscore-gm-admin* - The GM knows the names of application groups
- Need for reviews

Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-core-oscore-discovery

Backup

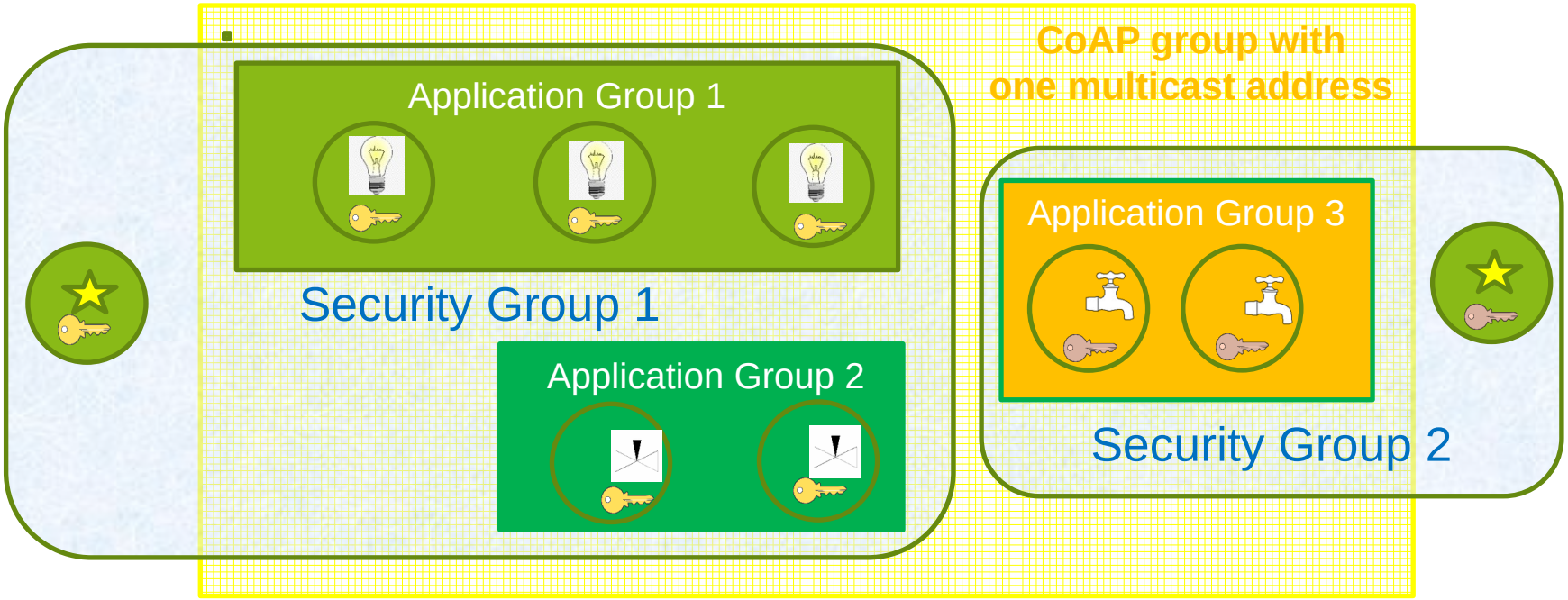
Application/CoAP/Security Groups

- Application group
  - Defined in {RD} and reused as is
  - Set of CoAP endpoints sharing a pool of resources
  - Registered and looked up just as per Appendix A of {RD}

- CoAP Group
  - Defined in *draft-ietf-core-groupcomm-bis*
  - Set of CoAP endpoints listening to the same IP multicast address
  - The IP multicast address is the ‘base’ address of the link to the application group

- (OSCORE) Security Group
  - Set of CoAP endpoints sharing a common security material (e.g. OSCORE Ctx)
  - A GM registers the group-membership resources for accessing its groups

Application vs. Security Groups



Client of application group

Different key sets

Resources for given function

Alg/key related parameters

- New optional parameters for a registered group-membership resource
  - (*)(**) *cs_alg* : countersignature algorithm, e.g. “EdDSA”
  - (*) *cs_alg_crv* : countersignature curve (if applicable), e.g. “Ed25519”
  - (*) *cs_key_kty* : countersignature key type, e.g. “OKP”
  - (*) *cs_key_crv* : countersignature curve (if applicable), e.g. “Ed25519”
  - (*) *cs_kenc* : encoding of public keys, e.g. “COSE_Key”
  - (**) *alg* : AEAD algorithm
  - (**) *hkdf* : HKDF algorithm

- Benefits for a joining node, when discovering the OSCORE group
  - (*) No need to ask the GM or to have a trial-and-error when joining the group
  - (**) Decide whether to join the group or not, based on supported the algorithms

Registration

- The GM registers itself with the RD
  - MUST include all its join resources, with their link attributes
  - New ‘rt’ value “core.osc.mbr”

```
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_alg_crv="6";
                             cs_key_kty="1";cs_key_crv=6";
                             cs_kenc="1",
<coap://as.example.com/token>;
      rel="authorization-server";
      anchor="coap://[2001:db8::ab]/group-oscore/feedca570000"

Response: RD -> GM

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

Discovery (1/2)

- The device performs a resource lookup at the RD
  - Known information: name of the Application Group, i.e. “group1”
  - Need to know: OSCORE Group Identifier; Join resource @ GM; Multicast IP address
  - ‘*app-gp*’ ✉ Name of the Application Group, acting as tie parameter in the RD

```
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_alg_crv="6";cs_key_kty="1";
    cs_key_crv=6";cs_kenc="1";anchor="coap://[2001:db8::ab]"
```

Discovery (2/2)

- The device performs an endpoint lookup at the RD
  - Still need to know the Multicast IP address
  - ‘ep’ // Name of the Application Group, value from ‘*app-gp*’
  - ‘base’ // Multicast IP address used in the Application Group

```
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]"
```