

**OCF “Fargo” – Update of aclist2 example in Security Considerations for Discovery –
Security WG CR 2752**

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HERewith INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2019 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

6.2 Security Considerations for Discovery

When defining discovery process, care must be taken that only a minimum set of Resources are exposed to the discovering entity without violating security of sensitive information or privacy requirements of the application at hand. This includes both data included in the Resources, as well as the corresponding metadata.

To achieve extensibility and scalability, this specification does not provide a mandate on discoverability of each individual Resource. Instead, the Server holding the Resource will rely on ACLs for each Resource to determine if the requester (the Client) is authorized to see/handle any of the Resources.

The `/oic/sec/acl2` Resource contains ACL entries governing access to the Server hosted Resources. (See 13.4)

Aside from the privacy and discoverability of Resources from ACL point of view, the discovery process itself needs to be secured. This specification sets the following requirements for the discovery process:

- 1) Providing integrity protection for discovered Resources.
- 2) Providing confidentiality protection for discovered Resources that are considered sensitive.

The discovery of Resources is done by doing a RETRIEVE operation (either unicast or multicast) on the known `/oic/res` Resource.

The discovery request is sent over a non-secure channel (multicast or unicast without DTLS), a Server cannot determine the identity of the requester. In such cases, a Server that wants to authenticate the Client before responding can list the secure discovery URI (e.g. `coaps://IP:PORT/oic/res`) in the unsecured `/oic/res` Resource response. This means the secure discovery URI is by default discoverable by any Client. The Client will then be required to send a separate unicast request using DTLS to the secure discovery URI.

For example, a Client with Device Id "d1" (UUID:"0685B960-736F-46F7-BEC0-9E6CBD61ADC1") makes a RETRIEVE request on the `/door` Resource hosted on a Server with Device Id "d3" where d3 has the ACL2s below:

```
{
  "aclist2": [
    {
      "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
      "resources": [{"href": "/door"}],
      "permission": 2, // RETRIEVE
      "aceid": 1
    },
    {
      "subject": {"authority": "owner", "role": "owner"}
      "resources": [{"href": "/door"}],
      "permission": 2, // RETRIEVE
      "aceid": 2
    },
    {
      "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
      "resources": [{"href": "/door/lock"}],
```

```
"permission": 4, // UPDATE
"aceid": 3
}
],
"rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
```

The ACL indicates that Client "d1" has RETRIEVE permissions on the Resource. Hence when device "d1" does a discovery on the "/door" Resource of the Server "d3", the response will include all the URIs in the "/door" Resource. Client "d2" without a Role ID "owner" will get an error response that includes no URI.

Discovery results delivered to d1 regarding d3's "/door" Resource from the secure Interface:

```
[
{
  "href": "/door",
  "rel": "self",
  "rt": ["oic.wk.col"],
  "if": ["oic.if.ll", "oic.if.b", "oic.if.baseline"],
  "eps":[
{"ep": "coaps://[2001:db8:a::b1d4]:5555"}
],
{
  "href": "/door/lock",
  "rt": ["oic.r.lock.status"],
  "if": ["oic.if.a", "oic.if.baseline"],
  "eps":[
{"ep": "coaps://[2001:db8:a::b1d4]:5555"}
]
}
]
```