OCF “Fargo” – Remove "rt" and "if" from ACE schema – Security WG CR 2955

Legal Disclaimer

START OF CHANGE

A.1 Access Control List-2

A.1.1 Introduction

This Resource specifies the local access control list.
When used without query parameters, all the ACE entries are returned.
When used with a query parameter, only the ACEs matching the specified parameter are returned.

A.1.2 Well-known URI

/oic/sec/acl2

A.1.3 Resource type

The Resource Type is defined as: "oic.r.acl2".

A.1.4 OpenAPI 2.0 definition

```
{
  "swagger": "2.0",
  "info": {
    "title": "Access Control List-2",
    "version": "20190111",
    "license": {
      "name": "OCF Data Model License",
      "url":
"https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4b
a/LICENSE.md",
      "x-copyright": "copyright 2016-2017, 2019 Open Connectivity Foundation, Inc. All rights
reserved."
    },
    "termsOfService": "https://openconnectivityfoundation.github.io/core/DISCLAIMER.md"
  },
  "schemes": ["http"],
  "consumes": ["application/json"],
  "produces": ["application/json"],
  "paths": {
    "/oic/sec/acl2" : {
      "get": {
        "description": "This Resource specifies the local access control list.\nWhen used
without query parameters, all the ACE entries are returned.\nWhen used with a query parameter,
only the ACEs matching the specified\nparameter are returned.\n",
        "parameters": [
          {"$ref": "#/parameters/interface"},
          {"$ref": "#/parameters/ace-filtered"}
        ],
        "responses": {
            "200": {
              "description" : "",
              "x-example":
                {
                  "rt" : ["oic.r.acl2"],
                  "aclist2": [
                    {
                      "aceid": 1,
                      "subject": {
                        "authority": "484b8a51-cb23-46c0-a5f1-b4aebef50ebe",
                        "role": "SOME_STRING"
                      },
                      "resources": [
                        {
                          "href": "/light"
                        },
```

```
                        {
                          "href": "/door"
                        }
                      ],
                      "permission": 24
                    },
                    {
                      "aceid": 2,
                      "subject": {
                        "uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
                      },
                      "resources": [
                        {
                          "href": "/light"
                        },
                        {
                          "href": "/door"
                        }
                      ],
                      "permission": 24
                      },
                      {
                        "aceid": 3,
                        "subject": {"conntype": "anon-clear"},
                        "resources": [
                          {
                            "href": "/light"
                          },
                          {
                            "href": "/door"
                          }
                        ],
                        "permission": 16,
                        "validity": [
                          {
                            "period":"20160101T180000Z/20170102T070000Z",
                            "recurrence": [ "DSTART:XXXXX",
"RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1" ]
                          },
                          {
                            "period":"20160101T180000Z/PT5H30M",
                            "recurrence":
[ "RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1" ]
                          }
                        ]
                      }
                  ],
                  "rowneruuid": "de305d54-75b4-431b-adb2-eb6b9e546014"
                },
              "schema": { "$ref": "#/definitions/Acl2" }
            },
            "400": {
              "description" : "The request is invalid."
            }
        }
      },
      "post": {
        "description": "Updates the ACL Resource with the provided ACEs.\n\nACEs provided in the
update with aceids not currently in the ACL\nResource are added.\n\nACEs provided in the update
with aceid(s) already in the ACL completely\nreplace the ACE(s) in the ACL Resource.\n\nACEs
provided in the update without aceid properties are added and\nassigned unique aceids in the ACL
Resource.\n",
        "parameters": [
          {"$ref": "#/parameters/interface"},
          {"$ref": "#/parameters/ace-filtered"},
          {
            "name": "body",
            "in": "body",
            "required": true,
            "schema": { "$ref": "#/definitions/Acl2-Update" },
```

```
            "x-example":
              {
                "aclist2": [
                  {
                    "aceid": 1,
                    "subject": {
                      "authority": "484b8a51-cb23-46c0-a5f1-b4aebef50ebe",
                      "role": "SOME_STRING"
                    },
                    "resources": [
                      {
                        "href": "/light"
                      },
                      {
                        "href": "/door"
                      }
                    ],
                    "permission": 24
                  },
                  {
                    "aceid": 3,
                    "subject": {
                      "uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
                    },
                    "resources": [
                      {
                        "href": "/light"
                      },
                      {
                        "href": "/door"
                      }
                    ],
                    "permission": 24
                  }
                ],
                "rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
              }
          }
        ],
        "responses": {
            "400": {
              "description" : "The request is invalid."
            },
            "201": {
              "description" : "The ACL entry is created."
            },
            "204": {
              "description" : "The ACL entry is updated."
            }
        }
      },
      "delete": {
        "description": "Deletes ACL entries.\nWhen DELETE is used without query parameters, all
the ACE entries are deleted.\nWhen DELETE is used with a query parameter, only the ACEs matching
the\nspecified parameter are deleted.\n",
        "parameters": [
          {"$ref": "#/parameters/interface"},
          {"$ref": "#/parameters/ace-filtered"}
        ],
        "responses": {
            "200": {
              "description" : "The matching ACEs or the entire ACL Resource has been
successfully deleted."
            },
            "400": {
              "description" : "The request is invalid."
            }
        }
      }
    }
```

```
  },
  "parameters": {
    "interface" : {
      "in" : "query",
      "name" : "if",
      "type" : "string",
      "enum" : ["oic.if.baseline"]
    },
    "ace-filtered" : {
      "in" : "query",
      "name" : "aceid",
      "required" : false,
      "type" : "integer",
      "description" : "Only applies to the ACE with the specified aceid.",
      "x-example" : 2112
    }
  },
  "definitions": {
    "Acl2" : {
      "properties": {
        "rowneruuid" : {
          "description": "The value identifies the unique Resource owner\nFormat pattern
according to IETF RFC 4122.",
          "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
9]{12}$",
          "type": "string"
        },
        "rt" : {
          "description": "Resource Type of the Resource.",
          "items": {
            "maxLength": 64,
            "type": "string",
            "enum": ["oic.r.acl2"]
          },
          "minItems": 1,
          "maxItems": 1,
          "readOnly": true,
          "type": "array"
        },
        "aclist2" : {
          "description": "Access Control Entries in the ACL Resource.",
          "items": {
            "properties": {
              "aceid": {
                "description": "An identifier for the ACE that is unique within the ACL. In
cases where it isn't supplied in an update, the Server will add the ACE and assign it a unique
value.",
                "minimum": 1,
                "type": "integer"
              },
              "permission": {
                "description": "Bitmask encoding of CRUDN permission\nThe encoded bitmask
indicating permissions.",
                "x-detail-desc": [
                  "0  - No permissions",
                  "1 - Create permission is granted",
                  "2 - Read, observe, discover permission is granted",
                  "4 - Write, update permission is granted",
                  "8 - Delete permission is granted",
                  "16 - Notify permission is granted"
                ],
                "maximum": 31,
                "minimum": 0,
                "type": "integer"
              },
              "resources": {
                "description": "References the application's Resources to which a security
policy applies.",
                "items": {
                  "description": "Each Resource must have at least one of these properties
```

```
set.",
                  "properties": {
                    "href": {
                      "description": "When present, the ACE only applies when the href
matches\nThis is the target URI, it can be specified as a Relative Reference or fully-qualified
URI.",
                      "format": "uri",
                      "maxLength": 256,
                      "type": "string"
                    },

                    "wc": {
                      "description": "A wildcard matching policy.",
                      "pattern": "^[-+*]$",
                      "type": "string"
                    }
                  },
                  "type": "object"
                },
                "type": "array"
              },
              "subject": {
                "anyOf": [
                  {
                    "description": "This is the Device identifier.",
                    "properties": {
                      "uuid": {
                        "description": "A UUID Device ID\nFormat pattern according to IETF RFC
4122.",
                        "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
9]{4}-[a-fA-F0-9]{12}$",
                        "type": "string"
                      }
                    },
                    "required": [
                      "uuid"
                    ],
                    "type": "object"
                  },
                  {
                    "description": "Security role specified as an <Authority> & <Rolename>. A
NULL <Authority> refers to the local entity or Device.",
                    "properties": {
                      "authority": {
                        "description": "The Authority component of the entity being identified.
A NULL <Authority> refers to the local entity or Device.",
                        "type": "string"
                      },
                      "role": {
                        "description": "The ID of the role being identified.",
                        "type": "string"
                      }
                    },
                    "required": [
                      "role"
                    ],
                    "type": "object"
                  },
                  {
                    "properties": {
                      "conntype": {
                        "description": "This property allows an ACE to be matched based on the
connection or message type.",
                        "x-detail-desc": [
                          "auth-crypt - ACE applies if the Client is authenticated and the data
channel or message is encrypted and integrity protected",
                          "anon-clear - ACE applies if the Client is not authenticated and the
data channel or message is not encrypted but may be integrity protected"
                        ],
                        "enum": [
```

```
                        "auth-crypt",
                        "anon-clear"
                      ],
                      "type": "string"
                    }
                  },
                  "required": [
                    "conntype"
                  ],
                  "type": "object"
                }
              ]
            },
            "validity": {
              "description": "validity is an array of time-pattern objects.",
              "items": {
                "description": "The time-pattern contains a period and recurrence expressed in
RFC5545 syntax.",
                "properties": {
                  "period": {
                    "description": "String represents a period using the RFC5545 Period.",
                    "type": "string"
                  },
                  "recurrence": {
                    "description": "String array represents a recurrence rule using the
RFC5545 Recurrence.",
                    "items": {
                      "type": "string"
                    },
                    "type": "array"
                  }
                },
                "required": [
                  "period"
                ],
                "type": "object"
              },
              "type": "array"
            }
          },
          "required": [
            "aceid",
            "resources",
            "permission",
            "subject"
          ],
          "type": "object"
        },
        "type": "array"
      },
      "n": {
        "$ref":
"https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
schema.json#/definitions/n"
      },
      "id": {
        "$ref":
"https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
schema.json#/definitions/id"
      },
      "if" : {
        "description": "The interface set supported by this Resource.",
        "items": {
          "enum": [
            "oic.if.baseline"
          ],
          "type": "string"
        },
        "minItems": 1,
        "maxItems": 1,
```

```
          "readOnly": true,
          "type": "array"
        }
      },
      "type" : "object",
      "required": ["aclist2", "rowneruuid"]
    },
    "Acl2-Update" : {
      "properties": {
        "rowneruuid" : {
           "description": "The value identifies the unique Resource owner\n Format pattern
according to IETF RFC 4122.",
           "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
9]{12}$",
           "type": "string"
        },
        "aclist2" : {
          "description": "Access Control Entries in the ACL Resource.",
          "items": {
            "properties": {
              "aceid": {
                "description": "An identifier for the ACE that is unique within the ACL. In
cases where it isn't supplied in an update, the Server will add the ACE and assign it a unique
value.",
                "minimum": 1,
                "type": "integer"
              },
              "permission": {
                "description": "Bitmask encoding of CRUDN permission\nThe encoded bitmask
indicating permissions.",
                "x-detail-desc": [
                  "0  - No permissions",
                  "1 - Create permission is granted",
                  "2 - Read, observe, discover permission is granted",
                  "4 - Write, update permission is granted",
                  "8 - Delete permission is granted",
                  "16 - Notify permission is granted"
                ],
                "maximum": 31,
                "minimum": 0,
                "type": "integer"
              },
              "resources": {
                "description": "References the application's Resources to which a security
policy applies.",
                "items": {
                  "description": "Each Resource must have at least one of these properties
set.",
                  "properties": {
                    "href": {
                      "description": "When present, the ACE only applies when the href
matches\nThis is the target URI, it can be specified as a Relative Reference or fully-qualified
URI.",
                      "format": "uri",
                      "maxLength": 256,
                      "type": "string"
                    },

                    "wc": {
                      "description": "A wildcard matching policy.",
                      "x-detail-desc": [
                        "+ - Matches all discoverable Resources",
                        "- - Matches all non-discoverable Resources",
                        "* - Matches all Resources"
                      ],
                      "enum": [
                        "+",
                        "-",
                        "*"
                      ],
```

```
                    "type": "string"
                  }
                },
                "type": "object"
              },
              "type": "array"
            },
            "subject": {
              "anyOf": [
                {
                  "description": "This is the Device identifier.",
                  "properties": {
                    "uuid": {
                      "description": "A UUID Device ID\n Format pattern according to IETF RFC
4122.",
                      "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
9]{4}-[a-fA-F0-9]{12}$",
                      "type": "string"
                    }
                  },
                  "required": [
                    "uuid"
                  ],
                  "type": "object"
                },
                {
                  "description": "Security role specified as an <Authority> & <Rolename>. A
NULL <Authority> refers to the local entity or Device.",
                  "properties": {
                    "authority": {
                      "description": "The Authority component of the entity being identified.
A NULL <Authority> refers to the local entity or Device.",
                      "type": "string"
                    },
                    "role": {
                      "description": "The ID of the role being identified.",
                      "type": "string"
                    }
                  },
                  "required": [
                    "role"
                  ],
                  "type": "object"
                },
                {
                  "properties": {
                    "conntype": {
                      "description": "This property allows an ACE to be matched based on the
connection or message type.",
                      "x-detail-desc": [
                        "auth-crypt - ACE applies if the Client is authenticated and the data
channel or message is encrypted and integrity protected",
                        "anon-clear - ACE applies if the Client is not authenticated and the
data channel or message is not encrypted but may be integrity protected"
                      ],
                      "enum": [
                        "auth-crypt",
                        "anon-clear"
                      ],
                      "type": "string"
                    }
                  },
                  "required": [
                    "conntype"
                  ],
                  "type": "object"
                }
              ]
            },
            "validity": {
```

```
                "description": "validity is an array of time-pattern objects.",
                "items": {
                  "description": "The time-pattern contains a period and recurrence expressed in
RFC5545 syntax.",
                  "properties": {
                    "period": {
                      "description": "String represents a period using the RFC5545 Period.",
                      "type": "string"
                    },
                    "recurrence": {
                      "description": "String array represents a recurrence rule using the
RFC5545 Recurrence.",
                      "items": {
                        "type": "string"
                      },
                      "type": "array"
                    }
                  },
                  "required": [
                    "period"
                  ],
                  "type": "object"
                },
                "type": "array"
              }
            },
            "required": [
              "resources",
              "permission",
              "subject"
            ],
            "type": "object"
          },
          "type": "array"
        }
      },
      "type" : "object"
    }
  }
}
```

A.1.5 Property definition

Table C.4 defines the Properties that are part of the "oic.r.acl2" Resource Type.

Table C.1 – The Property definitions of the Resource with type "rt" = "oic.r.acl2".

Property name	Value type	Mandatory	Access mode	Description
aclist2	array: see schema	No	Read Write	Access Control Entries in the ACL Resource.
rowneruuid	string	No	Read Write	The value identifies the unique Resource owner Format pattern according to IETF RFC 4122.
id	multiple types: see schema	No	Read Write	
n	multiple types: see schema	No	Read Write	
rt	array: see schema	No	Read Only	Resource Type of the Resource.

aclist2	array: see schema	Yes	Read Write	Access Control Entries in the ACL Resource.
rowneruuid	string	Yes	Read Write	The value identifies the unique Resource owner Format pattern according to IETF RFC 4122.
if	array: see schema	No	Read Only	The interface set supported by this Resource.

A.1.6 CRUDN behaviour

Table C.5 defines the CRUDN operations that are supported on the "oic.r.acl2" Resource Type.

Table C.2 – The CRUDN operations of the Resource with type "rt" = "oic.r.acl2".

Create	Read	Update	Delete	Notify
	get	post	delete	observe

END OF CHANGE