OCF 1.0 Security CR - CR34

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.

1 Overview

Section 12.2 includes the wording:

> 1975 A wild card resource identifier should be used to apply a blanket policy for a collection of
> 1976 resources. For example, /a/light/* matches all instances of the light resource.
> 1977 Evaluation of local ACL resources completes when all ACL resources have been queried and no
> 1978 entry can be found for the requested resource for the requestor – e.g. /oic/sec/acl /oic/sec/sacl
> 1979 and /oic/sec/amacl do not match the subject and the requested resource.

The wording does not describe expected use of wildcards in the context of the currently specified *oic-link* structure where parameters of OCF command line are broken out into 'href', 'if', 'rt' and other properties.

The possible use of optional properties for the purpose of controlling access is also not specified. This CR describes expected matching behaviours for optional properties contained in oic-link.

Efficient matching processing methods are not described in the specification. Although it is a non-goal for the specification to define implementation, this CR defines resource matching evaluation order such that if a first match is found, subsequent evaluation can be skipped without concern for undesired privilege escalations.

2 ACE2 Resource Matching

This applies to Section 12.2 and replaces lines 1975 and 1976.

The ACE2 resource matching algorithm uses an array of resource references to match resources to which the ACE2 access policy applies. Matching consists of comparing the values of the ACE2 "resources" property to the requested resource.

2.1 Host Reference Matching

When present in an ACE2 element, tThe Host Reference (href) property shall be used for resource matching.

- The href property shall be used to find an exact match of the resource.

2.2 Resource Type Matching

When present in an ACE2 element, The Resource Type (rt) property shall be used for resource matching.

- The rt property shall be used to find an exact match of the resource type.
- An array of strings is used to match resources that implement multiple esource types (e.g. collection resources).

2.3 Interface Matching

When present in the ACE2 element, the interface (if) property shall be used for resource matching.

- The ‘if’ property shall be used to find an exact match of the resource interface.
- An array of strings is used when the resource implements multiple interfaces.

2.4 Multiple Criteria Matching

If multiple matching criteria are supplied in the same ACE2 resources structure (e.g. ‘href’ and ‘rt’ and ‘if’) then a logical AND for the criteria shall be applied. For example, if both ‘href’=”/a/light and ‘if’=”oic.if.s” are given, then a match exists only when both the ‘href’ and the ‘if’ criterion are true for the candidate resources.

If multiple ACE2 “resources” entries exist, then a logical OR is applied for each resource element in the array. For example, if a first element of the resources array contains ‘href’=”/a/light” and the second element of the resources array contains ‘if’=”oic.if.s”, then resources that match both the ‘href’ criteria and the ‘if’ criteria are included in the set of matched resources.

2.5 Wildcard Matching

A wildcard expression may be used to match all resources using a property contained in a the oic.sec.ace2.resource-ref structure The following matching strings are defined:

String	Description
“+”	Shall match all discoverable resources.
“-”	Shall match all non-discoverable resources.
“*”	Shall match all resources.

3 Order of Evaluation

This applies to Section 12.2.

The OCF Server shall apply an ACE2 matching algorithm that matches in the following sequence:

1. If the /oic/sec/sacl resource exists and if the signature verification is successful, these ACE2 entries contribute to the set of local ACE2 entries in step 3. The OCF Server shall verify the signature, at least once, following update of the /oic/sec/sacl resource.
2. The local /oic/r/acl2 resource contributes its ACE2 entries for matching.
3. Access shall be granted when all these criteria are met:
    a. The requestor is matched by the ACE2 “subject” property.
    b. The requested Resource is matched by the ACE2 “resources” property and the requested Resource shall exist on the local Server.

c. The “period” property constraint shall be satisfied.

d. The “permission: property constraint shall be applied.

Note: If multiple ACE2 entries match the Resource request, the union of permissions, for all matching ACEs, defines the *effective* permission granted. E.g. If Perm1=CR---; Perm2=--UDN; Then UNION(Perm1, Perm2)=CRUDN.

The Server shall enforce access based on the effective permissions granted.

Example JSON for Resource matching

```
{
  [
//Matches Resources named “/x/door1” or “/x/door2”
     {
         "href":"/x/door1"
    },
     {
         "href":"/x/door2"
    },
//Matches Resources with Resource Type “oic.sec.crl” and
“oic.sec.cred”
     {
         "rt":[" oic.sec.crl ", “oic.sec.cred "]
    },
// Matches Resources that implement both “oic.if.baseline” and
“oic.if.rw” Interfaces.

        “if”:[“oic.if.baseline”, “oic.if.rw”]
    },
//Matches Resources named “/x/light1” or “/x/light2” and have
Resource Types “x.light.led”, “x.light.flourescent” and
“x.light.color”.
     {
       "href":"/x/light1",
        “rt”:[“x.light.led”,“x.light.flourescent”,
“x.light.color”]
    },
     {
        "href":"/x/light2",
        “rt”:[“x.light.led”,“x.light.flourescent”,
“x.light.color”]
    },
//Matches all Resources.
    {
         “wc”:“*”
```

```
      }
   ]
}
```

13.5 ACL Resources(/oic/sec/acl)

13.5.2 ACL Resource

The **oic.sec.ace2** structure is defined as follows:

Property Name	Value Type	Mandatory	Description
subject	oic.sec.roletype, oic.sec.didtype, "*"	Yes	The OCF Client is the subject of the ACE when the roles, device identity, "*" (for any authenticated or unauthenticated), in the ACE matches.
resources	array of oic.sec.ace2.resource-ref	Yes	The application's Resources to which a security policy applies
permission	oic.sec.crudntype.bitmask	Yes	Bitmask encoding of CRUDN permission
validity	array of oic.sec.time-pattern	No	An array of a tuple of period and recurrence. Each item in this array contains a string representing a period using the RFC5545 Period, and a string array representing a recurrence rule using the RFC5545 Recurrence.

Table 32 – oic.sec.ace2 data type definition.

Property Name	Value Type	Mandatory	Description
href	uri	No	A URI referring to a resource to which the containing ACE applies
rt	array of strings	No	The resource types to which the containing ACE applies
if	array of strings	No	The interfaces to which the containing ACE applies
wc	string	No	A wildcard matching policy where: "+" – Matches all discoverable resources "-" – Matches all non-discoverable resources "*" – Matches all resources

Table 33 - oic.sec.ace2.resource-ref data type definition.

At least one of the properties in oic.sec.ace2.resource-ref shall be supplied.