OCF 1.0 Security CR - CR48

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 BNF Definition

Note: This applies to Section 13.5.1

Current definition:

13.5.1 OIC Access Control List (ACL) BNF defines ACL structures.

ACL structure in Backus-Naur Form (BNF) notation:

<ACL>	<ACE>,{<ACE>};
<ACE>	<SBACE> | <RBACE>;
<SBACE>	<SubjectId>, <ResourceRef>, <Operation>, [<Validity>,{<Validity>}];
<RBACE>	<RoleId>,<ResourceRef>,<Operation>,[<Validity>,{<Validity>}];
<RoleId>	[<Authority>], '/', [<RoleName>];
<RoleName>	[URI]
<Authority>	[UUID]
<ResourceRef>	[<SSID>] | [<DeviceID>], '/', [<ResourceName>,'/',<Number>]
<ResourceName>	<URI_String>
<SubjectId>	<DeviceID>, <GroupId>;
<SSID>	<UInt16>

Figure 26 – BNF Definition of OIC ACL

Proposed definition:

<ACL>	<ACE> {<ACE>}
<ACE>	<SubjectId> <ResourceRef> <Permission> {<Validity>}
<SubjectId>	<DeviceId> | <Wildcard> | <RoleId>
<DeviceId>	<UUID>
<RoleId>	[<Authority>] <RoleName> {<RoleName>}
<RoleName>	<URI>
<Authority>	<UUID>
<ResourceRef>	' (' <OIC_LINK> {',' {OIC_LINK>} ')'
<Permission>	('C' | '-') ('R' | '-') ('U' | '-') ('D' | '-') ('N' | '-')
<Validity>	<Period> {<Recurrence>}
<Wildcard>	'*'
<URI>	RFC3986 //Core spec defined
<UUID>	RFC4122 //Core spec defined
<Period>	RFC5545 Period
<Recurrence>	RFC5545 Recurrence
<OIC_LINK>	Core spec defined in JSON Schema

Figure 26 – BNF Definition of OCF ACL

The <DeviceId> token means the requestor must possess a credential that uses <UUID> as its identity in order to match the requestor to the <ACE> policy.

The <RoleID> token means the requestor must possess a role credential with <URI> as its role in order to match the requestor to the <ACE> policy.

The <Wildcard> token "*" means any requestor is matched to the <ACE> policy, with or without authentication.

When a <SubjectId> is matched to an <ACE> policy the <ResourceRef> is used to match the <ACE> policy to resources.

The <OIC_LINK> token contains values used to query existence of hosted resources.

The <Permission> token specifies the privileges granted by the <ACE> policy given the <SubjectId> and <ResourceRef> matching does not produce the empty set match.

Permissions are defined in terms of CREATE (‘C’), READ (‘R’), UPDATE (‘U’), DELETE (‘D’), NOTIFY (‘N’) and NIL (‘-‘). NIL is substituted for a permissions character that signifies the respective permission is not granted.

The empty set match result defaults to a condition where no access rights are granted.

If the <Validity> token exists, the <Permission> granted is constrained to the time <Period>. <Validity> may further be segmented into a <Recurrence> pattern where access may alternatively be granted and rescinded according to the pattern.

Note: BNF descriptions are informative content.

2 ACL Resource

Note: This applies to Section 13.5.2.

Table 29 currently is defined as follows:

Fixed URI	Resource Type Title	Resource Type ID (“rt” value)	Interfaces	Description	Related Functional Interaction
/oic/sec/acl	ACL	urn:oic.r.acl	baseline	Resource for managing access	Security

Table 27 – Definition of the oic.r.acl Resource

Property Title	Property Name	Value Type	Value Rule	Unit	Access Mode	Mandatory	Description
ACE List	aclist	oic.sec.ace	-	-	RW	Yes	Access Control Entries in the ACL resource. This property contains “aces”, an array of oic.sec.ace1 resources and “aces2”, an array of oic.sec.ace2 resources
Resource Owner ID	rowneruuid	String	uuid	-	RW	Yes	A uuid that identifies the device that is the owner of this resource. The owning device has implicit RW access to the resource, regardless of ACL configuration.
Resource Owner	rowner	oic.sec.svctype , oic.sec.didtype	-, -	-	RW	No	This resource’s owner. Represented either as a service resource or in the form of a device id The owning device has implicit RW access to the resource, regardless of ACL configuration.

Table 28 – Properties of the oic.r.acl Resource

Property Title	Property Name	Value Type	Value Rule	Unit	Access Mode	Mandatory	Description
Resources	resources	oic.oic-link	array	-	RW	Yes	The application's resources to which a security policy applies
Permission	permission	oic.sec.crudntype	bitmask	-	RW	Yes	Bitmask encoding of CRUDN permission
Validity	validity	oic.sec.ace/definitions/time-interval	array	-	RW	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.
For ACEs in an "aces" list							
Subject ID	subjectuuid	String	uuid, "*"	-	RW	Yes	A uuid that identifies the device to which this ACE applies to or "*" for anonymous access.
For ACEs in an "aces2" list							
Subject	subject	oic.sec.roletype, oic.sec.didtype	- , -	-	RW	Yes	The subject to whom this ace applies, either a deviceId or a role.

Table 29 – Properties of the oic.sec.ace Property

Note: The table 29 is updated to deprecate the use of 'Subject' and more clearly specify the use of deviceIDs, roleIDs and wildcard for anonymous matching are mandatory to implement.

CR48 Changes

13.5.2 ACL Resource

There are two types of ACLs, 'acl' is a list of type 'ace' and 'acl2' is a list of type 'ace2'. The 'acl' type exists for backwards compatibility and should not be used on devices that support 'acl2'. The difference between 'ace' and 'ace2' is how the subject is encoded. In 'ace' it is a UUID or "*", which matches any requestor, with or without authentication. In 'ace2' the subject is a UUID, a role, or "*".

Definition of "oic.sec.subject" {

"oneof": [

"property": "oic.sec.roletype",

"property": "oic.sec.didtype",

"string": "*"

]

}

When the ACE subject is specified as a device, the OCF Server must verify the authenticated OCF client possesses a valid credential naming the device. When the ACE subject is specified as a role, the server must verify the authenticated OCF client possesses a valid credential granting the role.

When the ACE subject is specified as the wildcard string “*” any requestor is matched. The OCF server may authenticate the OCF client, but is not required to.

Property Title	Property Name	Value Type	Value Rule	Unit	Access Mode	Mandatory	Description
ACE List	aclist	oic.sec.ace	-	-	RW	Yes	Access Control Entries in the ACL resource that supports subjects defined as UUID.
~~Resource Owner ID~~	~~rowneruuid~~	~~String~~	~~uuid~~	~~-~~	~~RW~~	~~Yes~~	~~A uuid that identifies the device that is the owner of this resource.~~ ~~The owning device has implicit RW access to the resource, regardless of ACL configuration.~~
Note: ‘rowner’ property removed.							
rowneruuid	uuid	Yes					The resource owner property (rowneruuid) is used by the Server to reference a service provider trusted by the OCF Server. OCF Server shall verify the service provider is authorized to perform the requested action.
			RESET	R			OCF Server shall set property to NULL
			RFOTM	RW			The OBT (established by successful owner transfer method) should configure the resource owner after the secure session has been established.
			RFPRO	R			n/a
			RFNOP	R			n/a
			SRESET	RW			The device owner (/doxm.devowneruuid) may update the resource owner property (rowneruuid) after a mutually authenticated secure session is established. If the device owner does not refer to a valid service provider the OCF Server shall transition to RESET device state.

Table 28 – Properties of the oic.r.acl Resource

Property Title	Property Name	Value Type	Value Rule	Unit	Access Mode	Mandatory	Description
Resources	resources	array of oic.oic-link	array	-	RW	Yes	The application's resources to which a security policy applies
Permission	permission	oic.sec.crudntypе.bitmask	bitmask	-	RW	Yes	Bitmask encoding of CRUDN permission
Validity	validity	array of oic.sec.time-pattern	array	-	RW	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.
Subject ID	subjectuuid	String	uuid, "*"	-	RW	Yes	A uuid that identifies the device to which this ACE applies to or "*" for anonymous access.
Note: 'subject' property removed.							

Table 29 – Properties of the oic.sec.ace structure.

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	Interfaces	Description	Related Functional Interaction
/oic/sec/acl2	ACL2	oic.r.acl2	baseline	Resource for managing access	Security

Table 30 – Definition of the oic.r.acl2 Resource

Property Name	Value Type	Mandatory	Device State	Access Mode	Description
aces	array of oic.sec.ace2	Yes			The aces property is an array of ACE records of type "oic.sec.ace2". The Server uses this list to apply access control to its local resources.
			RESET	R	Server shall set to manufacturer defaults.
			RFOTM	RW	The OBT shall configure select oic.sec.ace2 entries after a secure session is established.
			RFPRO	RW	The AMS (referenced via rowneruuid property) shall update the oic.sec.ace2 entries after mutually authenticated secure session is established. Access to vertical resources is prohibited.
			RFNOP	R	Access to vertical resources is permitted after a matching ACE is found.

			SRESET	RW	The OBT (referenced via devowneruuid property) should evaluate the integrity of and may update oic.sec.ace2 entries when a secure session is established and the Server and OBT are authenticated.
rowneruuid	uuid	Yes	Same as rowneruuid in oic.sec.acl		

Table 31 – Properties of the oic.r.acl2 Resource

2.1 Definition of oic.sec.ace2 Structure

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.oic-link	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.