OCF “Essen” – Ensuring proper and consistent usage of Resource and Resource Type– Security WG CR 2876

Legal Disclaimer

Rationale

This CR proposes a consistent usage of Resource and Resource Type ID throughout the OCF Security Specification. In OCF Core Specification, both terms are defined as follows.

OCF 2.0.1 Core Specification
3.1.26 **Resource** represents an entity modelled and exposed by the Framework (3.1.14) **3.1.30** **Resource Type** a uniquely named definition of a class of Properties (3.1.29) and the interactions that are supported by that class Note 1 to entry: Each Resource (3.1.21) has a Property (3.1.29) "rt" whose value is the unique name of the Resource Type (3.1.30). **7.4.3 Resource Type definition** – *Resource Type ID* – the value of "rt" Property which identifies the Resource Type, (e.g., "oic.wk.p").

Technically speaking, a Resource Type (“rt”) is a Common Property of a Resource. Since a Resource could be defined by more than one Resource Type, Resource Type Property can be used to declare more than one Resource type.

In the latest OCF Security Specification, we noticed that the terms Resource and Resource Type ID are sometimes not correctly used. Such misusage confuses readers. For example,

OCF 2.0.2 Security Specification
5.1 Preamble 2) The Devices (e.g. Server and Client) exchange messages either with or without a mutually-authenticated secure channel between the two Devices. a) The "oic.sec.cred" Resource on each Devices holds the credentials used for mutual authentication and (when applicable) certificate validation.

"oic.sec.cred" should have been “/oic/sec/cred”

*** Paste the Change Request content here ***

1 Scope

2 Normative References

3 Terms, definitions, and abbreviated terms

4 Document Conventions and Organization

5 Security Overview

5.1 Preamble

The security theory of operation is depicted in Figure 2 and described in the following steps.

1) The Client establishes a network connection to the Server (Device holding the Resources). The connectivity abstraction layer ensures the Devices are able to connect despite differences in connectivity options.
2) The Devices (e.g. Server and Client) exchange messages either with or without a mutually-authenticated secure channel between the two Devices.
   a) The "/oic/sec/cred" Resource on each Devices holds the credentials used for mutual authentication and (when applicable) certificate validation.
   b) Messages received over a secured channel are associated with a "deviceUUID". In the case of a certificate credential, the "deviceUUID" is in the certificate received from the other Device. In the case of a symmetric key credential, the "deviceUUID" is configured with the credential in the "/oic/sec/cred" Resource.
   c) The Server can associate the Client with any number of roleid. In the case of mutual authentication using a certificate, the roleid (if any) are provided in role certificates; these are configured by the Client to the Server. In the case of a symmetric key, the allowed roleid (if any) are configured with the credential in the "/oic/sec/cred" Resource.
   d) Requests received by a Server over an unsecured channel are treated as anonymous and not associated with any deviceUUID or roleid.

Figure 3 depicts OCF Security Enforcement Points.

A Device is authorized to communicate with an OCF Cloud if a trusted Mediator has provisioned the Device.

– Device and Mediator connect over DTLS using "/oic/sec/cred" Resource
– Device is provisioned by Mediator with following information:
  – the URI of OCF Cloud
  – Token that can be validated by the OCF Cloud
  – UUID of the OCF Cloud

6 Security for the Discovery Process

7 Security Provisioning

Table 1 – Mapping of Properties of the "/oic/sec/account" and "oic.r.coapcloudconf" Resources

Resource	oic.r.coapcloudconf	/oic/sec/account	Description
Authorization Provider Name	apn	authprovider	The Authorization Provider through which Access Token was obtained.
OCF Cloud URL	cis	-	This is the URL connection is established between Device and OCF Cloud.
Access Token	at	accesstoken	The unique token valid only for the Device.
OCF Cloud UUID	sid	-	This is the identity of the OCF Cloud that the Device is configured to use.

8 Device Onboarding State Definitions

9 Security Credential Management

10 Device Authentication

11 Access Control

12 Security Resources

12.1 Security Resources General

OCF Security Resources are shown in Figure 34.

"/oic/sec/cred" Resource and Properties are shown in Figure 35.

"/oic/sec/acl2" Resource and Properties are shown in Figure 36.

"/oic/sec/amacl" Resource and Properties are shown in Figure 37.

"/oic/sec/sacl" Resource and Properties are shown in Figure 38.

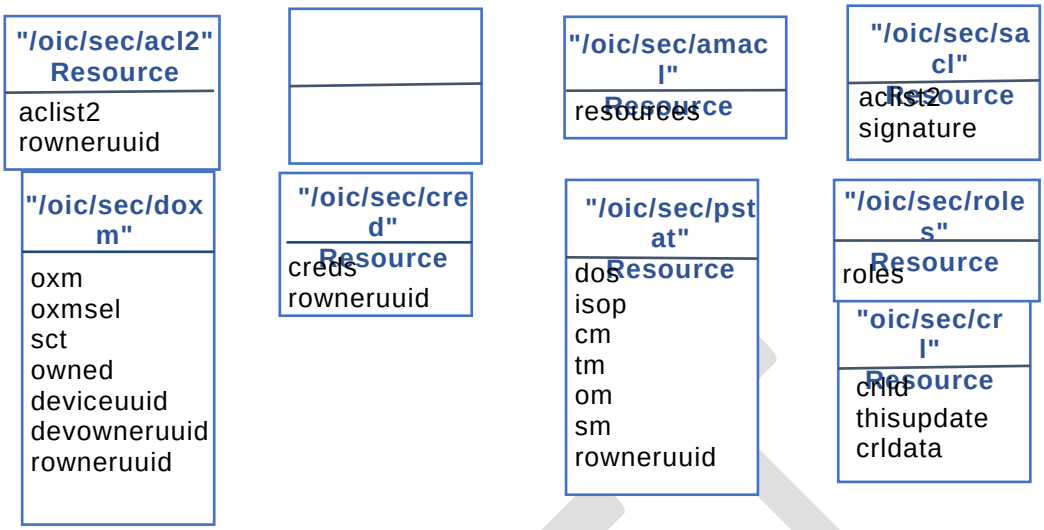

Figure 1 – OCF Security Resources

12.2 Device Owner Transfer Resource

12.2.1 Device Owner Transfer Resource General

Table 26 defines the Properties of the "/oic/sec/didtype".

Table 2 – Properties of the "oic.sec.didtype" Property

Property Title	Property Name	Value Type	Value Rule	Mandatory	Device State	Access Mode	Description
Device ID	uuid	String	uuid	Yes	RW	-	A uuid value

12.2.2 Persistent and Semi-Persistent Device Identifiers

The Device vendor determines whether a device identifier can be set by a configuration tool or whether it is immutable. If it is an immutable value this document refers to it as a persistent device identifier. Otherwise, it is referred to as a semi-persistent device identifier. There are four device identifiers that could be considered persistent or semi-persistent:

1) "deviceuuid" Property of "/oic/sec/doxm" Resource
2) "di" Property of "/oic/d" Resource
3) "piid" Property of "/oic/d" Resource
4) "pi" Property of "/oic/p" Resource

12.2.3 Onboarding Considerations for Device Identifier

12.2.4 OCF defined OTMs

12.3 Credential Resource

12.3.1 Credential Resource General

The "/oic/sec/cred" Resource maintains credentials used to authenticate the Server to Clients and support services as well as credentials used to verify Clients and support services.

Multiple credential types are anticipated by the OCF framework, including pair-wise pre-shared keys, asymmetric keys, certificates and others. The credential Resource uses a Subject UUID to distinguish the Clients and support services it recognizes by verifying an authentication challenge.

In order to provide an interface which allows management of the "creds" Array Property, the RETRIEVE, UPDATE and DELETE operations on the "/oic/sec/cred" Resource shall behave as follows:

1) A RETRIEVE shall return the full Resource representation, except that any write-only Properties shall be omitted (e.g. private key data).
2) An UPDATE shall replace or add to the Properties included in the representation sent with the UPDATE request, as follows:
   a) If an UPDATE representation includes the "creds" array Property, then:
      i) Supplied creds with a "credid" that matches an existing "credid" shall replace completely the corresponding cred in the existing "creds" array.
      ii) Supplied creds without a "credid" shall be appended to the existing "creds" array, and a unique (to the cred Resource) "credid" shall be created and assigned to the new cred by the Server. The "credid" of a deleted cred should not be reused, to improve the determinism of the interface and reduce opportunity for race conditions.
      iii) Supplied creds with a "credid" that does not match an existing "credid" shall be appended to the existing "creds" array, using the supplied "credid".
      iv) The rows in Table 29 corresponding to the "creds" array Property dictate the Device States in which an UPDATE of the "creds" array Property is always rejected. If OCF Device is in a Device State where the Access Mode in this row contains "R", then the OCF Device shall reject all UPDATEs of the "creds" array Property.
3) A DELETE without query parameters shall remove the entire "creds" array, but shall not remove the "/oic/sec/cred" Resource.
4) A DELETE with one or more "credid" query parameters shall remove the cred(s) with the corresponding credid(s) from the "creds" array.
5) The rows in Table 29 corresponding to the "creds" array Property dictate the Device States in which a DELETE is always rejected. If OCF Device is in a Device State where the Access Mode in this row contains "R", then the OCF Device shall reject all DELETEs.

NOTE The "/oic/sec/cred" Resource's use of the DELETE operation is not in accordance with the OCF Interfaces defined in ISO/IEC 30118-1:2018.

"/oic/sec/cred" Resource is defined in Table 28.

Table 3 – Definition of the "/oic/sec/cred" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/cred	Credentials	oic.r.cred	baseline	Resource containing credentials for Device authentication, verification and data protection	Security

Table 30 defines the Properties of "oic.sec.creds".

Table 4 – Properties of the "oic.sec.creds" Property

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Credential ID	credid	UINT16	0 – 64K-1	Yes	RW		Short credential ID for local references from other Resource

12.4 Certificate Revocation List

12.4.1 CRL Resource Definition

Device certificates and private keys are kept in `cred` Resource. CRL is maintained and updated with a separate `crl` Resource that is newly defined for maintaining the revocation list.

"/oic/sec/crl" Resource is defined in Table 39.

Table 5 – Definition of the "/oic/sec/crl" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/crl	CRLs	oic.r.crl	baseline	Resource containing CRLs for Device certificate revocation	Security

Table 40 defines the Properties of "/oic/sec/crl" Resource.

Table 6 – Properties of the "/oic/sec/crl" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
CRL Id	crlid	UINT16	0 – 64K-1	RW	Yes	CRL ID for references from other Resource
This Update	thisupdate	String	N/A	RW	Yes	This indicates the time when this CRL has been updated.(UTC)
CRL Data	crldata	String	N/A	RW	Yes	CRL data based on CertificateList in CRL profile

12.5 ACL Resources

12.5.1 ACL Resources General

12.5.2 OCF Access Control List (ACL) BNF defines ACL structures.

12.5.3 ACL Resource

There are two types of ACLs, "acl" is a list of type "ace" and "acl2" is a list of type "ace2". A Device shall not host the /acl Resource.

NOTE The /acl Resource is defined for backward compatibility and use by Provisioning Tools, etc.

In order to provide an interface which allows management of array elements of the "aclist2" Property associated with an "/oic/sec/acl2" Resource. The RETRIEVE, UPDATE and DELETE operations on the" /oic/sec/acl2" Resource SHALL behave as follows:

1) A RETRIEVE shall return the full Resource representation.
2) An UPDATE shall replace or add to the Properties included in the representation sent with the UPDATE request, as follows:

a) If an UPDATE representation includes the array Property, then:

i) Supplied ACEs with an "aceid" that matches an existing "aceid" shall replace completely the corresponding ACE in the existing "aces2" array.

ii) Supplied ACEs without an "aceid" shall be appended to the existing "aces2" array, and a unique (to the acl2 Resource) "aceid" shall be created and assigned to the new ACE by the Server. The "aceid" of a deleted ACE should not be reused, to improve the determinism of the interface and reduce opportunity for race conditions.

iii) Supplied ACEs with an "aceid" that does not match an existing "aceid" shall be appended to the existing "aces2" array, using the supplied "aceid".

The rows in Table 47 defines the Properties of "oic.sec.acl2".

iv) Table 47 corresponding to the "aclist2" array Property dictate the Device States in which an UPDATE of the "aclist2" array Property is always rejected. If OCF Device is in a Device State where the Access Mode in this row contains "R", then the OCF Device shall reject all UPDATEs of the "aclist2" array Property.

3) A DELETE without query parameters shall remove the entire "aces2" array, but shall not remove the "/oic/sec/acl2" Resource.

4) A DELETE with one or more "aceid" query parameters shall remove the ACE(s) with the corresponding aceid(s) from the "aces2" array.

The rows in Table 47 defines the Properties of "/oic/sec/acl2".

5) Table 47 corresponding to the "aclist2" array Property dictate the Device States in which a DELETE is always rejected. If OCF Device is in a Device State where the Access Mode in this row contains "R", then the OCF Device shall reject all DELETEs.

NOTE The "/oic/sec/acl2" Resource's use of the DELETE operation is not in accordance with the OCF Interfaces defined in ISO/IEC 30118-1:2018.

"oic/sec/acl2" Resource is defined in Table 46.

Table 7 – Definition of the "/oic/sec/acl2" Resource

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

Table 47 defines the Properties of "/oic/sec/acl2" Resource.

Table 8 – Properties of the "/oic/sec/acl2" Resource

Property Name	Value Type	Mandatory	Device State	Access Mode	Description
aclist2	array of oic.sec.ace2	Yes	N/A		The aclist2 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.

12.6 Access Manager ACL Resource

"/oic/sec/amacl" Resource is defined in Table 51.

Table 9 – Definition of the "/oic/sec/amacl" Resource

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

Table 52 defines the Properties of "/oic/sec/amacl" Resource.

Table 10 – Properties of the "oic.r.amacl" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
Resources	resources	oic.sec.ace2.resource-ref	array	RW	Yes	Multiple links to this host's Resources

12.7 Signed ACL Resource

"/oic/sec/sacl" Resource is defined in Table 53.

Table 11 – Definition of the "/oic/sec/sacl" Resource

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

Table 54 defines the Properties of "/oic/sec/sacl" Resource.

Table 12 – Properties of the "/oic/sec/sacl" Resource

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	State	Description
ACE List	aclist2	oic.sec.ace2	array	Yes	N/A	N/A	Access Control Entries in the ACL Resource
					N/A	RESET	Server shall set to manufacturer defaults.
					N/A	RFOTM	Set by DOTS after successful OTM
					N/A	RFPRO	The AMS (referenced via rowneruuid property) shall update the aclist entries after mutually authenticated secure session is established. Access to NCRs is prohibited.
					N/A	RFNOP	Access to NCRs is permitted after a matching ACE is found.
					N/A	SRESET	The DOTS (referenced via devowneruuid Property of "/oic/sec/doxm" Resource) should evaluate the integrity of and may update aclist entries when a secure session is established and the Server and DOTS are authenticated.
Signature	signature	oic.sec.sigtype	N/A	Yes	N/A	N/A	The signature over the ACL Resource

12.8 Provisioning Status Resource

"/oic/sec/pstat" Resource is defined in Table 56.

Table 13 – Definition of the "/oic/sec/pstat" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/pstat	Provisioning Status	oic.r.pstat	baseline	Resource for managing Device provisioning status	Configuration

Table 57 defines the Properties of "/oic/sec/pstat" Resource.

Table 14 – Properties of the "/oic/sec/pstat" Resource

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Device Onboarding State	dos	oic.sec.dostype	N/A	Yes	RW		Device Onboarding State

Table 58 defines the Properties of "oic.sec.dostype".

Table 15 – Properties of the "oic.sec.dostype" Property

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Device Onboarding State	s	UINT16	enum (0=RESET, 1=RFOTM, 2=RFPRO, 3=RFNOP, 4=SRESET	Y	R	RESET	The Device is in a hard reset state.
					RW	RFOTM	Set by DOTS after successful OTM to RFPRO.
					RW	RFPRO	Set by CMS, AMS, DOTS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOTS after successful authentication
					RW	SRESET	Set by CMS, AMS, DOTS after successful authentication
Pending state	p	Boolean	T | F	Y	R	All States	TRUE (1) – "s" state is pending until all necessary changes to Device resources are complete FALSE (0) – "s" state changes are complete

When Device state is RESET:

– All SVR content is removed and reset to manufacturer default values.
– The default manufacturer Device state is RESET.
– NCRs are reset to manufacturer default values.
– NCRs are inaccessible.
– After successfully processing RESET the SRM transitions to RFOTM by setting pstat.dos.s to RFOTM.

When Device state is RFOTM:

– NCRs are inaccessible.

– Before OTM is successful, the deviceuuid Property of "/oic/sec/doxm" Resource shall be set to a temporary non-repeated value as defined in clauses 13.2 and 13.16.
– Before OTM is successful, pstat.dos.s is read-only by unauthenticated requestors
– After the OTM is successful, pstat.dos.s is read-write by authorized requestors.
– The negotiated Device OC is used to create an authenticated session over which the DOTS directs the Device state to transition to RFPRO.
– If an authenticated session cannot be established the ownership transfer session should be disconnected and SRM sets back the Device state to RESET state.
– Ownership transfer session, especially Random PIN OTM, should not exceed 60 seconds, the SRM asserts the OTM failed, should be disconnected, and transitions to RESET (/pstat.dos.s=RESET).
– The DOTS UPDATES the devowneruuid Property in the "/oic/sec/doxm" Resource to a non-nil UUID value. The DOTS (or other authorized client) may update it multiple times while in RFOTM. It is not updatable while in other device states except when the Device state returns to RFOTM through RESET.
– The DOTS may have additional provisioning tasks to perform while in RFOTM. When done, the DOTS UPDATES the "owned" Property in the "/oic/sec/doxm" Resource to "true".

When Device state is RFPRO:

– The pstat.dos.s is read-only by unauthorized requestors and read-write by authorized requestors.
– NCRs are inaccessible, except for Easy Setup Resources, if supported.
– The OCF Server may re-create NCRs.
– An authorized Client may provision SVRs as needed for normal functioning in RFNOP.
– An authorized Client may perform consistency checks on SVRs to determine which shall be re-provisioned.
– Failure to successfully provision SVRs may trigger a state change to RESET. For example, if the Device has already transitioned from SRESET but consistency checks continue to fail.
– The authorized Client sets the /pstat.dos.s=RFNOP.

When Device state is SRESET:

– NCRs are inaccessible. The integrity of NCRs may be suspect but the SRM doesn't attempt to access or reference them.
– SVR integrity is not guaranteed, but access to some SVR Properties is necessary. These include devowneruuid Property of the "/oic/sec/doxm" Resource, "creds":[{…,{"subjectuuid":<devowneruuid>},…}] Property of the "/oic/sec/cred" Resource and pstat.dos.s of "/oic/sec/pstat" Resource.
– The certificates that identify and authorize the Device owner are sufficient to re-create minimalist "/oic/sec/cred" and "/oic/sec/doxm" Resources enabling Device owner control of SRESET. If the SRM can't establish these Resources, then it will transition to RESET state.
– An authorized Client performs SVR consistency checks. The caller may provision SVRs as needed to ensure they are available for continued provisioning in RFPRO or for normal functioning in RFNOP.
– The authorized Device owner may avoid entering RESET state and RFOTM by UPDATING pstat.dos.s with RFPRO or RFNOP values
– ACLs on SVR are presumed to be invalid. Access authorization is granted according to Device owner privileges.

– The SRM asserts a Client-directed operational mode (e.g. /pstat.om=CLIENT_DIRECTED).

12.9 Certificate Signing Request Resource

The "/oic/sec/csr" Resource is used by a Device to provide its desired identity, public key to be certified, and a proof of possession of the corresponding private key in the form of a IETF RFC 2986 PKCS#10 Certification Request. If the Device supports certificates (i.e. the sct Property of "/oic/sec/doxm" Resource has a 1 in the 0x8 bit position), the Device shall have a "/oic/sec/csr" Resource.

"/oic/sec/csr" Resource is defined in Table 64.

Table 16 – Definition of the "/oic/sec/csr" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/csr	Certificate Signing Request	oic.r.csr	baseline	The CSR resource contains a Certificate Signing Request for the Device's public key.	Configuration

Table 65 defines the Properties of "/oic/sec/csr" Resource.

Table 17 – Properties of the "/oic/sec/csr" Resource

Property Title	Property Name	Value Type	Access Mode	Mandatory	Description
Certificate Signing Request	csr	String	R	Yes	Contains the signed CSR encoded according to the encoding Property
Encoding	encoding	String	R	Yes	A string specifying the encoding format of the data contained in the csr Property "oic.sec.encoding.pem" – Encoding for PEM-encoded certificate signing request "oic.sec.encoding.der" – Encoding for DER-encoded certificate signing request

12.10 Roles Resource

1) A RETRIEVE request shall return all previously asserted roles associated with the currently connected and authenticated Client's identity. RETRIEVE requests with a "credid" query parameter is not supported; all previously asserted roles associated with the currently connected and authenticated Client's identity are returned.
2) An UPDATE request that includes the "roles" Property shall replace or add to the Properties included in the array as follows:
   a) If either the "publicdata" or the "optionaldata" are different than the existing entries in the "roles" array, the entry shall be added to the "roles" array with a new, unique "credid" value.
   b) If both the "publicdata" and the "optionaldata" match an existing entry in the "roles" array, the entry shall be considered to be the same. The Server shall reply with a 2.04 Changed response and a duplicate entry shall not be added to the array.
   c) The "credid" Property is optional in an UPDATE request and if included, it may be ignored by the Server. The Server shall assign a unique "credid" value for every entry of the "roles" array.
3) A DELETE request without a "credid" query parameter shall remove all entries from the "/oic/sec/roles" resource array corresponding to the currently connected and authenticated Client's identity.

4) A DELETE request with a "credid" query parameter shall remove only the entries of the "/oic/sec/roles" resource array corresponding to the currently connected and authenticated Client's identity and where the corresponding "credid" matches the entry.

NOTE The "/oic/sec/roles" Resource's use of the DELETE operation is not in accordance with the OCF Interfaces defined in ISO/IEC 30118-1:2018.

"/oic/sec/roles" Resource is defined in Table 66.

Table 18 – Definition of the "/oic/sec/roles" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/roles	Roles	oic.r.roles	baseline	Resource containing roles that have previously been asserted to this Server	Security

Table 67 defines the Properties of "/oic/sec/roles" Resource.

Table 19 – Properties of the "/oic/sec/roles" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
Roles	roles	oic.sec.cred	array	RW	Yes	List of roles previously asserted to this Server

Because "/oic/sec/roles" shares the "oic.sec.cred" schema with "/oic/sec/roles", "subjectuuid" is a required Property. However, "subjectuuid" is not used in a role certificate. Therefore, a Device may ignore the "subjectuuid" Property if the Property is contained in an UPDATE request to the "/oic/sec/roles" Resource.

12.11 Account Resource

The DELETE operation on the OCF Cloud's "/oic/sec/account" Resource should behave as follows:

– To deregister with the OCF Cloud, a DELETE operation shall be sent with the "accesstoken" and either "uid", or "di" to be deregistered with the OCF Cloud. On DELETE with the OCF Cloud, the Device should also delete values internally stored. Once deregister with an OCF Cloud, Device can connect to any other OCF Cloud. Device deregistered need to go through the steps in 7.5 again to be registered with the OCF Cloud.

"/oic/sec/account" Resource is defined in Table 68.

Table 20 – Definition of the "/oic/sec/account" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/account	Account	oic.r.account	oic.if.baseline	Resource used for a device to add itself under a given credential	N/A

Table 69 defines the Properties of "/oic/sec/account" Resource.

Table 21 – Properties of the "/oic/sec/account" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
Device ID	di	string	uuid	W	Yes	Unique Device identifier
Auth Provider	authprovider	string	N/A	W	No	The name of Authorization Provider through which Access Token was obtained.
Access-Token	accesstoken	string	Non-empty string	RW	Yes	Access-Token used for communication with OCF Cloud after account creation
Refresh Token	refreshtoken	string	Non-empty string	R	Yes	Refresh token can be used to refresh the Access Token before getting expired
Token Expiration	expiresin	integer	-	R	Yes	Access-Token life time in seconds (-1 if permanent)
User ID	uid	string	uuid	R	Yes	Unique OCF Cloud User identifier
Redirect URI	redirecturi	string	-	R	No	Using this URI, the Client needs to reconnect to a redirected OCF Cloud. If provided, this value shall be used by the Device instead of Mediator-provided URI during the Device Registration.

12.12 Account Session resource

The "/oic/sec/session" Resource hosted on the OCF Cloud is used for creating connections with the OCF Cloud subsequent to Device registration though "/oic/sec/account" Resource. The "/oic/sec/session" Resource requires the device ID, User ID and Access Token which are stored securely on the Device.

"/oic/sec/session" Resource is defined in Table 70.

Table 22 – Definition of the "/oic/sec/session" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/session	Account Session	oic.r.session	oic.if.baseline	Resource that enables a device to manage its session using login or logout	N/A

Table 71 defines the Properties of "/oic/sec/session" Resource.

Table 23 – Properties of the "/oic/sec/session" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
User ID	uid	string	uuid	W	Yes	User ID which provided by Device Registration process
Device ID	di	string	uuid	W	Yes	Unique device id registered for a Device
Access Token	accesstoken	string	A string of at least one character	W	Yes	Access-Token used to grant access right for the Device to login/sign-in
Login Status	login	boolean	N/A	W	Yes	Action for the request: true = login, false = logout
Token Expiration	expiresin	integer	N/A	R	Yes	Remaining Access-Token life time in seconds (-1 if permanent) This Property is only provided to Device during connection establishment (when "login" Property Value equals "true"), it's not available otherwise

12.13 Account Token Refresh Resource

The "/oic/sec/tokenrefresh" Resource is used by the Device for refreshing the Access Token.

The "/oic/sec/tokenrefresh" Resource is hosted by the OCF Cloud. It should be only accessible on a secure channel; non-secure channel cannot access this Resource.

The Device should use "/oic/sec/tokenrefresh" to refresh the Access Token with the OCF Cloud, when the time specified in "expiresin" is near.

The RETRIEVE operation on OCF Cloud's "/oic/sec/tokenrefresh" Resource is not allowed and the OCF Cloud is expected to reject all attempts to perform such operation.

The UPDATE operation is defined as follows for "/oic/sec/tokenrefresh" Resource

– The Device attempting to refresh the Access Token shall send an UPDATE request message to the OCF Cloud's "/oic/sec/tokenrefresh" Resource. The message shall include the "di" Property Value of "/oic/d" Resource, "uid" and "refreshtoken", as returned by OCF Cloud.

– OCF Cloud response is expected to include a "refreshtoken", new "accesstoken", and "expiresin". Received "accesstoken" is to be treated by Device as an Access Token with "Bearer" token type as defined in IETF RFC 6750. This Access Token is the permission for the Device to access the OCF Cloud. Received "refreshtoken" is to be treated by Device as a Refresh Token as defined in IETF RFC 6749. Received "refreshtoken" may be the new Refresh Token or the same one as provided by the Device in the UPDATE request. In case when new distinct "refreshtoken" is provided by the OCF Cloud, the Device shall discard the old value. The OCF Cloud's response values "refreshtoken", "acesstoken" and "expiresin" are securely stored on the Device.

"/oic/sec/tokenrefresh" Resource is defined in Table 72.

Table 24 – Definition of the "/oic/sec/tokenrefresh" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/tokenrefresh	Token Refresh	oic.r.tokenrefresh	oic.if.baseline	Resource to manage the access-token using refresh token	N/A

Table 73 defines the Properties of "/oic/sec/tokenrefresh" Resource.

Table 25 – Properties of the "/oic/sec/tokenrefresh" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
User ID	uid	string	uuid	W	Yes	User ID which provided by Sign-up process
Device ID	di	string	uuid	W	Yes	Unique device id registered for an OCF Cloud User account
Refresh Token	refreshtoken	string	A string of at least one character	RW	Yes	Refresh token received by account management or during token refresh procedure
Access Token	accesstoken	string	A string of at least one character	R	Yes	Granted Access-Token
Token Expiration	expiresin	integer	-	R	Yes	Access-Token life time in seconds (-1 if permanent)

12.14 Security Virtual Resources (SVRs) and Access Policy

The SVRs expose the security-related Properties of the Device.

Granting access requests (RETRIEVE, UPDATE, DELETE, etc.) for these SVRs to unauthenticated (anonymous) Clients could create privacy or security concerns.

For example, when the Device onboarding State is RFOTM, it is necessary to grant requests for the "/oic/sec/doxm" Resource to anonymous requesters, so that the Device can be discovered and onboarded by an OBT. Subsequently, it might be preferable to deny requests for the "/oic/sec/doxm" Resource to anonymous requesters, to preserve privacy.

13 Security Hardening Guidelines/ Execution Environment Security

13.1 Preamble

13.2 Execution Environment Elements

13.2.1 Execution Environment Elements General

13.2.2 Secure Storage

13.2.2.1 Secure Storage General

13.2.2.2 Hardware Secure Storage

13.2.2.3 Software Storage

13.2.2.4 Additional Security Guidelines and Best Practices

Some general practices that can help ensure that Sensitive Data is not compromised by various forms of security attacks:

1) FIPS Random Number Generator ("RNG") – Insufficient randomness or entropy in the RNG used for authentication challenges can substantially degrade security strength. For this reason, it is recommended that a FIPS 800-90A-compliant RNG with a certified noise source be used for all authentication challenges.
2) Secure download and boot – To prevent the loading and execution of malicious software, where it is practical, it is recommended that Secure Download and Secure Boot methods that authenticate a binary's source as well as its contents be used.
3) Deprecated algorithms – Algorithms included but not limited to the list below are considered unsecure and shall not be used for any security-related function:
   a) SHA-1
   b) MD5
   c) RC4
   d) RSA 1024
4) Encrypted transmission between blocks or components – Even if critical Sensitive Data is stored in Secure Storage, any use of that data that requires its transmission out of that Secure Storage should be encrypted to prevent eavesdropping by malicious software within an MCU/MPU.
5) It is recommended to avoid using wildcard in Subject Id ("*"), when setting up "/oic/sec/cred" Resource entries, since this opens up an identity spoofing opportunity.

13.3 Secure Boot

13.4 Attestation

13.5 Software Update

13.6 Non-OCF Endpoint interoperability

13.7 Security Levels

13.8 Security Profiles

13.8.1 Security Profiles General

13.8.2 Identification of Security Profiles (Normative)

13.8.2.1 Security Profiles in Prior Documents

13.8.2.2 Security Profile Resource Definition

The "/oic/sec/sp" Resource is used by the OCF Device to show which OCF Security Profiles the OCF Device is capable of supporting and which are authorized for use by the OCF Security Domain owner. Properties of the Resource identify which OCF Security Profile is currently operational. The ocfSecurityProfileOID value type shall represent OID values and may reference an entry in the form of strings (UTF-8).

"/oic/sec/sp" Resource is defined in Table 76.

Table 26 – Definition of the "/oic/sec/sp" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/sp	Security Profile Resource Definition	oic.r.sp	oic.if.baseline	Resource specifying supported and current security profile(s)	Discoverable

Table 77 defines the Properties of "/oic/sec/sp" Resource.

Table 27 – Properties of the "/oic/sec/sp" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
Supported Security Profiles	supportedprofiles	ocfSecurityProfileOID	array	RW	Yes	Array of supported Security Profiles (e.g. ["1.3.6.1.4.1.51414.0.0.2.0","1.3.6.1.4.1.51414.0.0.3.0"])
SecurityProfile	currentprofile	ocfSecurityProfileOID	N/A	RW	Yes	Currently active Security Profile (e.g. "1.3.6.1.4.1.51414.0.0.3.0")