OCF Security Specification

VERSION 2.0.2 | April 2019
LEGAL DISCLAIMER

NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY ANY OF THE AUTHORS OR DEVELOPERS OF THIS DOCUMENT. THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AUTHORS AND DEVELOPERS OF THIS SPECIFICATION HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OPEN INTERCONNECT CONSORTIUM, INC. FURTHER DISCLAIMS ANY AND ALL WARRANTIES OF NON-INFRINGEMENT, ACCURACY OR LACK OF VIRUSES.

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 © 2016-2019 Open Connectivity Foundation, Inc. All rights reserved.

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

1 Scope ....................................................................................................... 1
2 Normative References ............................................................................ 1
3 Terms, definitions, and abbreviated terms ........................................... 3
   3.1 Terms and definitions ..................................................................... 3
   3.2 Abbreviated terms ......................................................................... 6
4 Document Conventions and Organization ........................................... 10
   4.1 Conventions ................................................................................. 10
   4.2 Notation ....................................................................................... 10
   4.3 Data types ................................................................................... 11
   4.4 Document structure ..................................................................... 11
5 Security Overview .................................................................................. 12
   5.1 Preamble ..................................................................................... 12
   5.2 Access Control ............................................................................ 14
      5.2.1 ACL Architecture .................................................................. 16
      5.2.2 Access Control Scoping Levels ............................................ 19
   5.3 Onboarding Overview ................................................................... 21
      5.3.1 Onboarding General ............................................................. 21
      5.3.2 Onboarding Steps .................................................................. 23
      5.3.3 Establishing a Device Owner .................................................. 24
      5.3.4 Provisioning for Normal Operation ....................................... 25
      5.3.5 Device Provisioning for OCF Cloud and Device Registration Overview ........ 25
      5.3.6 OCF Compliance Management System .................................. 25
   5.4 Provisioning .................................................................................. 26
      5.4.1 Provisioning General ............................................................. 26
      5.4.2 Provisioning other services .................................................... 26
      5.4.3 Provisioning Credentials for Normal Operation ...................... 27
      5.4.4 Role Assignment and Provisioning for Normal Operation ........ 27
      5.4.5 ACL provisioning ................................................................. 27
   5.5 Secure Resource Manager (SRM) .................................................. 27
   5.6 Credential Overview ...................................................................... 28
6 Security for the Discovery Process ....................................................... 29
   6.1 Preamble ..................................................................................... 29
   6.2 Security Considerations for Discovery .......................................... 29
7 Security Provisioning .............................................................................. 32
   7.1 Device Identity ............................................................................. 32
      7.1.1 General Device Identity ........................................................ 32
      7.1.2 Device Identity for Devices with UAID [Deprecated] .............. 32
   7.2 Device Ownership ......................................................................... 32
   7.3 Device Ownership Transfer Methods .......................................... 33
      7.3.1 OTM implementation requirements ....................................... 33
      7.3.2 SharedKey Credential Calculation ........................................ 35
      7.3.3 Certificate Credential Generation .......................................... 35

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
C.12.1 Introduction ................................................................. 229
C.12.2 Well-known URI .......................................................... 229
C.12.3 Resource type .............................................................. 229
C.12.4 OpenAPI 2.0 definition ............................................... 229
C.12.5 Property definition ....................................................... 237
C.12.6 CRUDN behaviour ....................................................... 237
C.13 Session ............................................................................. 238
C.13.1 Introduction .................................................................... 238
C.13.2 Well-known URI .......................................................... 238
C.13.3 Resource type .............................................................. 238
C.13.4 OpenAPI 2.0 definition ............................................... 238
C.13.5 Property definition ....................................................... 240
C.13.6 CRUDN behaviour ....................................................... 240
C.14 Security Profile ............................................................... 241
C.14.1 Introduction .................................................................... 241
C.14.2 Well-known URI .......................................................... 241
C.14.3 Resource type .............................................................. 241
C.14.4 OpenAPI 2.0 definition ............................................... 241
C.14.5 Property definition ....................................................... 243
C.14.6 CRUDN behaviour ....................................................... 243
C.15 Token Refresh ................................................................... 244
C.15.1 Introduction .................................................................... 244
C.15.2 Well-known URI .......................................................... 244
C.15.3 Resource type .............................................................. 244
C.15.4 OpenAPI 2.0 definition ............................................... 244
C.15.5 Property definition ....................................................... 246
C.15.6 CRUDN behaviour ....................................................... 247
Annex D (informative) OID definitions .................................... 248
Annex E (informative) Security considerations specific to Bridged Protocols ........................................ 250
E.1 Security Considerations specific to the AllJoyn Protocol .................................................... 250
E.2 Security Considerations specific to the Bluetooth LE Protocol ........................................ 250
E.3 Security Considerations specific to the oneM2M Protocol .................................................... 250
E.4 Security Considerations specific to the U+ Protocol ...................................................... 251
E.5 Security Considerations specific to the Z-Wave Protocol .................................................... 251
E.6 Security Considerations specific to the Zigbee Protocol ..................................................... 252
FIGURES

Figure 1 – OCF Interaction ..............................................................................10
Figure 2 – OCF Layers ..................................................................................12
Figure 3 – OCF Security Enforcement Points ........................................................14
Figure 4 – Use case-1 showing simple ACL enforcement ........................................17
Figure 5 – Use case 2: A policy for the requested Resource is missing ..................17
Figure 6 – Use case-3 showing AMS supported ACL ..........................................18
Figure 7 – Use case-4 showing dynamically obtained ACL from an AMS ..............19
Figure 8 – Example Resource definition with opaque Properties ..........................20
Figure 9 – Property Level Access Control ............................................................20
Figure 10 – Onboarding Overview .....................................................................22
Figure 11 – OCF Onboarding Process ................................................................24
Figure 12 – OCF's SRM Architecture ..................................................................28
Figure 13 – Discover New Device Sequence .......................................................34
Figure 14 – A Just Works OTM .........................................................................36
Figure 15 – Random PIN-based OTM .................................................................37
Figure 16 – Manufacturer Certificate Based OTM Sequence ...............................41
Figure 17 – Vendor-specific Owner Transfer Sequence ..........................................42
Figure 18 – Establish Device Identity Flow ..........................................................44
Figure 19 – Owner Credential Selection Provisioning Sequence ............................45
Figure 20 – Symmetric Owner Credential Provisioning Sequence ..........................46
Figure 21 – Asymmetric Owner Credential Provisioning Sequence ..........................47
Figure 22 – Configure Device Services ...............................................................49
Figure 23 – Provision New Device for Peer to Peer Interaction Sequence ..............50
Figure 24 – Example of Client-directed provisioning ............................................53
Figure 25 – Example of Server-directed provisioning using a single provisioning service ....54
Figure 26 – Example of Server-directed provisioning involving multiple support services ....57
Figure 27 – Device state model ........................................................................59
Figure 28 – OBT Sanity Check Sequence in SRESET ...........................................63
Figure 29 – Client-directed Certificate Transfer ....................................................80
Figure 30 – Client-directed CRL Transfer ............................................................81
Figure 32 – Asserting a role with a certificate role credential ..................................85
Figure 33 – Device connection with OCF Cloud .................................................88
Figure 34 – OCF Security Resources .................................................................98
Figure 35 – "/oic/sec/cred" Resource and Properties ............................................99
Figure 36 – "/oic/sec/acl2" Resource and Properties ............................................99
Figure 37 – "/oic/sec/amacl" Resource and Properties ..........................................100
Figure 38 – "/oic/sec/sacl" Resource and Properties ............................................100
Figure 39 – Example of Soft AP and Easy Setup Resource in different Device states ....139

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
Table 38 – 256-bit symmetric key

Table 39 – Definition of the "oic.r.ctrl" Resource

Table 40 – Properties of the "oic.r.ctrl" Resource

Table 41 – BNF Definition of OCF ACL

Table 42 – Definition of the "oic.r.acl" Resource

Table 43 – Properties of the "oic.r.acl" Resource

Table 44 – Properties of the "oic.r.ace" Property

Table 45 – Value Definition of the "oic.sec.crudntype" Property

Table 46 – Definition of the "oic.sec.acl2" Resource

Table 47 – Properties of the "oic.sec.acl2" Resource

Table 48 – "oic.sec.ace2" data type definition

Table 49 – "oic.sec.ace2.resource-ref" data type definition

Table 50 – Value definition "oic.sec.conntype" Property

Table 51 – Definition of the "oic.r.amacl" Resource

Table 52 – Properties of the "oic.r.amacl" Resource

Table 53 – Definition of the "oic.r.sacl" Resource

Table 54 – Properties of the "oic.r.sacl" Resource

Table 55 – Properties of the "oic.sec.sigtype" Property

Table 56 – Definition of the "oic.r.pstat" Resource

Table 57 – Properties of the "oic.r.pstat" Resource

Table 58 – Properties of the "/oic/sec/dostype" Property

Table 59 – Definition of the "oic.sec.dpmtype" Property

Table 60 – Value Definition of the "oic.sec.dpmtype" Property (Low-Byte)

Table 61 – Value Definition of the "oic.sec.dpmtype" Property (High-Byte)

Table 62 – Definition of the "oic.sec.pomtype" Property

Table 63 – Value Definition of the "oic.sec.pomtype" Property

Table 64 – Definition of the "oic.r.csr" Resource

Table 65 – Properties of the "oic.r.csr" Resource

Table 66 – Definition of the "oic.r.roles" Resource

Table 67 – Properties of the "oic.r.roles" Resource

Table 68 – Definition of the "oic.r.account" Resource

Table 69 – Properties of the "oic.r.account" Resource

Table 70 – Definition of the "oic.r.session" Resource

Table 71 – Properties of the "oic.r.session" Resource

Table 72 – Definition of the "oic.r.tokenrefresh" Resource

Table 73 – Properties of the "oic.r.tokenrefresh" Resource

Table 74 – Core Resource Properties Access Modes given various Device States

Table 75 – Examples of Sensitive Data

Table 76 – Definition of the "oic.sec.sp" Resource

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
1 Scope

This document defines security objectives, philosophy, resources and mechanism that impacts OCF base layers of ISO/IEC 30118-1:2018. ISO/IEC 30118-1:2018 contains informative security content. The OCF Security Specification contains security normative content and may contain informative content related to the OCF base or other OCF documents.

2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

https://www.iso.org/standard/53238.html
Latest version available at: https://openconnectivity.org/specs/OCF_Core_Specification.pdf

https://www.iso.org/standard/74240.html

OCF Wi-Fi Easy Setup Specification
Latest version available at: https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf

OCF Cloud Specification


3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions
For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1:2018 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:
– ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1 Access Management Service (AMS)
dynamically constructs ACL Resources in response to a Device Resource request.

Note 1 to entry: An AMS can evaluate access policies remotely and supply the result to a Server which allows or denies a pending access request. An AMS is authorised to provision ACL Resources.

3.1.2 Access Token
a credential used to access protected resources. An Access Token is a string representing an authorization issued to the client.

3.1.3 Authorization Provider
a Server issuing Access Tokens (3.1.2) to the Client after successfully authenticating the OCF Cloud User (3.1.16) and obtaining authorization.

Note 1 to entry: Also known as authorization server in IETF RFC 6749.

3.1.4 Client
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.5 Credential Management Service (CMS)
a name and Resource Type ("oic.sec.cms") given to a Device that is authorized to provision credential Resources.

3.1.6 Device
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.7 Device Class
Note 1 to entry: As defined in IETF RFC 7228. IETF RFC 7228 defines classes of constrained devices that distinguish when the OCF small footprint stack is used vs. a large footprint stack. Class 2 and below is for small footprint stacks.

3.1.8 Device ID
a stack instance identifier.

3.1.9 Device Ownership Transfer Service (DOTS)
a logical entity that establishes device ownership
3.1.10 Device Registration
a process by which Device is enrolled/registered to the OCF Cloud infrastructure (using Device certificate and unique credential) and becomes ready for further remote operation through the cloud interface (e.g. connection to remote Resources or publishing of its own Resources for access).

3.1.11 End-Entity
any certificate holder which is not a Root or Intermediate Certificate Authority.

Note 1 to entry: Typically, a device certificate.

3.1.12 Entity
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.13 OCF Interface
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.14 Intermediary
a Device that implements both Client and Server roles and may perform protocol translation, virtual device to physical device mapping or Resource translation

3.1.15 OCF Cipher Suite
a set of algorithms and parameters that define the cryptographic functionality of a Device. The OCF Cipher Suite includes the definition of the public key group operations, signatures, and specific hashing and encoding used to support the public key.

3.1.16 OCF Cloud User
a person or organization authorizing a set of Devices to interact with each other via an OCF Cloud.

Note 1 to entry: For each of the Devices, the OCF Cloud User is either the same as, or a delegate of, the person or organization that onboarded that Device. The OCF Cloud User delegates, to the OCF Cloud authority, authority to route between Devices registered by the OCF Cloud User. The OCF Cloud delegtes, to the OCF Cloud User, authority to select the set of Devices which can register and use the services of the OCF Cloud.

3.1.17 OCF Rooted Certificate Chain
a collection of X.509 v3 certificates in which each certificate chains to a trust anchor certificate which has been issued by a certificate authority under the direction, authority, and approval of the Open Connectivity Foundation Board of Directors as a trusted root for the OCF ecosystem.

3.1.18 Onboarding Tool (OBT)
a tool that implements DOTS(3.1.9), AMS(3.1.1) and CMS(3.1.5) functionality

3.1.19 Out of Band Method
any mechanism for delivery of a secret from one party to another, not specified by OCF

3.1.20 Owner Credential (OC)
credential, provisioned by an OBT(3.1.18) to a Device during onboarding, for the purposes of mutual authentication of the Device and OBT(3.1.18) during subsequent interactions
3.1.21 Platform ID
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.22 Property
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.23 Resource
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.24 Role (Network context)
stereotyped behavior of a Device; one of [Client, Server or Intermediary]

3.1.25 Role Identifier
a Property of an OCF credentials Resource or element in a role certificate that identifies a privileged role that a Server Device associates with a Client Device for the purposes of making authorization decisions when the Client Device requests access to Device Resources.

3.1.26 Secure Resource Manager (SRM)
a module in the OCF Core that implements security functionality that includes management of security Resources such as ACLs, credentials and Device owner transfer state.

3.1.27 Security Virtual Resource (SVR)
a resource supporting security features.
Note 1 to entry: For a list of all the SVRs please see clause 13.

3.1.28 Server
Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.29 Trust Anchor
a well-defined, shared authority, within a trust hierarchy, by which two cryptographic entities (e.g. a Device and an OBT(3.1.18)) can assume trust.

3.1.30 Unique Authenticable Identifier
a unique identifier created from the hash of a public key and associated OCF Cipher Suite that is used to create the Device ID.
Note 1 to entry: The ownership of a UAID may be authenticated by peer Devices.

3.1.31 Device Configuration Resource (DCR)
a Resource that is any of the following:
a) a Discovery Core Resource, or
b) a Security Virtual Resource, or
c) a Wi-Fi Easy Setup Resource, or
d) a CoAP Cloud Configuration Resource.
3.1.32 Non-Configuration Resource (NCR)
a Resource that is not a Device Configuration Resource (3.1.31).

3.1.33 Bridged Device
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.34 Bridged Protocol
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.35 Bridge
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.36 Bridging Platform
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.37 Virtual Bridged Device
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.38 Virtual OCF Device
Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.39 OCF Security Domain
set of onboarded OCF Devices that are provisioned with credentialing information for confidential
communication with one another

3.1.40 Owned (or "in Owned State")
having the "owned" Property of the "/oic/sec/doxm" resource equal to "TRUE"

3.1.41 Unowned (or "in Unowned State")
having the "owned" Property of the "/oic/sec/doxm" resource equal to "FALSE"

3.2 Abbreviated terms
3.2.1 AC
Access Control

3.2.2 ACE
Access Control Entry

3.2.3 ACL
Access Control List

3.2.4 AES
Advanced Encryption Standard
Note 1 to entry: See NIST FIPS 197, "Advanced Encryption Standard (AES)"
3.2.5 AMS
Access Management Service

3.2.6 CMS
Credential Management Service

3.2.7 CRUDN
CREATE, RETRIEVE, UPDATE, DELETE, NOTIFY

3.2.8 CSR
Certificate Signing Request

3.2.9 CVC
Code Verification Certificate

3.2.10 ECC
Elliptic Curve Cryptography

3.2.11 ECDSA
Elliptic Curve Digital Signature Algorithm

3.2.12 ECU
Extended Key Usage

3.2.13 EPC
Embedded Platform Credential

3.2.14 EPK
Embedded Public Key

3.2.15 DOTS
Device Ownership Transfer Service

3.2.16 DPKP
Dynamic Public Key Pair

3.2.17 ID
Identity/Identifier

3.2.18 JSON
JavaScript Object Notation.

3.2.19 JWS JSON Web Signature.

Note 1 to entry: See IETF RFC 7515, "JSON Web Signature (JWS)"

3.2.20 KDF Key Derivation Function

3.2.21 MAC Message Authentication Code

3.2.22 MITM Man-in-the-Middle

3.2.23 NVRAM Non-Volatile Random-Access Memory

3.2.24 OC Owner Credential

3.2.25 OCSP Online Certificate Status Protocol

3.2.26 OBT Onboarding Tool

3.2.27 OID Object Identifier

3.2.28 OTM Owner Transfer Method

3.2.29 OOB Out of Band

3.2.30 OWASP Open Web Application Security Project.

Note 1 to entry: See https://www.owasp.org/

3.2.31 PE Policy Engine

3.2.32 PIN Personal Identification Number
3.2.33 PPSK PIN-authenticated pre-shared key

3.2.34 PRF Pseudo Random Function

3.2.35 PSI Persistent Storage Interface

3.2.36 PSK Pre Shared Key

3.2.37 RBAC Role Based Access Control

3.2.38 RM Resource Manager

3.2.39 RNG Random Number Generator

3.2.40 SAACL Signed Access Control List

3.2.41 SBAC Subject Based Access Control

3.2.42 SEE Secure Execution Environment

3.2.43 SRM Secure Resource Manager

3.2.44 SVR Security Virtual Resource

3.2.45 SW Software

3.2.46 UAID Unique Authenticable Identifier
3.2.47 URI
Uniform Resource Identifier


3.2.48 VOD
Virtual OCF Device


4 Document Conventions and Organization

4.1 Conventions
This document defines Resources, protocols and conventions used to implement security for OCF core framework and applications.

For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1:2018 apply.

Figure 1 depicts interaction between OCF Devices.

Figure 1 – OCF Interaction

Devices may implement a Client role that performs Actions on Servers. Actions access Resources managed by Servers. The OCF stack enforces access policies on Resources. End-to-end Device interaction can be protected using session protection protocol (e.g. DTLS) or with data encryption methods.

4.2 Notation
In this document, features are described as required, recommended, allowed or DEPRECATED as follows:

Required (or shall or mandatory).

These basic features shall be implemented to comply with OCF Core Architecture. The phrases "shall not", and "PROHIBITED" indicate behaviour that is prohibited, i.e. that if performed means the implementation is not in compliance.

Recommended (or should).

These features add functionality supported by OCF Core Architecture and should be implemented. Recommended features take advantage of the capabilities OCF Core Architecture, usually without imposing major increase of complexity. Notice that for compliance testing, if a recommended feature is implemented, it shall meet the specified requirements to be in
compliance with these guidelines. Some recommended features could become requirements in the future. The phrase "should not" indicates behaviour that is permitted but not recommended.

**Allowed (may or allowed)**

These features are neither required nor recommended by OCF Core Architecture, but if the feature is implemented, it shall meet the specified requirements to be in compliance with these guidelines.

**Conditionally allowed (CA)**

The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is allowed, otherwise it is not allowed.

**Conditionally required (CR)**

The definition or behaviour depends on a condition. If the specified condition is met, then the definition or behaviour is required. Otherwise the definition or behaviour is allowed as default unless specifically defined as not allowed.

**DEPRECATED**

Although these features are still described in this document, they should not be implemented except for backward compatibility. The occurrence of a deprecated feature during operation of an implementation compliant with the current document has no effect on the implementation's operation and does not produce any error conditions. Backward compatibility may require that a feature is implemented and functions as specified but it shall never be used by implementations compliant with this document.

Strings that are to be taken literally are enclosed in "double quotes".

Words that are emphasized are printed in italic.

### 4.3 Data types


### 4.4 Document structure

Informative clauses may be found in the Overview clauses, while normative clauses fall outside of those clauses.

The Security Specification may use the oneM2M Release 3 Specifications, http://www.onem2m.org/technical/published-drafts

OpenAPI specification as the API definition language. The mapping of the CRUDN actions is specified in ISO/IEC 30118-1:2018.
5 Security Overview

5.1 Preamble

This is an informative clause. The goal for the OCF security architecture is to protect the Resources and all aspects of HW and SW that are used to support the protection of Resource.

From OCF perspective, a Device is a logical entity that conforms to the OCF documents. In an interaction between the Devices, the Device acting as the Server holds and controls the Resources and provides the Device acting as a Client with access to those Resources, subject to a set of security mechanisms. The Platform, hosting the Device may provide security hardening that will be required for ensuring robustness of the variety of operations described in this document.

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".

d) Requests received by a Server over an unsecured channel are treated as anonymous and 
not associated with any deviceUUID or roleid.

3) The Client submits a request to the Server.

4) The Server receives the request.

a) If the request is received over an unsecured channel, the Server treats the request as 
anonymous and no deviceUUID or roleid are associated with the request.

b) If the request is received over a secure channel, then the Server associates the 
deviceUUID with the request, and the Server associates all valid roleid of the Client with 
the request.

c) The Server then consults the Access Control List (ACL), and looks for an ACL entry 
matching the following criteria:

   i) The requested Resource matches a Resource reference in the ACE

   ii) The requested operation is permitted by the "permissions" of the ACE, and

   iii) The "subjectUUID" contains either one of a special set of wildcard values or, if the 
Device is not anonymous, the subject matches the Client Deviceid associated with the 
request or a valid roleid associated with the request. The wildcard values match either 
all Devices communicating over an authenticated and encrypted session, or all 
Devices communicating over an unauthenticated and unencrypted session.

   If there is a matching ACE, then access to the Resource is permitted; otherwise 
access is denied. Access is enforced by the Server's Secure Resource manager 
(SRM).

5) The Server sends a response back to the Client.

Resource protection includes protection of data both while at rest and during transit. Aside from 
access control mechanisms, the OCF Security Specification does not include specification of 
secure storage of Resources, while stored at Servers. However, at rest protection for security 
Resources is expected to be provided through a combination of secure storage and access 
control. Secure storage can be accomplished through use of hardware security or encryption of 
data at rest. The exact implementation of secure storage is subject to a set of hardening 
requirements that are specified in clause 14 and may be subject to certification guidelines.

Data in transit protection, on the other hand, will be specified fully as a normative part of this 
document. In transit protection may be afforded at the resource layer or transport layer. This 
document only supports in transit protection at transport layer through use of mechanisms such 
as DTLS.

NOTE: DTLS will provide packet by packet protection, rather than protection for the payload as whole. For instance, if 
the integrity of the entire payload as a whole is required, separate signature mechanisms must have already been in 
place before passing the packet down to the transport layer.

Figure 3 depicts OCF Security Enforcement Points.
Figure 3 – 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"
- 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

The OpenAPI 2.0 definitions (Annex C) used in this document are normative. This includes that all defined payloads shall comply with the indicated OpenAPI 2.0 definitions. Annex C contains all of the OpenAPI 2.0 definitions for Resource Types defined in this document.

5.2 Access Control

The OCF framework assumes that Resources are hosted by a Server and are made available to Clients subject to access control and authorization mechanisms. The Resources at the end point are protected through implementation of access control, authentication and confidentiality protection. This clause provides an overview of Access Control (AC) through the use of ACLs. However, AC in the OCF stack is expected to be transport and connectivity abstraction layer agnostic.

Implementation of access control relies on a-priori definition of a set of access policies for the Resource. The policies may be stored by a local ACL or an Access Management Service (AMS) in form of Access Control Entries (ACE). Two types of access control mechanisms can be applied:

- Subject-based access control (SBAC), where each ACE will match a subject (e.g. identity of requestor) of the requesting entity against the subject included in the policy defined for Resource. Asserting the identity of the requestor requires an authentication process.
Role-based Access Control (RBAC), where each ACE will match a role identifier included in the policy for the Resource to a role identifier associated with the requestor.

If an OCF Server receives a batch request to an Atomic Measurement Resource containing only local references and there is an ACE matching the Atomic Measurement Resource which permits the request, then the corresponding requests to linked Resources are permitted by the OCF Server. The present paragraph shall apply to any Resource Type based on the Atomic Measurement Resource Type.

NOTE: The definition of an Atomic Measurement Resource prohibits direct access to the linked Resources. The nature of an Atomic Measurement also prohibits updating the "links" to add or remove Resources. Consequently, there is no risk of privilege escalation when using the ACE of an Atomic Measurement Resource to govern access to its linked Resources.

If an OCF Server receives a batch request to a Collection Resource containing only local references and there is an ACE matching the Collection Resource which permits the request, then the corresponding requests to linked Resources are permitted by the OCF Server. The present paragraph shall apply to any Resource Type based on the Collection Resource Type.

NOTE: This implies that the ACEs of the Collection Resource permit access to all the Collection's linked Resources via the batch OCF Interface, even if there are no ACEs permitting direct access to some or all the linked Resources. If not tightly governed, this could lead to privilege escalation. Restrictions on the use of Collection Resources have been provided in ISO/IEC 30118-1:2018 to mitigate the risk of privilege escalation. For example, ISO/IEC 30118-1:2018 prohibits updating "links" of a Collection Resource with the intent of obtaining access to the added Resource according to the ACEs of the Collection, when access to the Resource would have otherwise been denied.

In the OCF access control model, access to a Resource instance requires an associated access control policy. This means, each Device acting as Server, needs to have an ACE permitting access to each Resource it is protecting. This criterion can be satisfied for a Resource A if there is an ACE permitting batch requests to access Resource B containing a Link to Resource A, even if there are no ACEs permitting requests which access Resource A directly. Examples of the Resource Type for Resource B is the Atomic Measurement Resource Type and the Collection Resource Type. The lack of an ACE permitting access to a Resource, either directly or via a Link results in the Resource being inaccessible.

The ACE only applies if the ACE matches both the subject (i.e. OCF Client) and the requested Resource. There are multiple ways a subject could be matched, (1) DeviceID, (2) Role Identifier or (3) wildcard. The way in which the client connects to the server may be relevant context for making access control decisions. Wildcard matching on authenticated vs. unauthenticated and encrypted vs. unencrypted connection allows an access policy to be broadly applied to subject classes.

Example Wildcard Matching Policy:

```
"aclist2": {
  "subject": {"conntype": "anon-clear"},
  "resources":{
    "wc":":"*
  },
  "permission": 31
},

{"subject": {"conntype": "auth-crypt"},
  "resources":{
    "wc":":"*
  }
}
```

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
Details of the format for ACL are defined in clause 12. The ACL is composed of one or more ACEs. The ACL defines the access control policy for the Devices.

ACL Resource requires the same security protection as other sensitive Resources, when it comes to both storage and handling by SRM and PSI. Thus hardening of an underlying Platform (HW and SW) must be considered for protection of ACLs and as explained in clause 5.2.2 ACLs may have different scoping levels and thus hardening needs to be specially considered for each scoping level. For instance, a physical device may host multiple Device implementations and thus secure storage, usage and isolation of ACLs for different Servers on the same Device needs to be considered.

5.2.1 ACL Architecture

5.2.1.1 ACL Architecture General

The Server examines the Resource(s) requested by the client before processing the request. The access control resources (e.g. "/oic/sec/acl", "/oic/sec/acl2") are searched to find one or more ACE entries that match the requestor and the requested Resources. If a match is found, then permission and period constraints are applied. If more than one match is found, then the logical UNION of permissions is applied to the overlapping periods.

The server uses the connection context to determine whether the subject has authenticated or not and whether data confidentiality has been applied or not. Subject matching wildcard policies can match on each aspect. If the user has authenticated, then subject matching may happen at increased granularity based on role or device identity.

Each ACE contains the permission set that will be applied for a given Resource requestor. Permissions consist of a combination of CREATE, RETREIVE, UPDATE, DELETE and NOTIFY (CRUDN) actions. Requestors authenticate as a Device and optionally operating with one or more roles. Devices may acquire elevated access permissions when asserting a role. For example, an ADMINISTRATOR role might expose additional Resources and OCF Interfaces not normally accessible.

5.2.1.2 Use of local ACLs

Servers may host ACL Resources locally. Local ACLs allow greater autonomy in access control processing than remote ACL processing by an AMS.

The following use cases describe the operation of access control

Use Case 1: As depicted in Figure 4, Server Device hosts 4 Resources (R1, R2, R3 and R4). Client Device D1 requests access to Resource R1 hosted at Server Device 5. ACL[0] corresponds to Resource R1 and includes D1 as an authorized subject. Thus, Device D1 receives access to Resource R1 because the local ACL "/oic/sec/acl/0" matches the request.
Use Case 2: As depicted in Figure 5, Client Device D2 access is denied because no local ACL match is found for subject D2 pertaining Resource R2 and no AMS policy is found.

5.2.1.3 Use of AMS
AMS improves ACL policy management. However, they can become a central point of failure. Due to network latency overhead, ACL processing may be slower through an AMS.
AMS centralizes access control decisions, but Server Devices retain enforcement duties. The Server shall determine which ACL mechanism to use for which Resource set. The "/oic/sec/amacl" Resource is an ACL structure that specifies which Resources will use an AMS to resolve access decisions. The "/oic/sec/amacl" may be used in concert with local ACLs ("/oic/sec/acl").

The AMS is authenticated by referencing a credential issued to the device identifier contained in "/oic/sec/acl2.rowneruuid".

The Server Device may proactively open a connection to the AMS using the Device ID found in "/oic/sec/acl2.rowneruuid". Alternatively, the Server may reject the Resource access request with an error, ACCESS_DENIED_REQUIRES_SACL that instructs the requestor to obtain a suitable ACE policy using a SACL Resource "/oic/sec/sacl". The "/oic/sec/sacl" signature may be validated using the credential Resource associated with the "/oic/sec/acl2.rowneruuid".

The following use cases describe access control using the AMS:

Use Case 3: As depicted in Figure 6, Device D3 requests and receives access to Resource R3 with permission Perm1 because the "/oic/sec/amacl/0" matches a policy to consult the Access Manager Server AMS1 service.

![Figure 6 – Use case-3 showing AMS supported ACL](image)

Use Case 4: As depicted in Figure 7, Client Device D4 requests access to Resource R4 from Server Device 5, which fails to find a matching ACE and redirects the Client Device D4 to AMS1 by returning an error identifying AMS1 as a "/oic/sec/sacl" Resource issuer. Device D4 obtains Sacl1 signed by AMS1 and forwards the SACL to Server D5. D5 verifies the signature in the "/oic/sec/sacl" Resource and evaluates the ACE policy that grants Perm2 access.

ACE redirection may occur when D4 receives an error result with reason code indicating no match exists (i.e., ACCESS_DENIED_NO_ACE). D4 reads the "/oic/sec/acl2" Resource to find the "rowneruuid" which identifies the AMS and then submits a request to be provisioned, in this example the AMS chooses to supply a SACL Resource, however it may choose to re-provision the local ACL Resources "/oic/sec/acl" and "/oic/sec/acl2". The request is reissued subsequently.
D4 is presumed to have been introduced to the AMS as part of Device onboarding or through subsequent credential provisioning actions. If not, a Credential Management Service (CMS) can be consulted to provision needed credentials.

Figure 7 – Use case-4 showing dynamically obtained ACL from an AMS

5.2.2 Access Control Scoping Levels

**Group Level Access** - Group scope means applying AC to the group of Devices that are grouped for a specific context. Group Level Access means all group members have access to group data but non-group members must be granted explicit access. Group level access is implemented using Role Credentials and/or connection type.

**OCF Device Level Access** – OCF Device scope means applying AC to an individual Device, which may contain multiple Resources. Device level access implies accessibility extends to all Resources available to the Device identified by Device ID. Credentials used for AC mechanisms at Device are OCF Device-specific.

**OCF Resource Level Access** – OCF Resource level scope means applying AC to individual Resources. Resource access requires an ACL that specifies how the entity holding the Resource (Server) shall make a decision on allowing a requesting entity (Client) to access the Resource.

**Property Level Access** - Property level scope means applying AC only to an individual Property. Property level access control is only achieved by creating a Resource that contains a single Property.

Controlling access to static Resources where it is impractical to redesign the Resource, it may appropriate to introduce a collection Resource that references the child Resources having separate access permissions. An example is shown Figure 8, where an "oic.thing" Resource has two properties: Property-1 and Property-2 that would require different permissions.
Figure 8 – Example Resource definition with opaque Properties

Currently, OCF framework treats property level information as opaque; therefore, different permissions cannot be assigned as part of an ACL policy (e.g., read-only permission to Property-1 and write-only permission to Property-2). Thus, as shown in Figure 9, the “oic.thing” is split into two new Resource “oic.RsrcProp-1” and “oic.RsrcProp-2”. This way, Property level ACL can be achieved through use of Resource-level ACLs.

Figure 9 – Property Level Access Control
5.3 Onboarding Overview

5.3.1 Onboarding General

Before a Device becomes operational in an OCF environment and is able to interact with other Devices, it needs to be appropriately onboarded. The first step in onboarding a Device is to configure the ownership where the legitimate user that owns/purchases the Device uses an Onboarding tool (OBT) and using the OBT uses one of the Owner Transfer Methods (OTMs) to establish ownership. Once ownership is established, the OBT becomes the mechanism through which the Device can then be provisioned, at the end of which the Device becomes operational and is able to interact with other Devices in an OCF environment. An OBT shall be hosted on an OCF Device.

Figure 10 depicts Onboarding Overview.
This clause explains the onboarding and security provisioning process but leaves the provisioning of non-security aspects to other OCF documents. In the context of security, all Devices are required to be provisioned with minimal security configuration that allows the Device to securely interact/communicate with other Devices in an OCF environment. This minimal security configuration is defined as the Onboarded Device “Ready for Normal Operation” and is specified in 7.5.

Onboarding and provisioning implementations could utilize services defined outside this document, it is expected that in using other services, trust between the device being onboarded and the various tools is not transitive. This implies that the device being onboarded will individually authenticate the credentials of each and every tool used during the onboarding process.
process; that the tools not share credentials or imply a trust relationship where one has not been established.

5.3.2 Onboarding Steps

The flowchart in Figure 11 shows the typical steps that are involved during onboarding. Although onboarding may include a variety of non-security related steps, the diagram focus is mainly on the security related configuration to allow a new Device to function within an OCF environment. Onboarding typically begins with the Device becoming an Owned Device followed by configuring the Device for the environment that it will operate in. This would include setting information such as who can access the Device and what actions can be performed as well as what permissions the Device has for interacting with other Devices.
5.3.3 Establishing a Device Owner

The objective behind establishing Device ownership is to allow the legitimate user that owns/purchased the Device to assert itself as the owner and manager of the Device. This is done...
through the use of an OBT that includes the creation of an ownership context between the new Device and the OBT tool and asserts operational control and management of the Device. The OBT can be considered a logical entity hosted by tools/ Servers such as a network management console, a device management tool, a network-authoring tool, a network provisioning tool, a home gateway device, or a home automation controller. A physical device hosting the OBT will be subject to some security hardening requirements, thus preserving integrity and confidentiality of any credentials being stored. The tool/Server that establishes Device ownership is referred to as the OBT.

The OBT uses one of the OTMs specified in 7.3 to securely establish Device ownership. The term owner transfer is used since it is assumed that even for a new Device, the ownership is transferred from the manufacturer/provider of the Device to the buyer/legitimate user of the new Device.

An OTM establishes a new owner (the operator of OBT) that is authorized to manage the Device. Owner transfer establishes the following

– The DOTS provisions an Owner Credential (OC) to the creds Property in the "/oic/sec/cred" Resource of the Device. This OC allows the Device and DOTS to mutually authenticate during subsequent interactions. The OC associates the DOTS DeviceID with the rowneruuid property of the "/oic/sec/doxm" resource establishing it as the resource owner. The DOTS records the identity of Device as part of ownership transfer.
– The Device owner establishes trust in the Device through the OTM.
– Preparing the Device for provisioning by providing credentials that may be needed.

5.3.4 Provisioning for Normal Operation

Once the Device has the necessary information to initiate provisioning, the next step is to provision additional security configuration that allows the Device to become operational. This can include setting various parameters and may also involve multiple steps. Also provisioning of ACL’s for the various Resources hosted by the Server on the Device is done at this time. The provisioning step is not limited to this stage only. Device provisioning can happen at multiple stages in the Device's operational lifecycle. However specific security related provisioning of Resource and Property state would likely happen at this stage at the end of which, each Device reaches the Onboarded Device "Ready for Normal Operation" State. The "Ready for Normal Operation" State is expected to be consistent and well defined regardless of the specific OTM used or regardless of the variability in what gets provisioned. However individual OTM mechanisms and provisioning steps may specify additional configuration of Resources and Property states. The minimal mandatory configuration required for a Device to be in "Ready for Normal Operation" state is specified in 8.

5.3.5 Device Provisioning for OCF Cloud and Device Registration Overview

As mentioned in the start of clause 5, communication between a Device and OCF Cloud is subject to different criteria in comparison to Devices which are within a single local network. The Device is configured in order to connect to the OCF Cloud by a Mediator as specified in the "CoAPCloudConf" Resource clauses in OCF Cloud Specification. Provisioning includes the remote connectivity and local details such as URL where the OCF Cloud hosting environment can be found and the OCF Cloud verifiable Access Token.

5.3.6 OCF Compliance Management System

The OCF Compliance Management System (OCMS) is a service maintained by the OCF that provides Certification status and information for OCF Devices.

The OCMS shall provide a JSON-formatted Certified Product List (CPL), hosted at the URI: https://www.openconnectivity.org/certification/ocms-cpl.json
The OBT shall possess the Root Certificate needed to enable https connection to the URI https://www.openconnectivity.org/certification/ocms-cpl.json.

The OBT should periodically refresh its copy of the CPL via the URI https://www.openconnectivity.org/certification/ocms-cpl.json, as appropriate to OCF Security Domain owner policy requirements.

5.4 Provisioning

5.4.1 Provisioning General

In general, provisioning may include processes during manufacturing and distribution of the Device as well as processes after the Device has been brought into its intended environment (parts of onboarding process). In this document, security provisioning includes, processes after ownership transfer (even though some activities during ownership transfer and onboarding may lead to provisioning of some data in the Device) configuration of credentials for interacting with provisioning services, configuration of any security related Resources and credentials for dealing with any services that the Device need to contact later on.

Once the ownership transfer is complete, the Device needs to engage with the CMS and AMS to be provisioned with proper security credentials and parameters for regular operation. These parameters can include:

– Security credentials through a CMS, currently assumed to be deployed in the same OBT.
– Access control policies and ACLs through an AMS, currently assumed to be deployed in the same OBT, but may be part of AMS in future.

As mentioned, to accommodate a scalable and modular design, these functions are considered as services that in future could be deployed as separate servers. Currently, the deployment assumes that these services are all deployed as part of a OBT. Regardless of physical deployment scenario, the same security-hardening requirement) applies to any physical server that hosts the tools and security provisioning services discussed here.

Devices are aware of their security provisioning status. Self-awareness allows them to be proactive about provisioning or re-provisioning security Resources as needed to achieve the devices operational goals.

5.4.2 Provisioning other services

To be able to support the use of potentially different device management service hosts, each Device Secure Virtual Resource (SVR) has an associated Resource owner identified in the Resource's rowneruuid Property.

The DOTS shall update the rowneruuid Property of the "/oic/sec/doxm" and "/oic/sec/pstat" resources with the DOTS resource owner identifier.

The DOTS shall update the rowneruuid Property of the "/oic/sec/cred" resource with the CMS resource owner identifier.

The DOTS shall update the rowneruuid Property of the "/oic/sec/acl2" resource with the AMS resource owner identifier.

When these OCF Services are configured, the Device may proactively request provisioning and verify provisioning requests are authorized. The DOTS shall provision credentials that enable secure connections between OCF Services and the new Device. The DOTS may initiate client-directed provisioning by signaling the OCF Service. The DOTS may initiate server-directed provisioning by setting tm Property of the "/oic/sec/pstat" Resource.
5.4.3 Provisioning Credentials for Normal Operation

The "/oic/sec/cred" Resource supports multiple types of credentials including:

- Pairwise symmetric keys
- Group symmetric keys
- Certificates
- Raw asymmetric keys

The CMS shall securely provision credentials for Device-to-Device interactions using the CMS credential provisioned by the DOTS.

The following example describes how a Device updates a symmetric key credential involving a peer Device. The Device discovers the credential to be updated; for example, a secure connection attempt fails. The Device requests its CMS to supply the updated credential. The CMS returns an updated symmetric key credential. The CMS updates the corresponding symmetric key credential on the peer Device.

5.4.4 Role Assignment and Provisioning for Normal Operation

The Servers, receiving requests for Resources they host, need to verify the role identifier(s) asserted by the Client requesting the Resource and compare that role identifier(s) with the constraints described in the Server's ACLs. Thus, a Client Device may need to be provisioned with one or more role credentials.

Each Device holds the role information as a Property within the credential Resource.

Once provisioned, the Client can assert the role it is using as described in 10.4.2, if it has a certificate role credential.

All provisioned roles are used in ACL enforcement. When a server has multiple roles provisioned for a client, access to a Resource is granted if it would be granted under any of the roles.

5.4.5 ACL provisioning

ACL provisioning shall be performed over a secure connection between the AMS and its Devices. The AMS maintains an ACL policy for each Device it manages. The AMS shall provision the ACL policy by updating the Device's ACL Resources.

The AMS shall digitally sign an ACL as part of issuing a "/oic/sec/sacl" Resource if the Device supports the "/oic/sec/sacl" Resource. The public key used by the Device to verify the signature shall be provisioned by the CMS as needed. A "/oic/sec/cred" Resource with an asymmetric key type or signed asymmetric key type is used. The "PublicData" Property contains the AMS's public key.

5.5 Secure Resource Manager (SRM)

SRM plays a key role in the overall security operation. In short, SRM performs both management of SVR and access control for requests to access and manipulate Resources. SRM consists of 3 main functional elements:

- A Resource manager (RM): responsible for 1) Loading SVRs from persistent storage (using PSI) as needed. 2) Supplying the Policy Engine (PE) with Resources upon request. 3) Responding to requests for SVRs. While the SVRs are in SRM memory, the SVRs are in a format that is consistent with device-specific data store format. However, the RM will use JSON format to marshal SVR data structures before be passed to PSI for storage, or travel off-device.
- A Policy Engine (PE) that takes requests for access to SVRs and based on access control policies responds to the requests with either "ACCESS_GRANTED" or "ACCESS_DENIED". To make the access decisions, the PE consults the appropriate ACL and looks for best Access Control Entry (ACE) that can serve the request given the subject (Device or role) that was authenticated by DTLS.

- Persistent Storage Interface (PSI): PSI provides a set of APIs for the RM to manipulate files in its own memory and storage. The SRM design is modular such that it may be implemented in the Platform's secure execution environment; if available.

Figure 12 depicts OCF's SRM Architecture.

5.6 Credential Overview

Devices may use credentials to prove the identity and role(s) of the parties in bidirectional communication. Credentials can be symmetric or asymmetric. Each device stores secret and public parts of its own credentials where applicable, as well as credentials for other devices that have been provided by the DOTS or a CMS. These credentials are then used in the establishment of secure communication sessions (e.g. using DTLS) to validate the identities of the participating parties. Role credentials are used once an authenticated session is established, to assert one or more roles for a device.

Access Tokens are provided to an OCF Cloud once an authenticated session with an OCF Cloud is established, to verify the User ID with which the Device is to be associated.
6 Security for the Discovery Process

6.1 Preamble

The main function of a discovery mechanism is to provide Universal Resource Identifiers (URIs, called links) for the Resources hosted by the Server, complemented by attributes about those Resources and possible further link relations. (in accordance to clause 10 in ISO/IEC 30118-1:2018)

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 document 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 13.5)

Aside from the privacy and discoverability of Resources from ACL point of view, the discovery process itself needs to be secured. This document 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 secure discovery, any Resource that has an associated ACL2 will be listed in the response to "/oic/res" Resource if and only if the Client has permissions to perform at least one of the CRUDN operations (i.e. the bitwise OR of the CRUDN flags must be true).

For example, a Client with Device Id "d1" makes a RETRIEVE request on the "/door" Resource hosted on a Server with Device Id "d3" where d3 has the ACL2s:

```json
{
   "aclist2": [
      {
         "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
         "resources": ["href":"/door"],
         "permission": 2, // RETRIEVE
         "aceid": 1
      }
   ]
}
```
The ACL indicates that Client "d1" has RETRIEVE permissions on the Resource. Hence when device "d1" does a discovery on the "/oic/res" Resource of the Server "d3", the response will include the URI of the "/door" Resource metadata. Client "d2" will have access to both the Resources. ACE2 will prevent "d4" from update.

Discovery results delivered to d1 regarding d3’s "/oic/res" Resource from the secure interface:
"di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1",
}
]

Discovery results delivered to d2 regarding d3’s "/oic/res" Resource from the secure interface:

[
{
  "href": "/door",
  "rt": ["oic.r.door"],
  "if": ["oic.if.b", "oic.if.ll"],
  "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
},
{
  "href": "/door/lock",
  "rt": ["oic.r.lock"],
  "if": ["oic.if.b"],
  "type": ["application/json", "application/exi+xml"],
  "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
]

Discovery results delivered to d4 regarding d3’s "/oic/res" Resource from the secure interface:

[
{
  "href": "/door/lock",
  "rt": ["oic.r.lock"],
  "if": ["oic.if.b"],
  "type": ["application/json", "application/exi+xml"],
  "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
]

Discovery results delivered to any device regarding d3’s "/oic/res" Resource from the unsecure interface:

[
{
  "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1",
  "href": "/light",
  "rt": ["oic.r.light"],
  "if": ["oic.if.s"
}
]}
7 Security Provisioning

7.1 Device Identity

7.1.1 General Device Identity

Each Device, which is a logical device, is identified with a Device ID.

Devices shall be identified by a Device ID value that is established as part of device onboarding. The "/oic/sec/doxm" Resource specifies the Device ID format (e.g. "urn:uuid"). Device IDs shall be unique within the scope of operation of the corresponding OCF Security Domain, and should be universally unique. The DOTS shall ensure Device ID of the new Device is unique within the scope of the owner's OCF Security Domain. The DOTS shall verify the chosen new device identifier does not conflict with Device IDs previously introduced into the OCF Security Domain.

Devices maintain an association of Device ID and cryptographic credential using a "/oic/sec/cred" Resource. Devices regard the "/oic/sec/cred" Resource as authoritative when verifying authentication credentials of a peer device.

A Device maintains its Device ID in the "/oic/sec/doxm" Resource. It maintains a list of credentials, both its own and other Device credentials, in the "/oic/sec/cred" Resource. The device ID can be used to distinguish between a device's own credential, and credentials for other devices. Furthermore, the "/oic/sec/cred" Resource may contain multiple credentials for the device.

Device ID shall be:

- Unique
- Immutable
- Verifiable

When using manufacturer certificates, the certificate should bind the ID to the stored secret in the device as described later in this clause.

A physical Device, referred to as a Platform in OCF documents, may host multiple Devices. The Platform is identified by a Platform ID. The Platform ID shall be globally unique and inserted in the device in an integrity protected manner (e.g. inside secure storage or signed and verified).

An OCF Platform may have a secure execution environment, which shall be used to secure unique identifiers and secrets. If a Platform hosts multiple devices, some mechanism is needed to provide each Device with the appropriate and separate security.

7.1.2 Device Identity for Devices with UAID [Deprecated]

This clause is intentionally left blank.

7.2 Device Ownership

This is an informative clause. Devices are logical entities that are security endpoints that have an identity that is authenticable using cryptographic credentials. A Device is Unowned when it is first initialized. Establishing device ownership is a process by which the device asserts its identity to the DOTS and the DOTS provisions an owner identity. This exchange results in the device changing its ownership state, thereby preventing a different DOTS from asserting administrative control over the device.

The ownership transfer process starts with the OBT discovering a new device that is in Unowned state through examination of the "Owned" Property of the "/oic/sec/doxm" Resource of the new device. At the end of ownership transfer, the following is accomplished:
1) The DOTS shall establish a secure session with new device.
2) Optionally asserts any of the following:
   a) Proximity (using PIN) of the OBT to the Platform.
   b) Manufacturer’s certificate asserting Platform vendor, model and other Platform specific attributes.
3) Determines the device identifier.
4) Determines the device owner.
5) Specifies the device owner (e.g. Device ID of the OBT).
6) Provisions the device with owner’s credentials.
7) Sets the "Owned" state of the new device to TRUE.

NOTE A Device which connects to the OCF Cloud still retains the ownership established at onboarding with the DOTS.

7.3 Device Ownership Transfer Methods

7.3.1 OTM implementation requirements

This document provides specifications for several methods for ownership transfer. Implementation of each individual ownership transfer method is considered optional. However, each device shall implement at least one of the ownership transfer methods not including vendor specific methods.

All OTMs included in this document are considered optional. Each vendor is required to choose and implement at least one of the OTMs specified in this document. The OCF, does however, anticipate vendor-specific approaches will exist. Should the vendor wish to have interoperability between a vendor-specific OTM and OBTs from other vendors, the vendor must work directly with OBT vendors to ensure interoperability. Notwithstanding, standardization of OTMs is the preferred approach. In such cases, a set of guidelines is provided in 7.3.7 to help vendors in designing vendor-specific OTMs.

The "/oic/sec/doxm" Resource is extensible to accommodate vendor-defined owner transfer methods (OTM). The DOTS determines which OC is most appropriate to onboard the new Device. All OTMs shall represent the onboarding capabilities of the Device using the oxms Property of the "/oic/sec/doxm" Resource. The DOTS shall query the Device’s supported credential types using the credtypes Property of the "/oic/sec/cred" Resource. The DOTS and CMS shall provision credentials according to the credential types supported.

Figure 13 depicts new Device discovery sequence.
Figure 13 – Discover New Device Sequence

Table 1 – Discover New Device Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The OBT queries to see if the new device is not yet owned.</td>
</tr>
<tr>
<td>2</td>
<td>The new device returns the &quot;/oic/sec/doxm&quot; Resource containing ownership status and supported OTMs. It also contains a temporal device ID that may change subsequent to successful owner transfer. The device should supply a temporal ID to facilitate discovery as a guest device. Clause 7.3.9 provides security considerations regarding selecting an OTM.</td>
</tr>
</tbody>
</table>

Vendor-specific device OTMs shall adhere to the "/oic/sec/doxm" Resource Specification for OCs that results from vendor-specific device OTM. Vendor-specific OTM should include provisions for establishing trust in the new Device by the OBT an optionally establishing trust in the OBT by the new Device.

The new device may have to perform some initialization steps at the beginning of an OTM. For example, if the Random PIN Based OTM is initiated, the new device may generate a random PIN value. The OBT shall POST to the oxmsel property of "/oic/sec/doxm" the value corresponding to the OTM being used, before performing other OTM steps. This POST notifies the new device that ownership transfer is starting.

The end state of a vendor-specific OTM shall allow the new Device to authenticate to the OBT and the OBT to authenticate to the new device.

The DOTS may perform additional provisioning steps subsequent to owner transfer success leveraging the established OTM session.

After successful OTM, but before placing the newly-onboarded Device in RFNOP, the OBT shall remove all ACEs where the Subject is "anon-clear" or "auth-crypt", and the Resources array includes a SVR.
7.3.2 SharedKey Credential Calculation

The SharedKey credential is derived using a PRF that accepts the key_block value resulting from the DTLS handshake used for onboarding. The new Device and DOTS shall use the following calculation to ensure interoperability across vendor products:

\[
\text{SharedKey} = \text{PRF}(\text{Secret}, \text{Message})
\]

Where:

- \( \text{PRF} \) shall use TLS 1.2 PRF defined by IETF RFC 5246 clause 5.
- \( \text{Secret} \) is the key_block resulting from the DTLS handshake
  - See IETF RFC 5246 clause 6.3
  - The length of key_block depends on cipher suite.
    - (e.g. 96 bytes for TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, 40 bytes for TLS_PSK_WITH_AES_128_CCM_8)
- \( \text{Message} \) is a concatenation of the following:
  - DoxmType string for the current onboarding method (e.g. "oic.sec.doxm.jw")
  - See clause 13.2.4 for specific DoxmTypes
  - Owner ID is a UUID identifying the device owner identifier and the device that maintains SharedKey.
    - Use raw bytes as specified in IETF RFC 4122 clause 4.1.2
  - Device ID is new device's UUID Device ID
    - Use raw bytes as specified in IETF RFC 4122 clause 4.1.2
- SharedKey Length will be 32 octets.
  - If subsequent DTLS sessions use 128 bit encryption cipher suites the left most 16 octets will be used.
  - DTLS sessions using 256-bit encryption cipher suites will use all 32 octets.

7.3.3 Certificate Credential Generation

The Certificate Credential will be used by Devices for secure bidirectional communication. The certificates will be issued by a CMS or an external certificate authority (CA). This CA will be used to mutually establish the authenticity of the Device. The onboarding details for certificate generation will be specified in a later version of this document.

7.3.4 Just-Works OTM

7.3.4.1 Just-Works OTM General

Just-works OTM creates a symmetric key credential that is a pre-shared key used to establish a secure connection through which a device should be provisioned for use within the owner's OCF Security Domain. Provisioning additional credentials and Resources is a typical step following ownership establishment. The pre-shared key is called SharedKey.

The DOTS shall select the Just-works OTM and establish a DTLS session using a ciphersuite defined for the Just-works OTM.

The following OCF-defined vendor-specific ciphersuites are used for the Just-works OTM.

\[
\begin{align*}
\text{TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256,} \\
\text{TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256}
\end{align*}
\]

These are not registered in IANA, the ciphersuite values are assigned from the reserved area for private use (0xFF00 ~ 0xFFFF). The assigned values are 0xFF00 and 0xFF01, respectively.

Just Works OTM sequence is shown in Figure 14 and steps described in Table 2.
Perform Just-Works Owner Transfer Method

Execute Just Works Owner Transfer Method

Table 2 – A Just Works OTM Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT notifies the Device that it selected the &quot;Just Works&quot; method.</td>
</tr>
<tr>
<td>3 - 8</td>
<td>A DTLS session is established using anonymous Diffie-Hellman.\textsuperscript{a}</td>
</tr>
</tbody>
</table>

\textsuperscript{a} This method assumes the operator is aware of the potential for man-in-the-middle attack and has taken precautions to perform the method in a clean-room network.

7.3.4.2 Security Considerations

Anonymous Diffie-Hellman key agreement is subject to a man-in-the-middle attacker. Use of this method presumes that both the OBT and the new device perform the "just-works" method assumes onboarding happens in a relatively safe environment absent of an attack device.

This method doesn’t have a trustworthy way to prove the device ID asserted is reliably bound to the device.

The new device should use a temporal device ID prior to transitioning to an owned device while it is considered a guest device to prevent privacy sensitive tracking. The device asserts a non-temporal device ID that could differ from the temporal value during the secure session in which
owner transfer exchange takes place. The OBT will verify the asserted Device ID does not conflict with a Device ID already in use. If it is already in use the existing credentials are used to establish a secure session.

An un-owned Device that also has established device credentials might be an indication of a corrupted or compromised device.

### 7.3.5 Random PIN Based OTM

#### 7.3.5.1 Random PIN OTM General

The Random PIN method establishes physical proximity between the new device and the OBT can prevent man-in-the-middle attacks. The Device generates a random number that is communicated to the OBT over an out-of-band channel. The definition of out-of-band communications channel is outside the scope of the definition of device OTMs. The OBT and new Device use the PIN in a key exchange as evidence that someone authorized the transfer of ownership by having physical access to the new Device via the out-of-band-channel.

#### 7.3.5.2 Random PIN Owner Transfer Sequence

Random PIN-based OTM sequence is shown in Figure 15 and steps described in Table 3.

---

**Perform Random PIN Device Owner Transfer Method**

1. POST /oic/sec/doxm {"oxmSel":1,...}
2. RSP 2.04

**Execute Manufacturer Certificate Owner Transfer Method**

- OBT selects the oic.sec.oxm.rdp owner transfer method and executes it.

3. ClientHello(TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256)
4. HelloVerifyRequest(cookie)
5. ClientHello(TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256,cookie)

- ServerHello(TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256)
6. ServerKeyExchange(EC DH PublicKey + ECC Curve Param)
    - ServerHelloDone()
7. ClientKeyExchange(EC DH PublicKey)
    - ChangeCipherSpec + Finish
8. ChangeCipherSpec + Finish

---

**Figure 15 – Random PIN-based OTM**

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
Table 3 – Random PIN-based OTM Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT notifies the Device that it selected the “Random PIN” method.</td>
</tr>
<tr>
<td>3 - 8</td>
<td>A DTLS session is established using PSK-based Diffie-Hellman ciphersuite. The PIN is supplied as the PSK parameter. The PIN is randomly generated by the new device then communicated via an out-of-band channel that establishes proximal context between the new device and the OBT. The security principle is the attack device will be unable to intercept the PIN due to a lack of proximity.</td>
</tr>
</tbody>
</table>

The random PIN-based device OTM uses a pseudo-random function (PBKDF2) defined by IETF RFC 2898 and a PIN exchanged via an out-of-band method to generate a pre-shared key. The PIN-authenticated pre-shared key (PPSK) is supplied to TLS ciphersuites that accept a PSK.

\[
PPSK = PBKDF2(PR; PIN, Device ID, c, dkLen)
\]

The PBKDF2 function has the following parameters:

- **PR** – Uses the TLS 1.2 PRF defined by IETF RFC 5246.
- **PIN** – Obtain via out-of-band channel.
- **Device ID** – UUID of the new device.

Use raw bytes as specified in IETF RFC 4122 clause 4.1.2

- **c** – Iteration count initialized to 1000
- **dkLen** – Desired length of the derived PSK in octets.

### 7.3.5.3 Security Considerations

Security of the Random PIN mechanism depends on the entropy of the PIN. Using a PIN with insufficient entropy may allow a man-in-the-middle attack to recover any long-term credentials provisioned as a part of onboarding. In particular, learning provisioned symmetric key credentials, allows an attacker to masquerade as the onboarded device.

It is recommended that the entropy of the PIN be enough to withstand an online brute-force attack, 40 bits or more. For example, a 12-digit numeric PIN, or an 8-character alphanumeric (0-9a-z), or a 7-character case-sensitive alphanumeric PIN (0-9a-zA-Z). A man-in-the-middle attack (MITM) is when the attacker is active on the network and can intercept and modify messages between the OBT and device. In the MITM attack, the attacker must recover the PIN from the key exchange messages in "real time", i.e., before the peer's time out and abort the connection attempt. Having recovered the PIN, he can complete the authentication step of key exchange. The guidance given here calls for a minimum of 40 bits of entropy, however, the assurance this provides depends on the resources available to the attacker. Given the parallelizable nature of a brute force guessing attack, the attack enjoys a linear speedup as more cores/threads are added. A more conservative amount of entropy would be 64 bits. Since the Random PIN OTM requires using a DTLS ciphersuite that includes an ECDHE key exchange, the security of the Random PIN OTM is always at least equivalent to the security of the JustWorks OTM.

The Random PIN OTM also has an option to use PBKDF2 to derive key material from the PIN. The rationale is to increase the cost of a brute force attack, by increasing the cost of each guess in the attack by a tunable amount (the number of PBKDF2 iterations). In theory, this is an effective way to reduce the entropy requirement of the PIN. Unfortunately, it is difficult to quantify the reduction, since an X-fold increase in time spent by the honest peers does not directly translate to an X-fold increase in time by the attacker. This asymmetry is because the attacker may use specialized implementations and hardware not available to honest peers. For this...
reason, when deciding how much entropy to use for a PIN, it is recommended that implementers assume PBKDF2 provides no security, and ensure the PIN has sufficient entropy.

The Random PIN device OTM security depends on an assumption that a secure out-of-band method for communicating a randomly generated PIN from the new device to the OBT exists. If the OOB channel leaks some or the entire PIN to an attacker, this reduces the entropy of the PIN, and the attacks described above apply. The out-of-band mechanism should be chosen such that it requires proximity between the OBT and the new device. The attacker is assumed to not have compromised the out-of-band-channel. As an example OOB channel, the device may display a PIN to be entered into the OBT software. Another example is for the device to encode the PIN as a 2D barcode and display it for a camera on the OBT device to capture and decode.

7.3.6 Manufacturer Certificate Based OTM

7.3.6.1 Manufacturer Certificate Based OTM General

The manufacturer certificate-based OTM shall use a certificate embedded into the device by the manufacturer and may use a signed OBT, which determines the Trust Anchor between the device and the OBT.

Manufacturer embedded certificates do not necessarily need to chain to an OCF Root CA trust anchor.

For some environments, policies or administrators, additional information about device characteristics may be sought. This list of additional attestations that OCF may or may not have tested (understanding that some attestations are incapable of testing or for which testing may be infeasible or economically unviable) can be found under the OCF Security Claims x509.v3 extension described in 9.4.2.2.6.

When utilizing certificate-based ownership transfer, devices shall utilize asymmetric keys with certificate data to authenticate their identities with the OBT in the process of bringing a new device into operation on an OCF Security Domain. The onboarding process involves several discrete steps:

1) Pre-on-board conditions

   a) The credential element of the Device’s credential Resource ("/oic/sec/cred") containing the manufacturer certificate shall be identified by the properties:

      i) the subject Property shall refer to the Device

      ii) the credusage Property shall contain the string "oic.sec.cred.mfgcert" to indicate that the credential contains a manufacturer certificate

   b) The manufacturer certificate chain shall be contained in the identified credential element’s publicdata Property.

   c) The device shall contain a unique and immutable ECC asymmetric key pair.

   d) If the device requires authentication of the OBT as part of ownership transfer, it is presumed that the OBT has been registered and has obtained a certificate for its unique and immutable ECC asymmetric key pair signed by the predetermined Trust Anchor.

   e) User has configured the OBT app with network access info and account info (if any).

2) The OBT shall authenticate the Device using ECDSA to verify the signature. Additionally, the Device may authenticate the OBT to verify the OBT signature.

3) If authentication fails, the Device shall indicate the reason for failure and return to the Ready for OTM state. If authentication succeeds, the device and OBT shall establish an encrypted link in accordance with the negotiated cipher suite.
7.3.6.2 Certificate Profiles

See 9.4.2 for details.

7.3.6.3 Certificate Owner Transfer Sequence Security Considerations

In order for full, mutual authentication to occur between the device and the OBT, both the device and OBT must be able to trace back to a mutual Trust Anchor or Certificate Authority. This implies that OCF may need to obtain services from a Certificate Authority (e.g. Symantec, Verisign, etc.) to provide ultimate Trust Anchors from which all subsequent OCF Trust Anchors are derived.

The OBT shall authenticate the device during onboarding. However, the device is not required to authenticate the OBT due to potential resource constraints on the device.

In the case where the Device does NOT authenticate the OBT software, there is the possibility of malicious OBT software unwittingly deployed by users, or maliciously deployed by an adversary, which can compromise OCF Security Domain access credentials and/or personal information.

7.3.6.4 Manufacturer Certificate Based OTM Sequence

Random PIN-based OTM sequence is shown in Figure 16 and steps described in Table 4.
Table 4 – Manufacturer Certificate Based OTM Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT notifies the Device that it selected the &quot;Manufacturer Certificate&quot; method.</td>
</tr>
<tr>
<td>3 - 8</td>
<td>A DTLS session is established using the device's manufacturer certificate and optional OBT certificate. The device's manufacturer certificate may contain data.</td>
</tr>
</tbody>
</table>
7.3.6.5 Security Considerations

The manufacturer certificate private key is embedded in the Platform with a sufficient degree of assurance that the private key cannot be compromised.

The Platform manufacturer issues the manufacturer certificate and attests the private key protection mechanism.

7.3.7 Vendor Specific OTMs

7.3.7.1 Vendor Specific OTM General

The OCF anticipates situations where a vendor will need to implement an OTM that accommodates manufacturing or Device constraints. The Device OTM resource is extensible for this purpose. Vendor-specific OTMs must adhere to a set of conventions that all OTMs follow.

- The OBT must determine which credential types are supported by the Device. This is accomplished by querying the Device’s "/oic/sec/doxm" Resource to identify supported credential types.
- The OBT provisions the Device with OC(s).
- The OBT supplies the Device ID and credentials for subsequent access to the OBT.
- The OBT will supply second carrier settings sufficient for accessing the owner’s OCF Security Domain subsequent to ownership establishment.
- The OBT may perform additional provisioning steps but must not invalidate provisioning tasks to be performed by a security service.

7.3.7.2 Vendor-specific Owner Transfer Sequence Example

Vendor-specific OTM sequence example is shown in Figure 17 and steps described in Table 5.

**Figure 17 – Vendor-specific Owner Transfer Sequence**
Table 5 – Vendor-specific Owner Transfer Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT selects a vendor-specific OTM.</td>
</tr>
<tr>
<td>3</td>
<td>The vendor-specific OTM is applied</td>
</tr>
</tbody>
</table>

7.3.7.3 Security Considerations
The vendor is responsible for considering security threats and mitigation strategies.

7.3.8 Establishing Owner Credentials
Once the OBT and the new Device have authenticated and established an encrypted connection using one of the defined OTM methods.

Owner credentials may consist of certificates signed by the OBT or other authority, OCF Security Domain access information, provisioning functions, shared keys, or Kerberos tickets.

The OBT might then provision the new Device with additional credentials for Device management and Device-to-Device communications. These credentials may consist of certificates with signatures, UAID based on the Device public key, PSK, etc.

The steps for establishing Device’s owner credentials (OC) are:

1) The OBT shall establish the Device ID and Device owner uuid - Figure 18 and Table 6
2) The OBT then establishes Device’s OC - Figure 19 and Table 7. This can be either:
   a) Symmetric credential - Figure 20 and Table 8.
   b) Asymmetric credential - Figure 21 and Table 9.
3) Configure Device services - Figure 22 and Table 10.
4) Configure Device for peer to peer interaction - Figure 23 and Table 11.
Table 6 – Establish Device Identity Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT obtains the doxm properties again, using the secure session. It verifies that these properties match those retrieved before the authenticated connection. A mismatch in parameter values is treated as an authentication error.</td>
</tr>
<tr>
<td>3, 4</td>
<td>The OBT queries to determine if the Device is operationally ready to transfer Device ownership.</td>
</tr>
</tbody>
</table>
The OBT asserts that it will follow the Client provisioning convention.

The OBT asserts itself as the owner of the new Device by setting the Device ID to its ID.

The OBT obtains doxm properties again, this time Device returns new Device persistent UUID.

**Establish Owner Credentials Sequence**

**Establish Owner Credentials**

Discover which credential types are supported by the new device.

1. GET /oic/sec/doxm
2. RSP {includes supported credential types bitmask}
3. Select pair-wise symmetric key credential type.

**See Figure 20 - Symmetric Owner Credential Provisioning Sequence**

4. Select authentication certificate credential type.

**See Figure 21 - Asymmetric Owner Credential Provisioning Sequence**

**Figure 19 – Owner Credential Selection Provisioning Sequence**

**Table 7 – Owner Credential Selection Details**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT obtains the doxm properties to check ownership transfer mechanism supported on the new Device.</td>
</tr>
<tr>
<td>3, 4</td>
<td>The OBT uses selected credential type for ownership provisioning.</td>
</tr>
</tbody>
</table>
Table 8 – Symmetric Owner Credential Assignment Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT uses a pseudo-random-function (PRF), the master secret resulting from the DTLS handshake, and other information to generate a symmetric key credential resource Property - SharedKey.</td>
</tr>
<tr>
<td>3</td>
<td>The OBT creates a credential resource Property set based on SharedKey and then sends the resource Property set to the new Device with empty &quot;privatedata&quot; Property value.</td>
</tr>
<tr>
<td>4, 5</td>
<td>The new Device locally generates the SharedKey and updates it to the &quot;privatedata&quot; Property of the credential resource Property set.</td>
</tr>
<tr>
<td>6</td>
<td>The new Device sends a success message.</td>
</tr>
<tr>
<td>7</td>
<td>The onboarding service creates a subjects resource for the new device (e.g./A71C3xxx-...)</td>
</tr>
<tr>
<td>8</td>
<td>The onboarding service provisions its own &quot;/oic/sec/cred&quot; resource with the owner credential. Credential type is SYMMETRIC KEY.</td>
</tr>
</tbody>
</table>
| 9   | (optional) The onboarding service provisions its own "/oic/sec/cred" resource with the owner credential for...
In particular, if the OBT selects symmetric owner credentials:

- The OBT shall generate a Shared Key using the SharedKey Credential Calculation method described in 7.3.2.
- The OBT shall send an empty key to the new Device’s "/oic/sec/cred" Resource, identified as a symmetric pair-wise key.
- Upon receipt of the OBT’s symmetric owner credential, the new Device shall independently generate the Shared Key using the SharedKey Credential Calculation method described in 7.3.2 and store it with the owner credential.
- The new Device shall use the Shared Key owner credential(s) stored via the "/oic/sec/cred" Resource to authenticate the owner during subsequent connections.

**Figure 21 – Asymmetric Owner Credential Provisioning Sequence**

**Table 9 – Asymmetric Owner Credential Assignment Details**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>The OBT creates an asymmetric type credential</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>The new Device creates an asymmetric key pair.</td>
</tr>
<tr>
<td>4, 5</td>
<td>The OBT reads the new Device's asymmetric type credential Resource Property set generated at step 25. It may be used subsequently to authenticate the new Device.</td>
</tr>
</tbody>
</table>

If certificate owner credential type is selected by the OBT:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-8</td>
<td>The steps for creating an asymmetric credential type are performed. In addition, the OBT instantiates a newly-created certificate (or certificate chain) on the new Device.</td>
</tr>
<tr>
<td>9</td>
<td>The onboarding service creates a subjects resource for the new device (e.g./A71C3xxx-...)</td>
</tr>
<tr>
<td>10</td>
<td>The onboarding service provisions its &quot;/oic/svc/dots/subjects/A71C3xxx-cred&quot; resource with the owner credential. Credential type is PUBLIC KEY.</td>
</tr>
<tr>
<td>11</td>
<td>(optional) The onboarding service provisions its own &quot;/oic/sec/cred resource&quot; with the owner credential for new device. Credential type is PUBLIC KEY.</td>
</tr>
<tr>
<td>12</td>
<td>(optional) The onboarding service provisions its own &quot;/oic/sec/cred&quot; resource with the owner credential for new device. Credential type is CERTIFICATE.</td>
</tr>
</tbody>
</table>

If the OBT selects asymmetric owner credentials:
- The OBT shall add its public key to the new Device's "/oic/sec/cred" Resource, identified as an Asymmetric Encryption Key.
- The OBT shall query the "/oic/sec/cred" Resource from the new Device, supplying the new Device's UUID via the SubjectID query parameter. In response, the new Device shall return the public Asymmetric Encryption Key, which the OBT shall retain for future owner authentication of the new Device.

If the OBT selects certificate owner credentials:
- The OBT shall create a certificate or certificate chain with the leaf certificate containing the public key returned by the new Device, signed by a mutually-trusted CA, and complying with the Certificate Credential Generation requirements defined in 7.3.3.
- The OBT shall add the newly-created certificate chain to the "/oic/sec/cred" Resource, identified as an Asymmetric Signing Key with Certificate.
Configure Device Services

Table 10 – Configure Device Services Detail

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 8</td>
<td>The OBT assigns rowneruuid for different SVRs.</td>
</tr>
<tr>
<td>9 - 10</td>
<td>Provision the new Device with credentials for CMS</td>
</tr>
<tr>
<td>11 - 12</td>
<td>Provision the new Device with credentials for AMS</td>
</tr>
<tr>
<td>13 - 14</td>
<td>Update the &quot;oic.sec.doxm.owned&quot; to TRUE. Device is ready to move to provision and RFPRO state.</td>
</tr>
</tbody>
</table>
Figure 23 – Provision New Device for Peer to Peer Interaction Sequence

Table 11 – Provision New Device for Peer to Peer Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 4</td>
<td>The OBT set the Devices in the ready for provisioning status by setting &quot;oic.sec.pstat.dos&quot; to 2.</td>
</tr>
<tr>
<td>5 - 8</td>
<td>The OBT provision the Device with peer credentials</td>
</tr>
<tr>
<td>9 - 12</td>
<td>The OBT provision the Device with access control entities for peer Devices.</td>
</tr>
<tr>
<td>13 - 16</td>
<td>Enable Device to RFNOP state by setting &quot;oic.sec.pstat.dos&quot; to 3.</td>
</tr>
</tbody>
</table>
7.3.9 Security considerations regarding selecting an Ownership Transfer Method

An OBT and/or OBT's operator might have strict requirements for the list of OTMs that are acceptable when transferring ownership of a new Device. Some of the factors to be considered when determining those requirements are:

- The security considerations described for each of the OTMs
- The probability that a man-in-the-middle attacker might be present in the environment used to perform the ownership transfer

For example, the operator of an OBT might require that all of the Devices being onboarded support either the Random PIN or the Manufacturer Certificate OTM.

When such a local OTM policy exists, the OBT should try to use just the OTMs that are acceptable according to that policy, regardless of the doxm contents obtained during step 1 from the sequence diagram above (GET "/oic/sec/doxm"). If step 1 is performed over an unauthenticated and/or unencrypted connection between the OBT and the Device, the contents of the response to the GET request might have been tampered by a man-in-the-middle attacker. For example, the list of OTMs supported by the new Device might have been altered by the attacker.

Also, a man-in-the-middle attacker can force the DTLS session between the OBT and the new Device to fail. In such cases, the OBT has no way of determining if the session failed because the new Device doesn’t support the OTM selected by the OBT, or because a man-in-the-middle injected such a failure into the communication between the OBT and the new Device.

The current version of this document leaves the design and user experience related to the OTM policy as OBT implementation details.

7.3.10 Security Profile Assignment

OCF Devices may have been evaluated according to an OCF Security Profile. Evaluation results could be accessed from a manufacturer's certificate, OCF web server or other public repository. The DOTS reviews evaluation results to determine which OCF Security Profiles the OCF Device is authorized to possess and configures the Device with the subset of evaluated security profiles best suited for the OCF Security Domain owner's intended segmentation strategy.

The OCF Device vendor shall set a manufacturer default value for the "supportedprofiles" Property of the "/oic/sec/sp" Resource to match those approved by OCF’s testing and certification process. The "currentprofile" Property of the "/oic/sec/sp" Resource shall be set to one of the values contained in the "supportedprofiles". The manufacturer default value shall be re-asserted when the Device transitions to RESET Device State.

The OCF Device shall only allow the "/oic/sec/sp" Resource to be updated when the Device is in one of the following Device States: RFOTM, RFPRO, SRESET and may not allow any update as directed by a Security Profile.

The DOTS may update the "supportedprofiles" Property of the "/oic/sec/sp" Resource with a subset of the OCF Security Profiles values the Device achieved as part of OCF Conformance testing. The DOTS may locate conformance results by inspecting manufacturer certificates supplied with the OCF Device by selecting the "credusage" Property of the "/oic/sec/cred" Resource having the value of "oic.sec.cred.mfgcert". The DOTS may further locate conformance results by visiting a well-known OCF web site URI corresponding to the ocfCPLAttributes extension fields (clause 9.4.2.2.7). The DOTS may select a subset of Security Profiles (from those evaluated by OCF conformance testing) based on a local policy.

As part of onboarding (while the OTM session is active) the DOTS should configure ACE entries to allow DOTS access subsequent to onboarding.
The DOTS should update the "currentprofile" Property of the "/oic/sec/sp" Resource with the value that most correctly depicts the OCF Security Domain owner's intended Device deployment strategy.

The CMS may issue role credentials using the Security Profile value (e.g. the "sp-blue-v0 OID") to indicate the OCF Security Domain owner's intention to segment the OCF Security Domain according to a Security Profile. The CMS retrieves the supportedprofiles Property of the "/oic/sec/sp" Resource to select role names corroborated with the Device's supported Security Profiles when issuing role credentials.

If the CMS issues role credentials based on a Security Profile, the AMS supplies access control entries that include the role designation(s).

7.4 Provisioning
7.4.1 Provisioning Flows
7.4.1.1 Provisioning Flows General

As part of onboarding a new Device a secure channel is formed between the new Device and the OBT. Subsequent to the Device ownership status being changed to "owned", there is an opportunity to begin provisioning. The OBT decides how the new Device will be managed going forward and provisions the support services that should be subsequently used to complete Device provisioning and on-going Device management.

The Device employs a Server-directed or Client-directed provisioning strategy. The "/oic/sec/pstat" Resource identifies the provisioning strategy and current provisioning status. The provisioning service should determine which provisioning strategy is most appropriate for the OCF Security Domain. See 13.8 for additional detail.

7.4.1.2 Client-directed Provisioning

Client-directed provisioning relies on a provisioning service that identifies Servers in need of provisioning then performs all necessary provisioning duties.

An example of Client-directed provisioning is shown in Figure 24 and steps described in Table 12.
Figure 24 – Example of Client-directed provisioning

Table 12 – Steps describing Client-directed provisioning

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Discover Devices that are owned and support Client-directed provisioning.</td>
</tr>
<tr>
<td>2</td>
<td>The &quot;/oic/sec/doxmt&quot; Resource identifies the Device and its owned status.</td>
</tr>
<tr>
<td>3</td>
<td>Provisioning Tool (PT) obtains the new Device’s provisioning status found in &quot;/oic/sec/pstat&quot; Resource.</td>
</tr>
<tr>
<td>4</td>
<td>The pstat Resource describes the types of provisioning modes supported and which is currently configured. A Device manufacturer should set a default current operational mode (om). If the Om isn’t configured for Client-directed provisioning, its om value can be changed.</td>
</tr>
<tr>
<td>5 - 6</td>
<td>Change Device state to Ready-for-Provisioning.</td>
</tr>
<tr>
<td>7 - 8</td>
<td>PT instantiates the &quot;/oic/sec/cred&quot; Resource. It contains credentials for the provisioned services and other Devices</td>
</tr>
<tr>
<td>9 - 10</td>
<td>PT instantiates &quot;/oic/sec/acl&quot; Resources.</td>
</tr>
<tr>
<td>11</td>
<td>The new Device provisioning status mode is updated to reflect that ACLs have been configured. (Ready-for-Normal-Operation state)</td>
</tr>
<tr>
<td>12</td>
<td>The secure session is closed.</td>
</tr>
</tbody>
</table>
7.4.1.3 Server-directed Provisioning

Server-directed provisioning relies on the Server (i.e. new Device) for directing much of the provisioning work. As part of the onboarding process the support services used by the Server to seek additional provisioning are provisioned. The new Device uses a self-directed, state-driven approach to analyse current provisioning state, and tries to drive toward target state. This example assumes a single support service is used to provision the new Device.

An example of Client-directed provisioning is shown in Figure 25 and steps described in Table 13.

![Diagram](image)

**Figure 25 – Example of Server-directed provisioning using a single provisioning service**

**Table 13 – Steps for Server-directed provisioning using a single provisioning service**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The new Device verifies it is owned.</td>
</tr>
<tr>
<td>2</td>
<td>The new Device verifies it is in self-provisioning mode.</td>
</tr>
<tr>
<td>3</td>
<td>The new Device verifies its target provisioning state is fully provisioned.</td>
</tr>
<tr>
<td>4</td>
<td>The new Device verifies its current provisioning state requires provisioning.</td>
</tr>
<tr>
<td>5</td>
<td>The new Device initiates a secure session with the provisioning tool using the &quot;/oic/sec/doxm&quot;. DevOwner value to open a TLS connection using SharedKey.</td>
</tr>
<tr>
<td>6 - 9</td>
<td>The new Devices gets the &quot;/oic/sec/cred&quot; Resources. It contains credentials for the provisioned services and</td>
</tr>
</tbody>
</table>
7.4.1.4 Server-directed Provisioning Involving Multiple Support Services

A Server-directed provisioning flow, involving multiple support services distributes the provisioning work across multiple support services. Employing multiple support services is an effective way to distribute provisioning workload or to deploy specialized support. The example in Figure 26 demonstrates using a provisioning tool to configure two support services, a CMS and an AMS. Steps for the example are described in Table 14.
Table 14 – Steps for Server-directed provisioning involving multiple support services

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The new Device verifies it is owned.</td>
</tr>
<tr>
<td>2</td>
<td>The new Device verifies it is in self-provisioning mode.</td>
</tr>
<tr>
<td>3</td>
<td>The new Device initiates a secure session with the provisioning tool using the &quot;/oic/sec/doxm&quot;. DevOwner value to open a TLS connection using SharedKey.</td>
</tr>
<tr>
<td>4-5</td>
<td>The new Device gets credentials Resource for the provisioned services and other Devices</td>
</tr>
<tr>
<td>6</td>
<td>The new Device closes the DTLS session with the provisioning tool.</td>
</tr>
<tr>
<td>7</td>
<td>The new Device finds the CMS from the &quot;/oic/sec/cred&quot; Resource, rowneruuid Property and opens a DTLS connection. The new device finds the credential to use from the &quot;/oic/sec/cred&quot; Resource.</td>
</tr>
<tr>
<td>8-9</td>
<td>The new Device requests additional credentials that are needed for interaction with other devices.</td>
</tr>
<tr>
<td>10</td>
<td>The DTLS connection is closed.</td>
</tr>
<tr>
<td>11</td>
<td>The new Device finds the ACL provisioning and management service from the &quot;/oic/sec/acl2&quot; Resource, rowneruuid Property and opens a DTLS connection. The new device finds the ACL to use from the &quot;/oic/sec/acl2&quot; Resource.</td>
</tr>
<tr>
<td>12-13</td>
<td>The new Device gets ACL Resources that it will use to enforce access to local Resources.</td>
</tr>
<tr>
<td>14-15</td>
<td>The new Device should get SACL Resources immediately or in response to a subsequent Device Resource request.</td>
</tr>
<tr>
<td>16-17</td>
<td>The new Device should also get a list of Resources that should consult an Access Manager for making the access control decision.</td>
</tr>
<tr>
<td>18</td>
<td>The DTLS connection is closed.</td>
</tr>
</tbody>
</table>

7.5 Device Provisioning for OCF Cloud

7.5.1 Cloud Provisioning General

The Device that connects to the OCF Cloud shall support the "oic.r.coapcloudconf" Resource on Device and following SVRs on the OCF Cloud: "/oic/sec/account", "/oic/sec/session", "/oic/sec/tokenrefresh".

The OCF Cloud is expected to use a secure mechanism for associating a Mediator with an OCF Cloud User. The choice of mechanism is up to the OCF Cloud. Example, mechanisms include HTTP authentication (with username and password) or OAuth 2.0 (using an Authorization Server which could be operated by the OCF Cloud provider or a third party). OCF Cloud is expected to ensure that the suitable authentication mechanism is used to authenticate the OCF Cloud User.

7.5.2 Device Provisioning by Mediator

The Mediator and the Device shall use the secure session to provision the Device to connect with the OCF Cloud.

The Mediator obtains an Access Token from the OCF Cloud as described in OCF Cloud Specification. This Access Token is then used by the Device for registering with the OCF Cloud.
as described in 10.5. The OCF Cloud maintains a map where Access Token and Mediator provided Device ID are stored. At the time of Device Registration OCF Cloud validates the Access Token and associates the TLS session with corresponding Device ID.

The Mediator provisions the Device, as described in OCF Cloud Specification. The Mediator provisions OCF Cloud URI to the "cis" Property of "oic.r.coapcloudconf" Resource, OCF Cloud UUID to the "sid" Property of "oic.r.coapcloudconf" Resource and per-device Access Token to the "at" Property of "oic.r.coapcloudconf" Resource on Device. Provisioned "at" is to be treated by Device as an Access Token with "Bearer" token type as defined in IETF RFC 6750.

For the purposes of access control, the Device shall identify the OCF Cloud using the OCF Cloud UUID in the Common Name field of the End-Entity certificate used to authenticate the OCF Cloud.

AMS should configure the ACE2 entries on a Device so that the Mediator(s) is the only Device(s) with UPDATE permission for the "oic.r.coapcloudconf" Resource.

The AMS should configure the ACE2 entries on the Device to allow request from the OCF Cloud. By request from the Mediator, the AMS removes old ACL2 entries with previous OCF Cloud UUID. This request happens before "oic.r.coapcloudconf" is configured by the Mediator for the new OCF Cloud. The Mediator also requests AMS to set the OCF Cloud UUID as the "subject" Property for the new ACL2 entries. AMS may use "sid" Property of "oic.r.coapcloudconf" Resource as the current OCF Cloud UUID. AMS could either provision a wildcard entry for the OCF Cloud or provision an entry listing each Resource published on the Device.

If OCF Cloud provides "redirecturi" Value as response during Device Registration, the redirected to OCF Cloud is assumed to have the same OCF Cloud UUID and to use the same trust anchor. Otherwise, presented OCF Cloud UUID wouldn't match the provisioned ACL2 entries.

The Mediator should provision the "oic.r.coapcloudconf" Resource with the Properties in Table 15. These details once provisioned are used by the Device to perform Device Registration to the OCF Cloud. After the initial registration, the Device should use updated values received from the OCF Cloud instead. If OCF Cloud User wants the Device to re-register with the OCF Cloud, they can use the Mediator to re-provision the "oic.r.coapcloudconf" Resource with the new values.

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

### Table 15 – Mapping of Properties of the "oic.r.account" and "oic.r.coapcloudconf" Resources

8 Device Onboarding State Definitions

8.1 Device Onboarding General

As explained in 5.3, the process of onboarding completes after the ownership of the Device has been transferred and the Device has been provisioned with relevant configuration/services as
explained in 5.4. The Figure 27 shows the various states a Device can be in during the Device lifecycle.

The /pstat.dos.s Property is RW by the /oic/sec/pstat resource owner (e.g. "doxs" service) so that the resource owner can remotely update the Device state. When the Device is in RFNOP or RFPRO, ACLs can be used to allow remote control of Device state by other Devices. When the Device state is SRESET the Device OC may be the only indication of authorization to access the Device. The Device owner may perform low-level consistency checks and re-provisioning to get the Device suitable for a transition to RFPRO.

As shown in the diagram, at the conclusion of the provisioning step, the Device comes in the "Ready for Normal Operation" state where it has all it needs in order to start interoperating with other Devices. 8.2 specifies the minimum mandatory configuration that a Device shall hold in order to be considered as "Ready for Normal Operation".

In the event of power loss or Device failure, the Device should remain in the same state that it was in prior to the power loss / failure.

If a Device or resource owner OBSERVEs /pstat.dos.s, then transitions to SRESET will give early warning notification of Devices that may require SVR consistency checking.

In order for onboarding to function, the Device shall have the following Resources installed:

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
8.2 Device Onboarding-Reset State Definition

The /pstat.dos.s = RESET state is defined as a "hard" reset to manufacturer defaults. Hard reset also defines a state where the Device asset is ready to be transferred to another party.

The Platform manufacturer should provide a physical mechanism (e.g. button) that forces Platform reset. All Devices hosted on the same Platform transition their Device states to RESET when the Platform reset is asserted.

The following Resources and their specific properties shall have the value as specified:

1) The owned Property of the "/oic/sec/doxm" Resource shall transition to FALSE.
2) The devowneruuid Property of the "/oic/sec/doxm" Resource shall be nil UUID.
3) The devowner Property of the "/oic/sec/doxm" Resource shall be nil UUID, if this Property is implemented.
4) The deviceuuid Property of the "/oic/sec/doxm" Resource shall be set to the manufacturer default value.
5) The deviceid Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value, if this Property is implemented.
6) The sct Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value.
7) The oxmsel Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value.
8) The isop Property of the "/oic/sec/pstat" Resource shall be FALSE.
9) The dos Property of the "/oic/sec/pstat" Resource shall be updated: dos.s shall equal "RESET" state and dos.p shall equal "FALSE".
10)
11) The om (operational modes) Property of the "/oic/sec/pstat" Resource shall be set to the manufacturer default value.
12) The sm (supported operational modes) Property of the "/oic/sec/pstat" Resource shall be set to the manufacturer default value.
13) The rowneruuid Property of "/oic/sec/pstat", "/oic/sec/doxm", "/oic/sec/acl", "/oic/sec/amacl", "/oic/sec/sacl", and "/oic/sec/cred" Resources shall be nil UUID.
14) The supportedprofiles Property of the "/oic/sec/sp" Resource shall be set to the manufacturer default value.
15) The currentprofile Property of the "/oic/sec/sp" Resource shall be set to the manufacturer default value.

8.3 Device Ready-for-OTM State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for ownership transfer:

1) The owned Property of the "/oic/sec/doxm" Resource shall be FALSE and will transition to TRUE.
2) The devowner Property of the "/oic/sec/doxm" Resource shall be nil UUID, if this Property is implemented.

3) The devowneruuid Property of the "/oic/sec/doxm" Resource shall be nil UUID.

4) The deviceid Property of the "/oic/sec/doxm" Resource may be nil UUID, if this Property is implemented. The value of the di Property in "/oic/d" is undefined.

5) The deviceuuid Property of the "/oic/sec/doxm" Resource shall be set to the manufacturer default value.

6) The isop Property of the "/oic/sec/pstat" Resource shall be FALSE.

7) The dos of the "/oic/sec/pstat" Resource shall be updated: dos.s shall equal "RFOTM" state and dos.p shall equal "FALSE".

8) The "/oic/sec/cred" Resource shall contain credential(s) if required by the selected OTM.

8.4 Device Ready-for-Provisioning State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for provisioning:

1) The owned Property of the "/oic/sec/doxm" Resource shall be TRUE.

2) The devowneruuid Property of the "/oic/sec/doxm" Resource shall not be nil UUID.

3) The deviceuuid Property of the "/oic/sec/doxm" Resource shall not be nil UUID and shall be set to the value that was determined during RFOTM processing. Also the value of the di Property in "/oic/d" Resource shall be the same as the deviceid Property in the "/oic/sec/doxm" Resource.

4) The oxmsel Property of the "/oic/sec/doxm" Resource shall have the value of the actual OTM used during ownership transfer.

5) The isop Property of the "/oic/sec/pstat" Resource shall be FALSE.

6) The dos of the "/oic/sec/pstat" Resource shall be updated: dos.s shall equal "RFPRO" state and dos.p shall equal "FALSE".

7) The rowneruuid Property of every installed Resource shall be set to a valid Resource owner (i.e. an entity that is authorized to instantiate or update the given Resource). Failure to set a rowneruuid may result in an orphan Resource.

8) The "/oic/sec/cred" Resource shall contain credentials for each entity referenced by an rowneruuid, amsuuid, devowneruuid.

8.5 Device Ready-for-Normal-Operation State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for normal operation:

1) The owned Property of the "/oic/sec/doxm" Resource shall be TRUE.

2) The devowneruuid Property of the "/oic/sec/doxm" Resource shall not be nil UUID.

3) The deviceuuid Property of the "/oic/sec/doxm" Resource shall not be nil UUID and shall be set to the ID that was configured during OTM. Also the value of the "di" Property in "/oic/d" shall be the same as the deviceuuid.

4) The oxmsel Property of the "/oic/sec/doxm" Resource shall have the value of the actual OTM used during ownership transfer.

5) The isop Property of the "/oic/sec/pstat" Resource shall be set to TRUE by the Server once transition to RFNOP is otherwise complete.

6) The dos of the "/oic/sec/pstat" Resource shall be updated: dos.s shall equal "RFNOP" state and dos.p shall equal "FALSE".
7) The rowneruuid Property of every installed Resource shall be set to a valid resource owner (i.e. an entity that is authorized to instantiate or update the given Resource). Failure to set a rowneruuid results in an orphan Resource.

8) The "/oic/sec/cred" Resource shall contain credentials for each service referenced by a rowneruuid, amsuuid, devowneruuid.

8.6 Device Soft Reset State Definition

The soft reset state is defined (e.g. /pstat.dos.s = SRESET) where entrance into this state means the Device is not operational but remains owned by the current owner. The Device may exit SRESET by authenticating to a DOTS (e.g. "rt" = "oic.r.doxs") using the OC provided during original onboarding (but should not require use of an OTM /doxm.oxms).

The DOTS should perform a consistency check of the SVR and if necessary, re-provision them sufficiently to allow the Device to transition to RFPRO.

Figure 28 depicts OBT Sanity Check Sequence in SRESET.
The DOTS should perform a sanity check of SVRs before final transition to RFPRO Device state. If the DOTS credential cannot be found or is determined to be corrupted, the Device state transitions to RESET. The Device should remain in SRESET if the DOTS credential fails to validate the DOTS. This mitigates denial-of-service attacks that may be attempted by non-DOTS Devices.

When in SRESET, the following Resources and their specific Properties shall have the values as specified.

1) The owned Property of the "/oic/sec/doxm" Resource shall be TRUE.
2) The devowneruuid Property of the "/oic/sec/doxm" Resource shall remain non-null.
3) The devowner Property of the "/oic/sec/doxm" Resource shall be non-null, if this Property is implemented.
4) The deviceuuidProperty of the "/oic/sec/doxm" Resource shall remain non-null.
5) The deviceid Property of the "/oic/sec/doxm" Resource shall remain non-null.
6) The sct Property of the "/oic/sec/doxm" Resource shall retain its value.
7) The oxmsel Property of the "/oic/sec/doxm" Resource shall retain its value.
8) The isop Property of the "/oic/sec/pstat" Resource shall be FALSE.
9) The "/oic/sec/pstat.dos.s" Property shall be SRESET.
10) The om (operational modes) Property of the "/oic/sec/pstat" Resource shall be "client-directed mode".
11) The sm (supported operational modes) Property of "/oic/sec/pstat" Resource may be updated by the Device owner (aka DOTS).
12) The rowneruuid Property of "/oic/sec/pstat", "/oic/sec/doxm", "/oic/sec/acl", "/oic/sec/acl2", "/oic/sec/amacl", "/oic/sec/sacl", and "/oic/sec/cred" Resources may be reset by the Device owner (aka DOTS) and re-provisioned.
9 Security Credential Management

9.1 Preamble
This clause provides an overview of the credential types in OCF, along with details of credential use, provisioning and ongoing management.

9.2 Credential Lifecycle

9.2.1 Credential Lifecycle General
OCF credential lifecycle has the following phases: (1) creation, (2) deletion, (3) refresh, (4) issuance and (5) revocation.

9.2.2 Creation
The CMS shall provision credential Resources to the Device. The Device shall verify the CMS is authorized by matching the owneruuid Property of the "/oic/sec/cred" resource to the DeviceID of the credential the CMS used to establish the secure connection.

Credential Resources created using a CMS may involve specialized credential issuance protocols and messages. These may involve the use of public key infrastructure (PKI) such as a certificate authority (CA), symmetric key management such as a key distribution centre (KDC) or as part of a provisioning action by a DOTS, CMS or AMS.

9.2.3 Deletion
The CMS should delete known compromised credential Resources. The Device (e.g. the Device where the credential Resource is hosted) should delete credential Resources that have expired.

An expired credential Resource may be deleted to manage memory and storage space.

Deletion in OCF key management is equivalent to credential suspension.

9.2.4 Refresh
Credential refresh may be performed before it expires. The CMS shall perform credential refresh.

The "/oic/sec/cred" Resource supports expiry using the Period Property. Credential refresh may be applied when a credential is about to expire or is about to exceed a maximum threshold for bytes encrypted.

A credential refresh method specifies the options available when performing key refresh. The Period Property informs when the credential should expire. The Device may proactively obtain a new credential using a credential refresh method using current unexpired credentials to refresh the existing credential. If the Device does not have an internal time source, the current time should be obtained from a CMS at regular intervals.

If the CMS credential is allowed to expire, the DOTS service may be used to re-provision the CMS credentials to the Device. If the onboarding established credentials are allowed to expire the DOTS shall re-onboard the Device to re-apply device owner transfer steps.

All Devices shall support at least one credential refresh method.

9.2.5 Revocation
Credentials issued by a CMS may be equipped with revocation capabilities. In situations where the revocation method involves provisioning of a revocation object that identifies a credential that is to be revoked prior to its normal expiration period, a credential Resource is created containing the revocation information that supersedes the originally issued credential. The revocation object
expiration should match that of the revoked credential so that the revocation object is cleaned up upon expiry.

It is conceptually reasonable to consider revocation applying to a credential or to a Device. Device revocation asserts all credentials associated with the revoked Device should be considered for revocation. Device revocation is necessary when a Device is lost, stolen or compromised. Deletion of credentials on a revoked Device might not be possible or reliable.

9.3 Credential Types

9.3.1 Preamble

The "/oic/sec/cred" Resource maintains a credential type Property that supports several cryptographic keys and other information used for authentication and data protection. The credential types supported include pair-wise symmetric keys, group symmetric keys, asymmetric authentication keys, certificates (i.e. signed asymmetric keys) and shared-secrets (i.e. PIN/password).

9.3.2 Pair-wise Symmetric Key Credentials

The CMS shall provision exactly one other pair-wise symmetric credential to a peer Device. The CMS should not store pair-wise symmetric keys it provisions to managed Devices.

Pair-wise keys could be established through ad-hoc key agreement protocols.

The PrivateData Property in the "/oic/sec/cred" Resource contains the symmetric key.

The PublicData Property may contain a token encrypted to the peer Device containing the pair-wise key.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.

The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crt", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.

9.3.3 Group Symmetric Key Credentials

Group keys are symmetric keys shared among a group of Devices (3 or more). Group keys are used for efficient sharing of data among group participants.

Group keys do not provide authentication of Devices but only establish membership in a group.

The CMS shall provision group symmetric key credentials to the group members. The CMS maintains the group memberships.

The PrivateData Property in the "/oic/sec/cred" Resource contains the symmetric key.

The PublicData Property may contain the group name.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.
The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crl", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.

9.3.4 Asymmetric Authentication Key Credentials

9.3.4.1 Asymmetric Authentication Key Credentials General

Asymmetric authentication key credentials contain either a public and private key pair or only a public key. The private key is used to sign Device authentication challenges. The public key is used to verify a device authentication challenge-response.

The PrivateData Property in the "/oic/sec/cred" Resource contains the private key.

The PublicData Property contains the public key.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.

Devices should generate asymmetric authentication key pairs internally to ensure the private key is only known by the Device. See 9.3.4.2 for when it is necessary to transport private key material between Devices.

The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crl", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.

9.3.4.2 External Creation of Asymmetric Authentication Key Credentials

Devices should employ industry-standard high-assurance techniques when allowing off-device key pair creation and provisioning. Use of such key pairs should be minimized, particularly if the key pair is immutable and cannot be changed or replaced after provisioning.

When used as part of onboarding, these key pairs can be used to prove the Device possesses the manufacturer-asserted properties in a certificate to convince a DOTS or a user to accept onboarding the Device. See 7.3.3 for the OTM that uses such a certificate to authenticate the Device, and then provisions new OCF Security Domain credentials for use.

9.3.5 Asymmetric Key Encryption Key Credentials

The asymmetric key-encryption-key (KEK) credentials are used to wrap symmetric keys when distributing or storing the key.

The PrivateData Property in the "/oic/sec/cred" Resource contains the private key.

The PublicData Property contains the public key.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.

The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crl", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.
9.3.6 Certificate Credentials

Certificate credentials are asymmetric keys that are accompanied by a certificate issued by a CMS or an external certificate authority (CA).

A certificate enrolment protocol is used to obtain a certificate and establish proof-of-possession.

The issued certificate is stored with the asymmetric key credential Resource.

Other objects useful in managing certificate lifecycle such as certificate revocation status are associated with the credential Resource.

Either an asymmetric key credential Resource or a self-signed certificate credential is used to terminate a path validation.

The PrivateData Property in the "/oic/sec/cred" Resource contains the private key.

The PublicData Property contains the issued certificate.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.

The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crl", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.

9.3.7 Password Credentials

Shared secret credentials are used to maintain a PIN or password that authorizes Device access to a foreign system or Device that doesn’t support any other OCF credential types.

The PrivateData Property in the "/oic/sec/cred" Resource contains the PIN, password and other values useful for changing and verifying the password.

The PublicData Property may contain the user or account name if applicable.

The OptionalData Property may contain revocation status.

The Device implementer should apply hardened key storage techniques that ensure the PrivateData remains private.

The Device implementer should apply appropriate integrity, confidentiality and access protection of the "/oic/sec/cred", "/oic/sec/crl", "/oic/sec/roles", "/oic/sec/csr" Resources to prevent unauthorized modifications.

9.4 Certificate Based Key Management

9.4.1 Overview

To achieve authentication and transport security during communications in OCF Security Domain, certificates containing public keys of communicating parties and private keys can be used.

The certificate and private key may be issued by a local or remote certificate authority (CA). For the local CA, a certificate revocation list (CRL) based on X.509 is used to validate proof of identity. In the case of a remote CA, Online Certificate Status Protocol (OCSP) can be used to validate proof of identity and validity.
The OCF certificate and OCF CRL (Certificate Revocation List) format is a subset of X.509 format, only elliptic curve algorithm and DER encoding format are allowed, most of optional fields in X.509 are not supported so that the format intends to meet the constrained Device’s requirement.

As for the certificate and CRL management in the Server, the process of storing, retrieving and parsing Resources of the certificates and CRL will be performed at the security resource manager layer; the relevant interfaces may be exposed to the upper layer.

A SRM is the security enforcement point in a Server as described in clause 5.5, so the data of certificates and CRL will be stored and managed in SVR database.

The CMS manages the certificate lifecycle for certificates it issues. The DOTS shall assign a CMS to a Device when it is newly onboarded. The issuing CMS should process certificate revocations for certificates it issues. If a certificate private key is compromised, the CMS should revoke the certificate. If CRLs are used by a Device, the CMS should regularly (for example; every 3 months) update the "/oic/sec/crl" resource for the Devices it manages.

### 9.4.2 X.509 Digital Certificate Profiles

#### 9.4.2.1 Digital Certificate Profile General

An OCF certificate format is a subset of X.509 format (version 3 or above) as defined in IETF RFC 5280.

This clause develops a profile to facilitate the use of X.509 certificates within OCF applications for those communities wishing to make use of X.509 technology. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of OCF specific extension(s). The supported standard certificate extensions are also listed.

Certificate Format: The OCF certificate profile is derived from IETF RFC 5280. However, this document does not support the "issuerUniqueID" and "subjectUniqueID" fields which are deprecated and shall not be used in the context of OCF. If these fields are present in a certificate, compliant entities shall ignore their contents.

Certificate Encoding: Conforming entities shall use the Distinguished Encoding Rules (DER) as defined in ISO/IEC 8825-1 to encode certificates.

Certificates Hierarchy and Crypto Parameters. OCF supports a three-tier hierarchy for its Public Key Infrastructure (i.e., a Root CA, an Intermediate CA, and EE certificates). OCF accredited CAs SHALL use Elliptic Curve Cryptography (ECC) keys (secp256r1 – OID:1.2.840.10045.3.1.7) and use the ecdsaWithSHA256 (OID:1.2.840.10045.4.3.2) algorithm for certificate signatures.

The following clauses specify the supported standard and custom extensions for the OCF certificates profile.

#### 9.4.2.2 Certificate Profile and Fields

#### 9.4.2.2.1 Root CA Certificate Profile

Table 16 describes X.509 v1 fields required for Root CA Certificates.

<table>
<thead>
<tr>
<th>V1 Field</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>signatureAlgorithm</td>
<td>ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)</td>
</tr>
<tr>
<td>Version</td>
<td>v3 (value is 2)</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>SHALL be a positive integer, unique among all certificates issued by a given CA</td>
</tr>
</tbody>
</table>
Table 17 describes X.509 v3 extensions required for Root CA Certificates.

Table 17 - X.509 v3 extensions for Root CA Certificates

<table>
<thead>
<tr>
<th>Extension</th>
<th>Required/Optional</th>
<th>Criticality</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorityKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>subjectKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>keyUsage</td>
<td>REQUIRED</td>
<td>Critical</td>
<td>keyCertSign (5) &amp; cRLSign (6) bits shall be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>digitalSignature(0) bit may be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All other bits shall not be enabled.</td>
</tr>
<tr>
<td>basicConstraints</td>
<td>REQUIRED</td>
<td>Critical</td>
<td>cA = TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>pathLenConstraint = not present (unlimited)</td>
</tr>
</tbody>
</table>

9.4.2.2.2 Intermediate CA Certificate Profile

Table 18 describes X.509 v1 fields required for Intermediate CA Certificates.

Table 18 - X.509 v1 fields for Intermediate CA Certificates

<table>
<thead>
<tr>
<th>V1 Field</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>signatureAlgorithm</td>
<td>ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)</td>
</tr>
<tr>
<td>Version</td>
<td>v3 (value is 2)</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>SHALL be a positive integer, unique among all</td>
</tr>
<tr>
<td></td>
<td>certificates issued by Root CA</td>
</tr>
<tr>
<td>Issuer</td>
<td>SHALL match the Subject field of the issuing Root CA</td>
</tr>
<tr>
<td>Subject</td>
<td>(no stipulation)</td>
</tr>
<tr>
<td>notBefore</td>
<td>The time at which the Intermediate CA Certificate was</td>
</tr>
<tr>
<td></td>
<td>generated.</td>
</tr>
<tr>
<td></td>
<td>See clause 10.4.5 for details around IETF RFC 5280-</td>
</tr>
<tr>
<td></td>
<td>compliant validity field formatting.</td>
</tr>
<tr>
<td>notAfter</td>
<td>No stipulation for expiry date.</td>
</tr>
<tr>
<td></td>
<td>See clause 10.4.5 for details around IETF RFC 5280-</td>
</tr>
<tr>
<td></td>
<td>compliant validity field formatting.</td>
</tr>
<tr>
<td>Subject Public Key Info</td>
<td>id-ecPublicKey (OID: 1.2.840.10045.2.1)</td>
</tr>
<tr>
<td></td>
<td>secp256r1 (OID: 1.2.840.10045.3.1.7)</td>
</tr>
</tbody>
</table>

Table 19 describes X.509 v3 extensions required for Intermediate CA Certificates.
Table 19 – X.509 v3 extensions for Intermediate CA Certificates

<table>
<thead>
<tr>
<th>Extension</th>
<th>Required/Optional</th>
<th>Criticality</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorityKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>subjectKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>keyUsage</td>
<td>REQUIRED</td>
<td>Critical</td>
<td>keyCertSign (5) &amp; cRLSign (6) bits shall be enabled. digitalSignature (0) bit may be enabled. All other bits shall not be enabled.</td>
</tr>
<tr>
<td>basicConstraints</td>
<td>REQUIRED</td>
<td>Critical</td>
<td>cA = TRUE pathLenConstraint = 0 (can only sign End-Entity certs)</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>(no stipulation)</td>
</tr>
<tr>
<td>cRLDistributionPoints</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>1 or more URIs where the Certificate Revocation List (CRL) from the Root can be obtained.</td>
</tr>
<tr>
<td>authorityInformationAccess</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>OCSP URI – the URI of the Root CA's OCSP Responder</td>
</tr>
</tbody>
</table>

9.4.2.2.3 End-Entity Black Certificate Profile

Table 20 describes X.509 v1 fields required for End-Entity Certificates used for Black security profile.

Table 20 – X.509 v1 fields for End-Entity Certificates

<table>
<thead>
<tr>
<th>V1 Field</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>signatureAlgorithm</td>
<td>ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)</td>
</tr>
<tr>
<td>Version</td>
<td>v3 (value is 2)</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>SHALL be a positive integer, unique among all certificates issued by the Intermediate CA</td>
</tr>
<tr>
<td>Issuer</td>
<td>SHALL match the Subject field of the issuing Intermediate CA</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject DN shall include:</td>
</tr>
<tr>
<td></td>
<td>o=OCF-verified device manufacturer organization name.</td>
</tr>
<tr>
<td></td>
<td>The Subject DN may include other attributes (e.g. cn, c, ou, etc.) with no stipulation by OCF.</td>
</tr>
<tr>
<td>notBefore</td>
<td>The time at which the End-Entity Certificate was generated. See clause 10.4.5 for details around IETF RFC 5280-compliant validity field formatting.</td>
</tr>
<tr>
<td>notAfter</td>
<td>No stipulation. See clause 10.4.5 for details around IETF RFC 5280-compliant validity field formatting.</td>
</tr>
<tr>
<td>Subject Public Key Info</td>
<td>id-ecPublicKey (OID: 1.2.840.10045.2.1) secp256r1 (OID:1.2.840.10045.3.1.7)</td>
</tr>
</tbody>
</table>

Table 21 describes X.509 v3 extensions required for End-Entity Certificates.
<table>
<thead>
<tr>
<th>Extension</th>
<th>Required/Optional</th>
<th>Criticality</th>
<th>Value / Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorityKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>subjectKeyIdentifier</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>N/A</td>
</tr>
<tr>
<td>keyUsage</td>
<td>REQUIRED</td>
<td>Critical</td>
<td>digitalSignature (0) and keyAgreement (4) bits SHALL be the only bits enabled</td>
</tr>
<tr>
<td>basicConstraints</td>
<td>OPTIONAL</td>
<td>Non-Critical</td>
<td>cA = FALSE, pathLenConstraint = not present</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>End-Entity certificates chaining to an OCF Root CA SHOULD contain at least one PolicyIdentifier set to the OCF Certificate Policy OID – (1.3.6.1.4.1.51414.0.1.2) corresponding to the version of the OCF Certificate Policy under which it was issued. Additional manufacturer-specific CP OIDs may also be populated.</td>
</tr>
<tr>
<td>extendedKeyUsage</td>
<td>REQUIRED</td>
<td>Non-critical</td>
<td>The following extendedKeyUsage (EKU) OIDs SHALL both be present:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- serverAuthentication - 1.3.6.1.5.5.7.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- clientAuthentication - 1.3.6.1.5.5.7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Exactly ONE of the following OIDs SHALL be present:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Identity certificate - 1.3.6.1.4.1.44924.1.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Role certificate - 1.3.6.1.4.1.44924.1.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>End-Entity certificates SHALL NOT contain the anyExtendedKeyUsage OID (2.5.29.37.0)</td>
</tr>
<tr>
<td>subjectAlternativeName</td>
<td>REQUIRED UNDER CERTAIN CONDITIONS</td>
<td>Non-critical</td>
<td>The subjectAltName extension is used to encode one or more Role ID values in role certificates, binding the roles to the subject public key. When the extendedKeyUsage (EKU) extension contains the Identity Certificate OID (1.3.6.1.4.1.44924.1.6), the subjectAltName extension SHOULD NOT be present. If the EKU extension contains the Role Certificate</td>
</tr>
<tr>
<td>Extension</td>
<td>Type</td>
<td>Criticality</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cRLDistributionPoints</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>1 or more URLs where the Certificate Revocation List (CRL) from the Intermediate CA can be obtained.</td>
</tr>
<tr>
<td>authorityInformationAccess</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>OCSP URI – the URI of the Intermediate CA's OCSP Responder</td>
</tr>
<tr>
<td>OCF Compliance</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>See 9.4.2.2.4</td>
</tr>
<tr>
<td>Manufacturer Usage Description (MUD)</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>Contains a single Uniform Resource Locator (URL) that points to an on-line Manufacturer Usage Description concerning the certificate subject. See 9.4.2.2.5</td>
</tr>
<tr>
<td>OCF Security Claims</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>Contains a list of security claims above those required by this OCF Compliance version or Security Profile. See 9.4.2.2.6</td>
</tr>
<tr>
<td>OCF CPL Attributes</td>
<td>OPTIONAL</td>
<td>Non-critical</td>
<td>Contains the list of OCF Attributes used to perform OCF Certified Product List lookups</td>
</tr>
</tbody>
</table>

**9.4.2.2.4 OCF Compliance X.509v3 Extension**

The OCF Compliance Extension defines required parameters to correctly identify the type of Device, its manufacturer, its OCF Version, and the Security Profile compliance of the device.

The extension carries an "ocfVersion" field which provides the specific base version of the OCF documents the device implements. The "ocfVersion" field shall contain a sequence of three integers ("major", "minor", and "build"). For example, if an entity is certified to be compliant with...
OCF specifications 1.3.2, then the "major", "minor", and "build" fields of the "ocfVersion" will be set to "1", "3", and "2" respectively. The "ocfVersion" may be used by Security Profiles to denote compliance to a specified base version of the OCF documents.

The "securityProfile" field shall carry the ocfSecurityProfile OID(s) (clause 14.8.3) of one or more supported Security Profiles associated with the certificate in string form (UTF-8). All Security Profiles associated with the certificate should be identified by this field.

The extension shall also carry two string fields (UTF-8): "DeviceName" and "deviceManufacturer". The fields carry human-readable descriptions of the Device's name and manufacturer, respectively.

The ASN.1 definition of the OCFCompliance extension (OID – 1.3.6.1.4.1.51414.1.0) is defined as follows:

```asn1
ocfVersion ::= SEQUENCE {
    major INTEGER, --Major version number
    minor INTEGER, --Minor version number
    build INTEGER, --Build/Micro version number
}

ocfCompliance ::= SEQUENCE {
    version   ocfVersion, --Device/OCF version
    securityProfile  SEQUENCE SIZE (1..MAX) OF ocfSecurityProfileOID, --Sequence of OCF Security Profile OID strings
    --Clause 14.8.2 defines valid ocfSecurityProfileOIDS
    deviceName  UTF8String, --Name of the device
    deviceManufacturer UTF8String, --Human-Readable Manufacturer
    --of the device
}
```

### 9.4.2.2.5 Manufacturer Usage Description (MUD) X.509v3 Extension

The goal of the Manufacturer Usage Description (MUD) extension is to provide a means for devices to signal to the network the access and network functionality they require to properly function. Access controls can be more easily achieved and deployed at scale when the MUD extension is used. The current draft of the MUD v3 extension at this time of writing is:


The ASN.1 definition of the MUD v3 extension is defined as follows:

```asn1
MUDURLExtxnModule-2016 { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7)
    id-mod(0) id-mod-mudURLExtxn2016(88) }
```

```asn1
-- IMPORTS
```

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
9.4.2.6 OCF Security Claims X.509v3 Extension

The OCF Security Claims Extension defines a list of OIDs representing security claims that the manufacturer/integrator is making as to the security posture of the device above those required by the OCF Compliance version or that of the OCF Security Profile being indicated by the device.

The purpose of this extension is to allow for programmatic evaluation of assertions made about security to enable some platforms/policies/administrators to better understand what is being onboarded or challenged.

The ASN.1 definition of the OCF Security Claims extension (OID – 1.3.6.1.4.1.51414.1.1) is defined as follows:

```
id-OCF OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) OCF(51414) }

id-ocfX509Extensions OBJECT IDENTIFIER ::= { id-OCF 1 }

id-ocfSecurityClaims OBJECT IDENTIFIER ::= { id-ocfX509Extensions 1 }

claim-secure-boot ::= ocfSecurityClaimsOID { id-ocfSecurityClaims 0 }
  -- Device claims that the boot process follows a procedure trusted by the firmware and the BIOS

claim-hw-backed-cred-storage ::= ocfSecurityClaimsOID { id-ocfSecurityClaims 1 }
  -- Device claims that credentials are stored in a specialized hardware protection environment such as a Trusted Platform Module (TPM) or similar mechanism.

ocfSecurityClaimsOID ::= OBJECT IDENTIFIER

ocfSecurityClaims ::= SEQUENCE SIZE (1..MAX) of ocfSecurityClaimsOID
```

9.4.2.7 OCF Certified Product List Attributes X.509v3 Extension

The OCF Certified Product List Extension defines required parameters to utilize the OCF Compliance Management System Certified Product List (OCMS-CPL). This clause is only applicable if you plan to utilize the OCMS-CPL. The OBT may make use of these attributes to verify the compliance level of a device.

The extension carries the OCF CPL Attributes: IANA Private Enterprise Number (PEN), Model and Version.
The 'cpl-at-IANAPen' IANA Private Enterprise Number (PEN) provides the manufacturer's unique PEN established in the IANA PEN list located at: https://www.iana.org/assignments/enterprise-numbers. The 'cpl-at-IANAPen' field found in end-products shall be the same information as reported during OCF Certification.

The 'cpl-at-model' represents an OCF-Certified product's model name. The 'cpl-at-model' field found in end-products shall be the same information as reported during OCF Certification.

The 'cpl-at-version' represents an OCF-Certified product's version. The 'cpl-at-version' field found in end-products shall be the same information as reported during OCF Certification.

The ASN.1 definition of the OCF CPL Attributes extension (OID – 1.3.6.1.4.1.51414.1.2) is defined as follows:

```asn1
id-OCF OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1)
  private(4) enterprise(1) OCF(51414) }

id-ocfx509Extensions OBJECT IDENTIFIER ::= { id-OCF 1 }

id-ocfCPLAttributes OBJECT IDENTIFIER ::= { id-ocfx509Extensions 2 }

cpl-at-IANAPen ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 0 }
cpl-at-model ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 1 }
cpl-at-version ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 2 }

ocfCPLAttributes ::= SEQUENCE {
  cpl-at-IANAPen UTF8String,
  -- Manufacturer's registered IANA Private Enterprise Number
  cpl-at-model UTF8String,
  -- Device OCF Security Profile
  cpl-at-version UTF8String
  -- Name of the device
}
```

9.4.2.3 Supported Certificate Extensions

As these certificate extensions are a standard part of IETF RFC 5280, this document includes the clause number from that RFC to include it by reference. Each extension is summarized here, and any modifications to the RFC definition are listed. Devices MUST implement and understand the extensions listed here; other extensions from the RFC are not included in this document and therefore are not required. 10.4 describes what Devices must implement when validating certificate chains, including processing of extensions, and actions to take when certain extensions are absent.

– Authority Key Identifier (4.2.1.1)

The Authority Key Identifier (AKI) extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This document makes the following modifications to the referenced definition of this extension:

The authorityCertIssuer or authorityCertSerialNumber fields of the AuthorityKeyIdentifier sequence are not permitted; only keyIdentifier is allowed. This results in the following grammar definition:

```asn1
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE {
  keyIdentifier [0] KeyIdentifier
}

KeyIdentifier ::= OCTET STRING
```

– Subject Key Identifier (4.2.1.2)
The Subject Key Identifier (SKI) extension provides a means of identifying certificates that contain a particular public key.

This document makes the following modification to the referenced definition of this extension:

Subject Key Identifiers SHOULD be derived from the public key contained in the certificate's SubjectPublicKeyInfo field or a method that generates unique values. This document RECOMMENDS the 256-bit SHA-2 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Devices verifying certificate chains must not assume any particular method of computing key identifiers, however, and must only base matching AKI's and SKI's in certification path constructions on key identifiers seen in certificates.

Subject Alternative Name

If the EKU extension is present, and has the value XXXXXX, indicating that this is a role certificate, the Subject Alternative Name (subjectAltName) extension shall be present and interpreted as described below. When no EKU is present, or has another value, the subjectAltName extension SHOULD be absent. The subjectAltName extension is used to encode one or more Role ID values in role certificates, binding the roles to the subject public key. The subjectAltName extension is defined in IETF RFC 5280 (See 4.2.1.6):

```
id-ce-subjectAltName OBJECT IDENTIFIER ::= { id-ce 17 }
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
  otherName                       [0]     OtherName,
  rfc5280Name                     [1]     IA5String,
  dNSName                         [2]     IA5String,
  x400Address                     [3]     ORAddress,
  directoryName                   [4]     Name,
  ediPartyName                    [5]     EDIPartyName,
  uniformResourceIdentifier       [6]     IA5String,
  iPAddress                       [7]     OCTET STRING,
  registeredID                    [8]     OBJECT IDENTIFIER }
EDIPartyName ::= SEQUENCE {
  nameAssigner            [0]     DirectoryString OPTIONAL,
  partyName               [1]     DirectoryString }
```

Each GeneralName in the GeneralNames SEQUENCE which encodes a role shall be a directoryName, which is of type Name. Name is an X.501 Distinguished Name. Each Name shall contain exactly one CN (Common Name) component, and zero or one OU (Organizational Unit) components. The OU component, if present, shall specify the authority that defined the semantics of the role. If the OU component is absent, the certificate issuer has defined the role. The CN component shall encode the role ID. Other GeneralName types in the SEQUENCE may be present, but shall not be interpreted as roles. Therefore, if the certificate issuer includes non-role names in the subjectAltName extension, the extension should not be marked critical.

The role, and authority need to be encoded as ASN.1 PrintableString type, the restricted character set [0-9a-z-A-Z ()+-.?/=].

Key Usage (4.2.1.3)

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.

This document does not modify the referenced definition of this extension.
– Basic Constraints (4.2.1.9)
The basic constraints extension identifies whether the subject of the certificate is a CA and
the maximum depth of valid certification paths that include this certificate. Without this
extension, a certificate cannot be an issuer of other certificates.
This document does not modify the referenced definition of this extension.

– Extended Key Usage (4.2.1.12)

Extended Key Usage describes allowed purposes for which the certified public key may can
be used. When a Device receives a certificate, it determines the purpose based on the
context of the interaction in which the certificate is presented, and verifies the certificate can
be used for that purpose.

This document makes the following modifications to the referenced definition of this extension:
CAs SHOULD mark this extension as critical.
CAs MUST NOT issue certificates with the anyExtendedKeyUsage OID (2.5.29.37.0).

The list of OCF-specific purposes and the assigned OIDs to represent them are:
– Identity certificate 1.3.6.1.4.1.44924.1.6
– Role certificate 1.3.6.1.4.1.44924.1.7

9.4.2.4 Cipher Suite for Authentication, Confidentiality and Integrity
See 9.4.3.5 for details.

9.4.2.5 Encoding of Certificate
See 9.4.2 for details.

9.4.3 Certificate Revocation List (CRL) Profile

9.4.3.1 CRL General
This clause provides a profile for Certificates Revocation Lists (or CRLs) to facilitate their use
within OCF applications for those communities wishing to support revocation features in their
PKIs.

The OCF CRL profile is derived from IETF RFC 5280 and supports the syntax specified in
IETF RFC 5280 – Clause 5.1

9.4.3.2 CRL Profile and Fields
This clause intentionally left empty.

9.4.3.3 Encoding of CRL
The ASN.1 distinguished encoding rules (DER method of encoding) defined in [ISO/IEC 8825-1]
should be used to encode CRL.

9.4.3.4 CRLs Supported Standard Extensions
The extensions defined by ANSI X9, ISO/IEC, and ITU-T for X.509 v2 CRLs [X.509] [X9.55]
provide methods for associating additional attributes with CRLs. The following list of X.509
extensions should be supported in this certificate profile:

– Authority Key Identifier (Optional; non-critical) - The authority key identifier extension provides
a means of identifying the public key corresponding to the private key used to sign a CRL.
Conforming CRL issuers should use the key identifier method, and shall include this extension
in all CRLs issued.
CRL Number (Optional; non-critical) - The CRL number is a non-critical CRL extension that conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer.

CRL Entry Extensions: The CRL entry extensions defined by ISO/IEC, ITU-T, and ANSI X9 for X.509 v2 CRLs provide methods for associating additional attributes with CRL entries [X.509][X9.55]. Although this document does not provide any recommendation about the use of specific extensions for CRL entries, conforming CAs may use them in CRLs as long as they are not marked critical.

9.4.3.5 Encryption Ciphers and TLS support
OCF compliant entities shall support TLS version 1.2. Compliant entities shall support TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite as defined in IETF RFC 7251 and may support additional ciphers as defined in the TLS v1.2 specifications.

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

The cred Resource contains the certificate information pertaining to the Device. The PublicData Property holds the device certificate and CA certificate chain. PrivateData Property holds the Device private key paired to the certificate. (See 13.3 for additional detail regarding the `/oic/sec/cred` Resource).

A certificate revocation list Resource is used to maintain a list of revoked certificates obtained through the CMS. The Device must consider revoked certificates as part of certificate path verification. If the CRL Resource is stale or there are insufficient Platform Resources to maintain a full list, the Device must query the CMS for current revocation status. (See 13.4 for additional detail regarding the `/oic/sec/crl` Resource).

9.4.5 Certificate Provisioning
The CMS (e.g. a hub or a smart phone) issues certificates for new Devices. The CMS shall have its own certificate and key pair. The certificate is either a) self-signed if it acts as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either case, the certificate shall have the format described in 9.4.2.

The CA in the CMS shall retrieve a Device's public key and proof of possession of the private key, generate a Device's certificate signed by this CA certificate, and then the CMS shall transfer them to the Device including its CA certificate chain. Optionally, the CMS may also transfer one or more role certificates, which shall have the format described in clause 9.4.2. The subjectPublicKey of each role certificate shall match the subjectPublicKey in the Device certificate.

In the sequence in Figure 29, the Certificate Signing Request (CSR) is defined by PKCS#10 in IETF RFC 2986, and is included here by reference.

The sequence flow of a certificate transfer for a Client-directed model is described in Figure 29.

1) The CMS retrieves a CSR from the Device that requests a certificate. In this CSR, the Device shall place its requested UUID into the subject and its public key in the SubjectPublicKeyInfo. The Device determines the public key to present; this may be an already-provisioned key it has selected for use with authentication, or if none is present, it may generate a new key pair internally and provide the public part. The key pair shall be compatible with the allowed ciphersuites listed in 9.4.2.4 and 11.3.4, since the certificate will be restricted for use in OCF authentication.

2) If the Device does not have a pre-provisioned key pair and is unable to generate a key pair on its own, then it is not capable of using certificates. The Device shall advertise this fact both by
setting the 0x8 bit position in the sct Property of "/oic/sec/doxm" to 0, and return an error that
the "/oic/sec/csr" resource does not exist.

3) The CMS shall transfer the issued certificate and CA chain to the designated Device using
the same credid, to maintain the association with the private key. The credential type
("oic.sec.cred") used to transfer certificates in Figure 29 is also used to transfer role
certificates, by including multiple credentials in the POST from CMS to Device. Identity
certificates shall be stored with the credusage Property set to "oic.sec.cred.cert" and role
certificates shall be stored with the credusage Property set to "oic.sec.cred.rolecert".

Client-directed Certificate Transfer

The Ownership Credential should be used to establish a secure connection.

1) RETRIEVE /oic/sec/csr
2) RSP ["csr":"<contents of CSR>", "encoding":"<supported-encoding-types>"
3) UPDATE /oic/sec/cred ["credtype":8, "subject":"deviceuid", "credusage":"oic.sec.cred.cert",
"publicdata":"<DER-encoded device and CA certificate chain in base64>"
4) RSP 2.04
5) UPDATE /oic/sec/pstat ["...", "im":"bx00100000", ..."]
6) RSP 2.04

Figure 29 – Client-directed Certificate Transfer

9.4.6 CRL Provisioning
The only pre-requisite of CRL issuing is that CMS (e.g. a hub or a smart phone) has the
function to register revocation certificates, to sign CRL and to transfer it to Devices.

The CMS sends the CRL to the Device.

Any certificate revocation reasons listed below cause CRL update on each Device.

- change of issuer name
- change of association between Devices and CA
- certificate compromise
- suspected compromise of the corresponding private key

CRL may be updated and delivered to all accessible Devices in the OCF Security Domain. In
some special cases, Devices may request CRL to a given CMS.

There are two options to update and deliver CRL;

- CMS pushes CRL to each Device
- each Device periodically requests to update CRL

The sequence flow of a CRL transfer for a Client-directed model is described in Figure 30.

1) The CMS may retrieve the CRL Resource Property.
2) If the Device requests the CMS to send CRL, it should transfer the latest CRL to the Device.

---

**Figure 30 – Client-directed CRL Transfer**

The sequence flow of a CRL transfer for a Server-directed model is described in Figure 31.

1) The Device retrieves the CRL Resource Property "tupdate" to the CMS.
2) If the CMS recognizes the updated CRL information after the designated "tupdate" time, it may transfer its CRL to the Device.
Server-directed CRL transfer

The Ownership Credential should be used to establish a secure connection

1. GET /oic/sec/crl?tupdate=NULL or UTC\$IME

2. POST /oic/sec/crl
   ["crlid":"","tupdate"..., "crldata" "DER-encoded CRL in base64"]

3. RSP 2.04

4. UPDATE /oic/sec/pstat
   ["cm"="b\times0010.0000", ...]

5. RSP 2.04
10 Device Authentication

10.1 Device Authentication General
When a Client is accessing a restricted Resource on a Server, the Server shall authenticate the Client. Clients shall authenticate Servers while requesting access. Clients may also assert one or more roles that the server can use in access control decisions. Roles may be asserted when the Device authentication is done with certificates.

10.2 Device Authentication with Symmetric Key Credentials
When using symmetric keys to authenticate, the Server Device shall include the ServerKeyExchange message and set psk_identity_hint to the Server's Device ID. The Client shall validate that it has a credential with the Subject ID set to the Server's Device ID, and a credential type of PSK. If it does not, the Client shall respond with an unknown_psk_identity error or other suitable error.

If the Client finds a suitable PSK credential, it shall reply with a ClientKeyExchange message that includes a psk_identity_hint set to the Client's Device ID. The Server shall verify that it has a credential with the matching Subject ID and type. If it does not, the Server shall respond with an unknown_psk_identity or other suitable error code. If it does, then it shall continue with the DTLS protocol, and both Client and Server shall compute the resulting premaster secret.

10.3 Device Authentication with Raw Asymmetric Key Credentials
When using raw asymmetric keys to authenticate, the Client and the Server shall include a suitable public key from a credential that is bound to their Device. Each Device shall verify that the provided public key matches the Public Data field of a credential they have, and use the corresponding Subject ID of the credential to identify the peer Device.

10.4 Device Authentication with Certificates

10.4.1 Device Authentication with Certificates General
When using certificates to authenticate, the Client and Server shall each include their certificate chain, as stored in the appropriate credential, as part of the selected authentication cipher suite. Each Device shall validate the certificate chain presented by the peer Device. Each certificate signature shall be verified until a public key is found within the "/oic/sec/cred" Resource with the "oic.sec.cred.trustca" credusage. Credential Resource found in "/oic/sec/cred" are used to terminate certificate path validation. Also, the validity period and revocation status should be checked for all above certificates, but at this time a failure to obtain a certificate's revocation status (CRL or OCSP response) MAY continue to allow the use of the certificate if all other verification checks succeed.

If available, revocation information should be used to verify the revocation status of the certificate. The URL referencing the revocation information should be retrieved from the certificate (via the authorityInformationAccess or crlDistributionPoints extensions). Other mechanisms may be used to gather relevant revocation information like CRLs or OCSP responses.

Each Device shall use the corresponding Subject ID of the credential to identify the peer Device.

Devices must follow the certificate path validation algorithm in clause 6 of IETF RFC 5280. In particular:

- For all non-End-Entity certificates, Devices shall verify that the basic constraints extension is present, and that the cA boolean in the extension is TRUE. If either is false, the certificate chain MUST be rejected. If the pathLenConstraint field is present, Devices will confirm the number of certificates between this certificate and the End-Entity certificate is less than or equal to pathLenConstraint. In particular, if pathLenConstraint is zero, only an End-Entity
certificate can be issued by this certificate. If the pathLenConstraint field is absent, there is no limit to the chain length.

– For all non-End-Entity certificates, Devices shall verify that the key usage extension is present, and that the keyCertSign bit is asserted.

– Devices may use the Authority Key Identifier extension to quickly locate the issuing certificate. Devices MUST NOT reject a certificate for lacking this extension, and must instead attempt validation with the public keys of possible issuer certificates whose subject name equals the issuer name of this certificate.

– The End-Entity certificate of the chain shall be verified to contain an Extended Key Usage (EKU) suitable to the purpose for which it is being presented. An End-Entity certificate which contains no EKU extension is not valid for any purpose and must be rejected. Any certificate which contains the anyExtendedKeyUsage OID (2.5.29.37.0) must be rejected, even if other valid EKUs are also present.

– Devices MUST verify "transitive EKU" for certificate chains. Issuer certificates (any certificate that is not an End-Entity) in the chain MUST all be valid for the purpose for which the certificate chain is being presented. An issuer certificate is valid for a purpose if it contains an EKU extension and the EKU OID for that purpose is listed in the extension, OR it does not have an EKU extension. An issuer certificate SHOULD contain an EKU extension and a complete list of EKUs for the purposes for which it is authorized to issue certificates. An issuer certificate without an EKU extension is valid for all purposes; this differs from End-Entity certificates without an EKU extension.

The list of purposes and their associated OIDs are defined in 9.4.2.3.

If the Device does not recognize an extension, it must examine the critical field. If the field is TRUE, the Device MUST reject the certificate. If the field is FALSE, the Device MUST treat the certificate as if the extension were absent and proceed accordingly. This applies to all certificates in a chain.

NOTE Certificate revocation mechanisms are currently out of scope of this version of the document.

10.4.2 Role Assertion with Certificates

This clause describes role assertion by a client to a server using a certificate role credential. If a server does not support the certificate credential type, clients should not attempt to assert roles with certificates.

Following authentication with a certificate, a client may assert one or more roles by updating the server’s roles resource with the role certificates it wants to use. The role credentials must be certificate credentials and shall include a certificate chain. The server shall validate each certificate chain as specified in clause 10.3. Additionally, the public key in the End-Entity certificate used for Device authentication must be identical to the public key in all role (End-Entity) certificates. Also, the subject distinguished name in the End-Entity authentication and role certificates must match. The roles asserted are encoded in the subjectAltName extension in the certificate. The subjectAltName field can have multiple values, allowing a single certificate to encode multiple roles that apply to the client. The server shall also check that the EKU extension of the role certificate(s) contains the value 1.3.6.1.4.1.44924.1.7 (see clause 9.4.2.2) indicating the certificate may be used to assert roles. Figure 32 describes how a client Device asserts roles to a server.
Figure 32 – Asserting a role with a certificate role credential.

Additional comments for Figure 32

1) The response shall contain "204 No Content" to indicate success or 4xx to indicate an error. If the server does not support certificate credentials, it should return "501 Not Implemented".

2) Roles asserted by the client may be kept for a duration chosen by the server. The duration shall not exceed the validity period of the role certificate. When fresh CRL information is obtained, the certificates in "/oic/sec/roles" should be checked, and the role removed if the certificate is revoked or expired.

3) Servers should choose a nonzero duration to avoid the cost of frequent re-assertion of a role by a client. It is recommended that servers use the validity period of the certificate as a duration, effectively allowing the CMS to decide the duration.

4) The format of the data sent in the create call shall be a list of credentials ("oic.sec.cred", see Table 28). They shall have credtype 8 (indicating certificates) and PrivateData field shall not be present. For fields that are duplicated in the "oic.sec.cred" object and the certificate, the value in the certificate shall be used for validation. For example, if the Period field is set in the credential, the server shall treat the validity period in the certificate as authoritative. Similar for the roleid data (authority, role).

5) Certificates shall be encoded as in Figure 29 (DER-encoded certificate chain in base64).

6) Clients may GET the "/oic/sec/roles" resource to determine the roles that have been previously asserted. An array of credential objects shall be returned. If there are no valid certificates corresponding to the currently connected and authenticated Client's identity, then an empty array (i.e. []) shall be returned.

10.4.3 OCF PKI Roots

This clause intentionally left empty.

10.4.4 PKI Trust Store

Each Device using a certificate chained to an OCF Root CA trust anchor SHALL securely store the OCF Root CA certificates in the oic/sec/cred resource and SHOULD physically store this resource in a hardened memory location where the certificates cannot be tampered with.
10.4.5 Path Validation and extension processing

Devices SHALL follow the certificate path validation algorithm in clause 6 of IETF RFC 5280. In addition, the following are best practices and SHALL be adhered to by any OCF-compliant application handling digital certificates.

- Validity Period checking

OCF-compliant applications SHALL conform to IETF RFC 5280 clauses 4.1.2.5, 4.1.2.5.1, and 4.1.2.5.2 when processing the notBefore and notAfter fields in X.509 certificates. In addition, for all certificates, the notAfter value SHALL NOT exceed the notAfter value of the issuing CA.

- Revocation checking

Relying applications SHOULD check the revocation status for all certificates, but at this time, an application MAY continue to allow the use of the certificate upon a failure to obtain a certificate’s revocation status (CRL or OCSP response), if all other verification checks succeed.

- basicConstraints

For all Root and Intermediate Certificate Authority (CA) certificates, Devices SHALL verify that the basicConstraints extension is present, flagged critical, and that the cA boolean value in the extension is TRUE. If any of these are false, the certificate chain SHALL be rejected.

If the pathLenConstraint field is present, Devices will confirm the number of certificates between this certificate and the End-Entity certificate is less than or equal to pathLenConstraint. In particular, if pathLenConstraint is zero, only an End-Entity certificate can be issued by this certificate. If the pathLenConstraint field is absent, there is no limit to the chain length.

For End-Entity certificates, if the basicConstraints extension is present, it SHALL be flagged critical, SHALL have a cA boolean value of FALSE, and SHALL NOT contain a pathLenConstraint ASN.1 sequence. An End-Entity certificate SHALL be rejected if a pathLenConstraint ASN.1 sequence is either present with an Integer value, or present with a null value.

In order to facilitate future flexibility in OCF-compliant PKI implementations, all OCF-compliant Root CA certificates SHALL NOT contain a pathLenConstraint. This allows additional tiers of Intermediate CAs to be implemented in the future without changing the Root CA trust anchors, should such a requirement emerge.

- keyUsage

For all certificates, Devices shall verify that the key usage extension is present and flagged critical.

For Root and Intermediate CA certificates, ONLY the keyCertSign(5) and crlSign(6) bits SHALL be asserted.

For End-Entity certificates, ONLY the digitalSignature(0) and keyAgreement(4) bits SHALL be asserted.

- extendedKeyUsage:

Any End-Entity certificate containing the anyExtendedKeyUsage OID (2.5.29.37.0) SHALL be rejected.

OIDs for serverAuthentication (1.3.6.1.5.5.7.3.1) and clientAuthentication (1.3.6.1.5.5.7.3.2) are required for compatibility with various TLS implementations.

At this time, an End-Entity certificate cannot be used for both Identity (1.3.6.1.4.1.44924.1.6) and Role (1.3.6.1.4.1.44924.1.7) purposes. Therefore, exactly one of the two OIDs SHALL be present and End-Entity certificates with EKU extensions containing both OIDs SHALL be rejected.
End-Entity certificates which chain to an OCF Root CA SHOULD contain at least one PolicyIdentifierId set to the OCF Certificate Policy OID – (1.3.6.1.4.1.51414.0.1.2) corresponding to the version of the OCF Certificate Policy under which it was issued. Additional manufacturer-specific CP OIDs may also be populated.

10.5 Device Authentication with OCF Cloud

10.5.1 Device Authentication with OCF Cloud General

The mechanisms for Device Authentication in clauses 10.2, 10.3 and 10.4 imply that a Device is authorized to communicate with any other Device meeting the criteria provisioned in ",/oic/sec/cred"; the ",/oic/sec/acl2" Resource (or ",/oic/sec/acl1" resource of OIC1.1 Servers) are additionally used to restrict access to specific Resources. The present clause describes Device authentication for OCF Cloud, which uses slightly different criteria as described in clause 5. A Device accessing an OCF Cloud shall establish a TLS session. The mutual authenticated TLS session is established using Server certificate and Client certificate.

Each Device is identified based on the Access Token it is assigned during Device Registration. The OCF Cloud holds an OCF Cloud association table that maps Access Token, User ID and Device ID. The Device Registration shall happen while the Device is in RFNOP state. After Device Registration, the updated Access Token, Device ID and User ID are used by the Device for the subsequent connection with the OCF Cloud.

10.5.2 Device Connection with the OCF Cloud

The Device should establish the TLS connection using the certificate based credential. The connection should be established after Device is provisioned by Mediator.

The TLS session is established between Device and the OCF Cloud as specified in IETF RFC 8323. The OCF Cloud is expected to provide certificate signed by trust anchor that is present in cred entries of the Device. These cred entries are expected to be configured by the Mediator.

The Device shall validate the OCF Cloud's identity based on the credentials that are contained in ",/oic/sec/cred" Resource entries of the Device.

The OCF Cloud is expected to validate the manufacturer certificate provided by the Device.

The assumption is that the OCF Cloud User trusts the OCF Cloud that the Device connects. The OCF Cloud connection should not happen without the consent of the OCF Cloud User. The assumption is that the OCF Cloud User has either service agreement with the OCF Cloud provider or uses manufacturer provided OCF Cloud.

If authentication fails, the "clec" Property of "oic.r.coapcloudconf" Resource on the Device shall be updated about the failed state, if it is supported by the Device. If authentication succeeds, the Device and OCF Cloud should establish an encrypted link in accordance with the negotiated cipher suite.

Figure 33 depicts sequence for Device connection with OCF Cloud and steps described in Table 22.
10.5.3 Security Considerations

When an OCF Server receives a request sent via the OCF Cloud, then the OCF Server permits that request using the identity of the OCF Cloud rather than the identity of the OCF Client. If there is no mechanism through which the OCF Cloud permits only those interactions which the user intends between OCF Clients and OCF Server via the OCF Cloud, and denies all other interactions, then OCF Clients might get elevated privileges by submitting a request via the OCF Cloud. This is highly undesirable from the security perspective. Consequently, OCF Cloud implementations are expected to provide some mechanism through which the OCF Cloud prevents OCF Clients getting elevated privileges when submitting a request via the OCF Cloud. In the present document release, the details of the mechanism are left to the implementation.
The security considerations about the manufacturer certificate as described in 7.3.6.5 are also applicable in the Device authentication with the OCF Cloud.

The Device should validate the OCF Cloud's TLS certificate as defined by IETF RFC 6125 and in accordance with its requirements for Server identity authentication.

The "uid" and "di" Property Value of "/oic/d" Resource may be considered personally identifiable information in some regulatory regions, and the OCF Cloud is expected to provide protections appropriate to its governing regulatory bodies.
11 Message Integrity and Confidentiality

11.1 Preamble
Secured communications between Clients and Servers are protected against eavesdropping, tampering, or message replay, using security mechanisms that provide message confidentiality and integrity.

11.2 Session Protection with DTLS
11.2.1 DTLS Protection General
Devices shall support DTLS for secured communications as defined in IETF RFC 6347. Devices using TCP shall support TLS v1.2 for secured communications as defined in IETF RFC 5246. See 11.3 for a list of required and optional cipher suites for message communication.

OCF Devices MUST support (D)TLS version 1.2 or greater and MUST NOT support versions 1.1 or lower.

Multicast session semantics are not yet defined in this version of the security document.

11.2.2 Unicast Session Semantics
For unicast messages between a Client and a Server, both Devices shall authenticate each other. See clause 10 for details on Device Authentication.

Secured unicast messages between a Client and a Server shall employ a cipher suite from 11.3. The sending Device shall encrypt and authenticate messages as defined by the selected cipher suite and the receiving Device shall verify and decrypt the messages before processing them.

11.2.3 Cloud Session Semantics
The messages between the OCF Cloud and Device shall be exchanged only if the Device and OCF Cloud authenticate each other as described in 10.4.3. The asymmetric cipher suites as described in 11.3.5 shall be employed for establishing a secured session and for encrypting/decrypting between the OCF Cloud and the Device. The OCF Endpoint sending the message shall encrypt and authenticate the message using the cipher suite as described in 11.3.5 and the OCF Endpoint shall verify and decrypt the message before processing it.

11.3 Cipher Suites
11.3.1 Cipher Suites General
The cipher suites allowed for use can vary depending on the context. This clause lists the cipher suites allowed during ownership transfer and normal operation. The following RFCs provide additional information about the cipher suites used in OCF.

IETF RFC 4279: Specifies use of pre-shared keys (PSK) in (D)TLS
IETF RFC 4492: Specifies use of elliptic curve cryptography in (D)TLS
IETF RFC 5489: Specifies use of cipher suites that use elliptic curve Diffie-Hellman (ECDHE) and PSKs
IETF RFC 6655 and IETF RFC 7251: Specifies AES-CCM mode cipher suites, with ECDHE

11.3.2 Cipher Suites for Device Ownership Transfer
11.3.2.1 Just Works Method Cipher Suites
The Just Works OTM may use the following (D)TLS cipher suites.

TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256,
All Devices supporting Just Works OTM shall implement:

**TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256** (with the value 0xFF00)

All Devices supporting Just Works OTM should implement:

**TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256** (with the value 0xFF01)

### 11.3.2.2 Random PIN Method Cipher Suites

The Random PIN Based OTM may use the following (D)TLS cipher suites.

**TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256**, **TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA256**

All Devices supporting Random Pin Based OTM shall implement:

**TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256**

### 11.3.2.3 Certificate Method Cipher Suites

The Manufacturer Certificate Based OTM may use the following (D)TLS cipher suites.

**TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8**, **TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8**, **TLS_ECDHE_ECDSA_WITH_AES_128_CCM**, **TLS_ECDHE_ECDSA_WITH_AES_256_CCM**

Using the following curve:

secp256r1 (See IETF RFC 4492)

All Devices supporting Manufacturer Certificate Based OTM shall implement:

**TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8**

Devices supporting Manufacturer Certificate Based OTM should implement:

**TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8**, **TLS_ECDHE_ECDSA_WITH_AES_128_CCM**, **TLS_ECDHE_ECDSA_WITH_AES_256_CCM**

### 11.3.3 Cipher Suites for Symmetric Keys

The following cipher suites are defined for (D)TLS communication using PSKs:

**TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256**, **TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA256**

**TLS_PSK_WITH_AES_128_CCM_8**, *8 OCTET Authentication tag*  
**TLS_PSK_WITH_AES_256_CCM_8**,  
**TLS_PSK_WITH_AES_128_CCM,** *16 OCTET Authentication tag*  
**TLS_PSK_WITH_AES_256_CCM**

All CCM based cipher suites also use HMAC-SHA-256 for authentication.

All Devices shall implement the following:
Devices should implement the following:

**11.3.4 Cipher Suites for Asymmetric Credentials**

The following cipher suites are defined for (D)TLS communication with asymmetric keys or certificates:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256

Using the following curve:

- secp256r1 (See IETF RFC 4492)

All Devices supporting Asymmetric Credentials shall implement:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256

**11.3.5 Cipher Suites for OCF Cloud Credentials**

The following cipher suites are defined for TLS communication with certificates:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256

All Devices supporting OCF Cloud Certificate Credentials shall implement:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
12 Access Control

12.1 ACL Generation and Management

This clause will be expanded in a future version of the document.

12.2 ACL Evaluation and Enforcement

12.2.1 ACL Evaluation and Enforcement General

The Server enforces access control over application Resources before exposing them to the requestor. The Security Layer in the Server authenticates the requestor when access is received via the secure port. Authenticated requestors, known as the "subject" can be used to match ACL entries that specify the requestor's identity, role or may match authenticated requestors using a subject wildcard.

If the request arrives over the unsecured port, the only ACL policies allowed are those that use a subject wildcard match of anonymous requestors.

Access is denied if a requested Resource is not matched by an ACL entry.

NOTE There are documented exceptions pertaining to Device onboarding where access to Security Virtual Resources may be granted prior to provisioning of ACL Resources.

The second generation ACL (i.e. "/oic/sec/acl2") contains an array of Access Control Entries (ACE2) that employ a Resource matching algorithm that 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 (see clause 13) to the requested Resource. Resources are matched in two ways:

1) host reference (href)
2) resource wildcard (wc).

12.2.2 Host Reference Matching

When present in an ACE2 matching element, the Host Reference (href) Property shall be used for Resource matching.

– The href Property shall be used to find an exact match of the Resource name if present.

12.2.3 Resource Wildcard Matching

When present, a wildcard (wc) expression shall be used to match multiple Resources using a wildcard Property contained in the "oic.sec.ace2.resource-ref" structure.

A wildcard expression may be used to match multiple Resources using a wildcard Property contained in the "oic.sec.ace2.resource-ref" structure. The wildcard matching strings are defined in Table 23.

Table 23 – ACE2 Wildcard Matching Strings Description

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;+&quot;</td>
<td>Shall match all Discoverable Non-Configuration Resources which expose at least one Secure OCF Endpoint.</td>
</tr>
<tr>
<td>&quot;.-&quot;</td>
<td>Shall match all Discoverable Non-Configuration Resources which expose at least one Unsecure OCF Endpoint.</td>
</tr>
<tr>
<td>***</td>
<td>Shall match all Non-Configuration Resources.</td>
</tr>
</tbody>
</table>

NOTE Discoverable resources appear in the "/oic/res" Resource, while non-discoverable resources may appear in other collection resources but do not appear in the /res collection.
12.2.4 Multiple Criteria Matching

If the ACE2 "resources" Property contains multiple entries, then a logical OR shall be applied for each array element. For example, if a first array element of the "resources" Property contains "href="/a/light" and the second array element of the "resources" Property contains "href="/a/led", then Resources that match either of the two "href" criteria shall be included in the set of matched Resources.

Example 1 JSON for Resource matching

```json
{
  "resources": [  
    {  
      "href": "/x/door1"
    },  
    {  
      "href": "/x/door2"
    }
  ]
}
```

Example 2 JSON for Resource matching

```json
{
  "resources": [  
    {  
      "wc": "*"
    }
  ]
}
```

12.2.5 Subject Matching using Wildcards

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.

Examples: JSON for subject wildcard matching

```json
//matches all subjects that have authenticated and confidentiality protections in place.
"subject": {
  "conntype": "auth-crypt"
}

//matches all subjects that have NOT authenticated and have NO confidentiality protections in place.
"subject": {
  "conntype": "anon-clear"
}
```

12.2.6 Subject Matching using Roles

When the ACE subject is specified as a role, a requestor shall be matched if either:

1) The requestor authenticated with a symmetric key credential, and the role is present in the roleid Property of the credential's entry in the credential resource, or
2) The requestor authenticated with a certificate, and a valid role certificate is present in the roles resource with the requestor's certificate's public key at the time of evaluation. Validating role certificates is defined in 10.3.1.

12.2.7 ACL Evaluation

12.2.7.1 ACE2 matching algorithm

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 Server shall verify the signature, at least once, following update of the "/oic/sec/sacl" Resource.

2) The local "/oic/sec/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.

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.

Batch requests to Resource containing Links require additional considerations when accessing the linked Resources. ACL considerations for batch request to the Atomic Measurement Resource Type are provided in clause 12.2.7.2. ACL considerations for batch request to the Collection Resource Type are provided in 12.2.7.3.

12.2.7.2 ACL considerations for batch request to the Atomic Measurement Resource Type

The present clause shall apply to any Resource Type based on the Atomic Measurement Resource Type.

If an OCF Server receives a batch request to an Atomic Measurement Resource containing only local references and there is an ACE matching the Atomic Measurement Resource which permits the request, then the corresponding requests to the linked Resources of the Atomic Measurement Resource shall be permitted by the OCF Server. That is, the request to each linked Resource is permitted regardless of whether there is an ACE configured on the OCF Server which would permit a corresponding request from the OCF Client (which sent the batch request to the Atomic Measurement Resource) addressing the linked Resource.

12.2.7.3 ACL considerations for batch request to the Collection Resource Type

The present clause shall apply to any Resource Type based on the Collection Resource Type.

If an OCF Server receives a batch request to a Collection Resource containing only local references and there is an ACE matching the Collection Resource which permits the request, then the corresponding requests to the linked Resources of the Collection Resource shall be permitted by the OCF Server. That is, the request to each linked Resource is permitted regardless of whether there is an ACE configured on the OCF Server which would permit a corresponding request from the OCF Client (which sent the batch request to the Collection Resource) addressing the linked Resource.
13 Security Resources

13.1 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 34 – OCF Security Resources
Figure 35 – "/oic/sec/cred" Resource and Properties

Figure 36 – "/oic/sec/acl2" Resource and Properties
13.2 Device Owner Transfer Resource

13.2.1 Device Owner Transfer Resource General

The "/oic/sec/doxm" Resource contains the set of supported Device OTMs.

Resource discovery processing respects the CRUDN constraints supplied as part of the security
Resource definitions contained in this document.

"/oic/sec/doxm" Resource is defined in Table 24.
Table 24 – Definition of the "/oic/sec/doxm" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/doxm</td>
<td>Device OTMs</td>
<td>oic.r.doxm</td>
<td>oic.if.baselin e</td>
<td>Resource for supporting Device owner transfer</td>
<td>Configuration</td>
</tr>
</tbody>
</table>

Table 25 defines the Properties of the "/oic/sec/doxm" Resource.

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

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Device State</th>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTM Selection</td>
<td>oxmsel</td>
<td>oic.sec.doxmtype</td>
<td>UINT16</td>
<td>Yes</td>
<td>RESET</td>
<td>RW</td>
<td>DOTS shall set to its selected DOTS and both parties execute the DOTS. After secure owner transfer session is established DOTS shall update the oxmsel again making it permanent. If the DOTS fails the Server shall transition device state to RESET.</td>
</tr>
<tr>
<td>Supported</td>
<td>sct</td>
<td>oic.sec.credtype</td>
<td>bitmask</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
<td>Server shall set to (4) &quot;oic.sec.oxm.self&quot;</td>
</tr>
<tr>
<td>Device Ownership Status</td>
<td>owned</td>
<td>Boolean</td>
<td>T</td>
<td>F</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
</tr>
<tr>
<td>Device UUID</td>
<td>deviceuuid</td>
<td>String</td>
<td>oic.sec.didt</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
<td>Server shall construct a temporary random UUID that differs for each transition to RESET.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>DOTS shall update to a value it has selected after secure owner transfer session is established. If update fails with error PROPERTY NOT_FOUND the DOTS shall either accept the Server provided value or update /doxm.owned=FALSE and terminate the session.</td>
</tr>
</tbody>
</table>

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
Table 26 - Properties of the "/oic/sec/didtype" Property

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Device State</th>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>devowneruuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
<td>Server shall set to the nil uuid value (e.g. &quot;00000000-0000-0000-0000-000000000000&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM</td>
<td>RW</td>
<td>DOTS shall set value after secure owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO</td>
<td>R</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP</td>
<td>R</td>
<td>n/a</td>
</tr>
</tbody>
</table>

| Resource Owner Id | rowneruuid    | String     | uuid       | Yes       | RESET        | R           | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000") |
|                  |               |            |            |           | RFOTM        | RW          | The DOTS shall configure the rowneruuid Property when a successful owner transfer session is established. |
|                  |               |            |            |           | RFPRO        | R           | n/a         |
|                  |               |            |            |           | RFNOP        | R           | n/a         |

SRESET RW The DOTS (referenced via devowneruuid Property) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the rowneruuid does not refer to a valid DOTS device identifier the Server shall transition to RESET Device state.

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

The oxms Property contains a list of OTM where the entries appear in the order of preference. This Property contains the higher priority methods appearing before the lower priority methods. The DOTS queries this list at the time of onboarding and selects the most appropriate method.

The DOTS shall update the oxmsel Property of the "/oic/sec/doxm" Resource with the OTM that was used to onboard the Device.

OTMs consist of two parts, a URI identifying the vendor or organization and the specific method.

<DoxmType> ::= <NSS>
(NSS) ::= <Identifier> | {{<NID>"."} <NameSpaceQualifier> "."} <Method>
(NID) ::= <Vendor-or-Organization>
IDENTGER
(NameSpaceQualifier) ::= String
(Method) ::= String
(Vendor-Organization) ::= String

When an OTM successfully completes, the owned Property is set to "1" (TRUE). Consequently, subsequent attempts to take ownership of the Device will fail.

The Server shall expose a persistent or semi-persistent a deviceuuid Property that is stored in the "/oic/sec/doxm" Resource when the devowneruuid Property of the "/oic/sec/doxm" Resource is UPDATED to non-nil UUID value.
The DOTS should RETRIEVE the updated deviceuuid Property of the "/oic/sec/doxm" Resource after it has updated the devowneruuid Property value of the "/oic/sec/doxm" Resource to a non-nil-UUID value.

The Device vendor shall determine that the Device identifier (deviceuuid) is persistent (not updatable) or that it is non-persistent (updatable by the owner transfer service – aka. DOTS).

If the deviceuuid Property of "/oic/sec/doxm" Resource is persistent, the request to UPDATE shall fail with the error PROPERTY_NOT_FOUND.

If the deviceuuid Property of the "/oic/sec/doxm" Resource is non-persistent, the request to UPDATE shall succeed and the value supplied by DOTS shall be remembered until the device is RESET. If the UPDATE to deviceuuid Property of the "/oic/sec/doxm" Resource fails while in the RFOTM Device state the device state shall transition to RESET where the Server shall set the value of the deviceuuid Property of the "/oic/sec/doxm" Resource to the nil-UUID (e.g. "00000000-0000-0000-0000-000000000000").

Regardless of whether the device has a persistent or semi-persistent deviceuuid Property of the "/oic/sec/doxm" Resource, a temporary random UUID is exposed by the Server via the deviceuuid Property of the "/oic/sec/doxm" Resource each time the device enters RESET Device state. The temporary deviceuuid value is used while the device state is in the RESET state and while in the RFOTM device state until the DOTS establishes a secure OTM connection. The DOTS should RETRIEVE the updated deviceuuid Property value of the "/oic/sec/doxm" Resource after it has updated devowneruuid Property value of the "/oic/sec/doxm" Resource to a non-nil-UUID value.

The deviceuuid Property of the "/oic/sec/doxm" Resource shall expose a persistent value (i.e. is not updatable via an OCF Interface) or a semi-persistent value (i.e. is updatable by the DOTS via an OCF Interface to the deviceuuid Property of the "/oic/sec/doxm" Resource during RFOTM Device state.).

This temporary non-repeated value shall be exposed by the Device until the DOTS establishes a secure OTM connection and UPDATES the devowneruuid Property to a non-nil UUID value. Subsequently, (while in RFPRO, RFNOP and SRESET Device states) the deviceuuid Property of the "/oic/sec/doxm" Resource shall reveal the persistent or semi-persistent value to authenticated requestors and shall reveal the temporary non-repeated value to unauthenticated requestors.

See 13.16 for additional details related to privacy sensitive considerations.

### 13.2.2 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"

2) "di" Property of "/oic/d"

3) "piid" Property of "/oic/d"

4) "pi" Property of "/oic/p"

### 13.2.3 Onboarding Considerations for Device Identifier

The deviceuuid is used to onboard the Device. The other identifiers (di, piid and pi) are not essential for onboarding. The onboarding service (aka DOTS) may not know a priori whether the Device to be onboarded is using persistent or semi-persistent identifiers. An OCF Security Domain owner may have a preference for persistent or semi-persistent device identifiers. Detecting whether the Device is using persistent or semi-persistent deviceuuid can be achieved by attempting to update it.
If the "deviceuuid" Property of the "/oic/sec/doxm" Resource is persistent, then an UPDATE request, at the appropriate time during onboarding shall fail with an appropriate error response.

The appropriate time to attempt to update deviceuuid during onboarding exists when the Device state is RFOTM and when devowneruuid Property value of the "/oic/sec/doxm" Resource has a non-nil UUID value.

If the "deviceuuid" Property of the "/oic/sec/doxm" Resource is semi-persistent, subsequent to a successful UPDATE request to change it; the Device shall remember the semi-persistent value until the next successful UPDATE request or until the Device state transitions to RESET.

See 13.16 for addition behaviour regarding "deviceuuid".

### 13.2.4 OCF defined OTMs

Table 27 defines the Properties of the "oic.sec.doxmtype".

<p>| Table 27 – Properties of the &quot;oic.sec.doxmtype&quot; Property |
|----------------------------------|----------------|----------------|----------------|</p>
<table>
<thead>
<tr>
<th>Value Type Name</th>
<th>Value TypeURN</th>
<th>Enumeration Value (mandatory)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCFJustWorks</td>
<td>oic.sec.doxm.jw 0</td>
<td>The just-works method relies on anonymous Diffie-Hellman key agreement protocol to allow an DOTS to assert ownership of the new Device. The first DOTS to make the assertion is accepted as the Device owner. The just-works method results in a shared secret that is used to authenticate the Device to the DOTS and likewise authenticates the DOTS to the Device. The Device allows the DOTS to take ownership of the Device, after which a second attempt to take ownership by a different DOTS will fail.</td>
<td></td>
</tr>
<tr>
<td>OCFSharedPin</td>
<td>oic.sec.doxm.rdp 1</td>
<td>The new Device randomly generates a PIN that is communicated via an out-of-band channel to a DOTS. An in-band Diffie-Hellman key agreement protocol establishes that both endpoints possess the PIN. Possession of the PIN by the DOTS signals the new Device that device ownership can be asserted.</td>
<td></td>
</tr>
<tr>
<td>OCFMfgCert</td>
<td>oic.sec.doxm.mfgcert 2</td>
<td>The new Device is presumed to have been manufactured with an embedded asymmetric private key that is used to sign a Diffie-Hellman exchange at Device onboarding. The manufacturer certificate should contain Platform hardening information and other security assurances assertions.</td>
<td></td>
</tr>
<tr>
<td>OCF Reserved</td>
<td>&lt;Reserved&gt;</td>
<td>3</td>
<td>Reserved</td>
</tr>
<tr>
<td>OCFSelf</td>
<td>oic.sec.oxm.self 4</td>
<td>The manufacturer shall set the /doxm.oxmsel value to (4). The Server shall reset this value to (4) upon entering RESET Device state.</td>
<td></td>
</tr>
<tr>
<td>OCF Reserved</td>
<td>&lt;Reserved&gt;</td>
<td>5~0xFEFF</td>
<td>Reserved for OCF use</td>
</tr>
<tr>
<td>Vendor-defined Value Type Name</td>
<td>&lt;Reserved&gt; 0xFF00~0xFFFF</td>
<td>Reserved for vendor-specific OTM use</td>
<td></td>
</tr>
</tbody>
</table>

a The just-works method is subject to a man-in-the-middle attacker. Precautions should be taken to provide physical security when this method is used.
13.3 Credential Resource

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

"oic.r.cred" Resource is defined in Table 28.

Table 28 – Definition of the "oic.r.cred" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/cred</td>
<td>Credentials</td>
<td>oic.r.cred</td>
<td>baseline</td>
<td>Resource containing credentials for Device authentication, verification and data protection</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 29 defines the Properties of the "/oic/sec/cred" Resource.
Table 29 – Properties of the "/oic/sec/cred" Resource

<table>
<thead>
<tr>
<th>Property</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Device State</th>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>creds</td>
<td>/oic/sec/cred</td>
<td>array</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
<td>Server shall set to manufacturer defaults.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM</td>
<td>RW</td>
<td>Set by DOTS after successful OTM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO</td>
<td>RW</td>
<td>Set by the CMS (referenced via the rowneruuid Property of &quot;/oic/sec/cred&quot; Resource) after successful authentication. Access to NCRs is prohibited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP</td>
<td>R</td>
<td>Access to NCRs is permitted after a matching ACE is found.</td>
</tr>
<tr>
<td>Resource Owner ID</td>
<td>rowneruuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>RESET</td>
<td>R</td>
<td>Server shall set to the nil uuid value (e.g. &quot;00000000-0000-0000-0000-000000000000&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM</td>
<td>RW</td>
<td>The DOTS shall configure the rowneruuid Property of &quot;/oic/sec/DOXM&quot; Resource when a successful owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO</td>
<td>R</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP</td>
<td>R</td>
<td>n/a</td>
</tr>
</tbody>
</table>

All secure Device accesses shall have a "/oic/sec/cred" Resource that protects the end-to-end interaction.

The "/oic/sec/cred" Resource shall be updateable by the service named in its rowneruuid Property.

ACLs naming "/oic/sec/cred" Resource should further restrict access beyond CRUDN access modes.

Table 30 defines the Properties of "oic.sec.cred".
### Table 30 – Properties of the "oic.sec.cred" Property

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Access Mode</th>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential ID</td>
<td>credid</td>
<td>UINT16</td>
<td>0 – 64K</td>
<td>Yes</td>
<td>RW</td>
<td></td>
<td>Short credential ID for local references from other Resource</td>
</tr>
<tr>
<td>Subject UUID</td>
<td>subjectuuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>RW</td>
<td></td>
<td>A uuid that identifies the subject to which this credential applies or &quot;*&quot; if any identity is acceptable</td>
</tr>
<tr>
<td>Role ID</td>
<td>roleid</td>
<td>oic.sec.roletyp</td>
<td></td>
<td>No</td>
<td>RW</td>
<td></td>
<td>Identifies the role(s) the subject is authorized to assert.</td>
</tr>
<tr>
<td>Credential Type</td>
<td>credtype</td>
<td>oic.sec.credtyp</td>
<td>bitmask</td>
<td>Yes</td>
<td>RW</td>
<td></td>
<td>Represents this credential's type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 – Used for testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 – Symmetric pair-wise key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 – Symmetric group key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 – Asymmetric signing key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8 – Asymmetric signing key with certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16 – PIN or password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>32 – Asymmetric encryption key</td>
</tr>
<tr>
<td>Credential Usage</td>
<td>credusage</td>
<td>oic.sec.credusagetype</td>
<td>String</td>
<td>No</td>
<td>RW</td>
<td></td>
<td>Used to resolve undecidability of the credential.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Provides indication for how/where the cred is used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oic.sec.cred.trustca: certificate trust anchor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oic.sec.cred.cert: identity certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oic.sec.cred.rolecert: role certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oic.sec.cred.mfgtrustca: manufacturer certificate trust anchor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>oic.sec.cred.mfgcert: manufacturer certificate</td>
</tr>
<tr>
<td>Public Data</td>
<td>publicdata</td>
<td>oic.sec.pubdatatype</td>
<td>-</td>
<td>No</td>
<td>RW</td>
<td>Public credential information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1:2: ticket, public SKDC values</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4, 32: Public key value</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8: A chain of one or more certificate</td>
<td></td>
</tr>
<tr>
<td>Private Data</td>
<td>privatedata</td>
<td>oic.sec.privdatatype</td>
<td>-</td>
<td>No</td>
<td></td>
<td>Server shall set to manufacturer default</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- RESET</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW RFOTM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>W RFPRO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- RFNOP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>W SRESET</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DOTS may modify to enable transition to RFPRO.</td>
<td></td>
</tr>
<tr>
<td>Optional Data</td>
<td>optionaldata</td>
<td>oic.sec.optdata</td>
<td>-</td>
<td>No</td>
<td>RW</td>
<td>Credential revocation status information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>type</td>
<td></td>
<td></td>
<td></td>
<td>1, 2, 4, 32: revocation status information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8: Revocation information</td>
<td></td>
</tr>
<tr>
<td>Period</td>
<td>period</td>
<td>String</td>
<td></td>
<td>No</td>
<td>RW</td>
<td>Period as defined by IETF RFC 5545. The credential should not be used if the current time is outside the Period window.</td>
<td></td>
</tr>
<tr>
<td>Credential Refresh Method</td>
<td>crms</td>
<td>oic.sec.crmtyp</td>
<td>array</td>
<td>No</td>
<td>RW</td>
<td>Credentials with a Period Property are refreshed using the credential refresh method (crm) according to the type definitions for &quot;oic.sec.crm&quot;.</td>
<td></td>
</tr>
</tbody>
</table>
Table 31 defines the Properties of "oic.sec.credusagetype".

**Table 31: Properties of the "oic.sec.credusagetype" Property**

<table>
<thead>
<tr>
<th>Value Type Name</th>
<th>Value Type URN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Anchor</td>
<td>oic.sec.cred.trustca</td>
</tr>
<tr>
<td>Certificate</td>
<td>oic.sec.cred.cert</td>
</tr>
<tr>
<td>Role Certificate</td>
<td>oic.sec.cred.rolecert</td>
</tr>
<tr>
<td>Manufacturer Trust CA</td>
<td>oic.sec.cred.mfgtrustca</td>
</tr>
<tr>
<td>Manufacturer CA</td>
<td>oic.sec.cred.mfgcert</td>
</tr>
</tbody>
</table>

Table 32 defines the Properties of "oic.sec.pubdatatype".

**Table 32 – Properties of the "oic.sec.pubdatatype" Property**

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encoding format</td>
<td>encoding</td>
<td>String</td>
<td>N/A</td>
<td>RW</td>
<td>No</td>
<td>A string specifying the encoding format of the data contained in the pubdata&lt;br&gt;&quot;oic.sec.encoding.jwt&quot; - IETF RFC 7519 JSON web token (JWT) encoding&lt;br&gt;&quot;oic.sec.encoding.cwt&quot; - IETF RFC 8392 CBOR web token (CWT) encoding&lt;br&gt;&quot;oic.sec.encoding.base64&quot; – Base64 encoding&lt;br&gt;&quot;oic.sec.encoding.uri&quot; – URI reference&lt;br&gt;&quot;oic.sec.encoding.pem&quot; – Encoding for PEM-encoded certificate or chain&lt;br&gt;&quot;oic.sec.encoding.der&quot; – Encoding for DER-encoded certificate or chain&lt;br&gt;&quot;oic.sec.encoding.raw&quot; – Raw hex encoded data</td>
</tr>
<tr>
<td>Data</td>
<td>data</td>
<td>String</td>
<td>N/A</td>
<td>RW</td>
<td>No</td>
<td>The encoded value</td>
</tr>
</tbody>
</table>

Table 33 defines the Properties of "oic.sec.privdatatype".

**Table 33 – Properties of the "oic.sec.privdatatype" Property**

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encoding format</td>
<td>encoding</td>
<td>String</td>
<td>N/A</td>
<td>RW</td>
<td>Yes</td>
<td>A string specifying the encoding format of the data contained in the privdata&lt;br&gt;&quot;oic.sec.encoding.jwt&quot; - IETF RFC 7519 JSON web token (JWT) encoding&lt;br&gt;&quot;oic.sec.encoding.cwt&quot; - IETF RFC 8392 CBOR web token (CWT) encoding&lt;br&gt;&quot;oic.sec.encoding.base64&quot; – Base64 encoding&lt;br&gt;&quot;oic.sec.encoding.uri&quot; – URI reference&lt;br&gt;&quot;oic.sec.encoding.pem&quot; – Encoding for PEM-encoded certificate or chain&lt;br&gt;&quot;oic.sec.encoding.der&quot; – Encoding for DER-encoded certificate or chain&lt;br&gt;&quot;oic.sec.encoding.raw&quot; – Raw hex encoded data</td>
</tr>
<tr>
<td>Data</td>
<td>data</td>
<td>String</td>
<td>N/A</td>
<td>W</td>
<td>No</td>
<td>The encoded value&lt;br&gt;This value shall not be RETRIEVE-able.</td>
</tr>
<tr>
<td>Handle</td>
<td>handle</td>
<td>UINT16</td>
<td>N/A</td>
<td>RW</td>
<td>No</td>
<td>Handle to a key storage resource</td>
</tr>
</tbody>
</table>
Table 34 defines the Properties of "oic.sec.optdatatype".

Table 34 – Properties of the "oic.sec.optdatatype" Property

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocation status</td>
<td>revstat</td>
<td>Boolean</td>
<td>T</td>
<td>F</td>
<td>RW</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Revocation status flag</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>True – revoked</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>False – not revoked</td>
</tr>
<tr>
<td>Encoding format</td>
<td>encoding</td>
<td>String</td>
<td>N/A</td>
<td>RW</td>
<td>No</td>
<td>A string specifying the encoding format of the data contained in the optdata</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.jwt&quot; – IETF RFC 7519 JSON web token (JWT) encoding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.cwt&quot; - IETF RFC 8392 CBOR web token (CWT) encoding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.base64&quot; – Base64 encoding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.pem&quot; – Encoding for PEM-encoded certificate or chain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.der&quot; – Encoding for DER-encoded certificate or chain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.encoding.raw&quot; – Raw hex encoded data</td>
</tr>
<tr>
<td>Data</td>
<td>data</td>
<td>String</td>
<td>N/A</td>
<td>RW</td>
<td>No</td>
<td>The encoded structure</td>
</tr>
</tbody>
</table>

Table 35 defines the Properties of "oic.sec.roletype".

Table 35 – Definition of the "oic.sec.roletype" Property.

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>authority</td>
<td>String</td>
<td>N/A</td>
<td>R</td>
<td>No</td>
<td>A name for the authority that defined the role. If not present, the credential issuer defined the role. If present, must be expressible as an ASN.1 PrintableString.</td>
</tr>
<tr>
<td>Role</td>
<td>role</td>
<td>String</td>
<td>N/A</td>
<td>R</td>
<td>Yes</td>
<td>An identifier for the role. Must be expressible as an ASN.1 PrintableString.</td>
</tr>
</tbody>
</table>

13.3.2 Properties of the Credential Resource

13.3.2.1 Credential ID

Credential ID (credid) is a local reference to an entry in a creds Property array of the "oic/sec/cred" Resource. The SRM generates it. The credid Property shall be used to disambiguate array elements of the creds Property.

13.3.2.2 Subject UUID

The subjectuuid Property identifies the Device to which an entry in a creds Property array of the "oic/sec/cred" Resource shall be used to establish a secure session, verify an authentication challenge-response or to authenticate an authentication challenge.

A subjectuuid Property that matches the Server’s own deviceuuid Property, distinguishes the array entries in the creds Property that pertain to this Device.

The subjectuuid Property shall be used to identify a group to which a group key is used to protect shared data.
When certificate chain is used during secure connection establishment, the "subjectuuid" Property shall also be used to verify the identity of the responder. The presented certificate chain shall be accepted, if there is a matching Credential entry on the Device that satisfies all of the following:

- Public Data of the entry contains trust anchor (root) of the presented chain.
- Subject UUID of the entry matches UUID in the Common Name field of the End-Entity certificate in the presented chain. If Subject UUID of the entry is set as a wildcard "+", this condition is automatically satisfied.
- Credential Usage of the entry is "oic.sec.cred.trustca".

13.3.2.3 Role ID

The roleid Property identifies a role that has been granted to the credential.

13.3.2.4 Credential Type

The credtype Property is used to interpret several of the other Property values whose contents can differ depending on credential type. These Properties include publicdata, privatedata and optionaldata. The credtype Property value of "0" ("no security mode") is reserved for testing and debugging circumstances. Production deployments shall not allow provisioning of credentials of type "0". The SRM should introduce checking code that prevents its use in production deployments.

13.3.2.5 Public Data

The publicdata Property contains information that provides additional context surrounding the issuance of the credential. For example, it might contain information included in a certificate or response data from a CMS. It might contain wrapped data.

13.3.2.6 Private Data

The privatedata Property contains secret information that is used to authenticate a Device, protect data or verify an authentication challenge-response.

The privatedata Property shall not be disclosed outside of the SRM’s trusted computing perimeter. A secure element (SE) or trusted execution environment (TEE) should be used to implement the SRM’s trusted computing perimeter. The privatedata contents may be referenced using a handle; for example, if used with a secure storage sub-system.

13.3.2.7 Optional Data

The optionaldata Property contains information that is optionally supplied, but facilitates key management, scalability or performance optimization.

13.3.2.8 Period

The period Property identifies the validity period for the credential. If no validity period is specified, the credential lifetime is undetermined. Constrained devices that do not implement a date-time capability shall obtain current date-time information from its CMS.

13.3.2.9 Credential Refresh Method Type Definition

The CMS shall implement the credential refresh methods specified in the crms Property of the "oic.sec.creds" array in the "/oic/sec/cred" Resource.

Table 36 defines the values of "oic.sec.cmttype".
### Table 36 – Value Definition of the "oic.sec.crmtype" Property

<table>
<thead>
<tr>
<th>Value Type Name</th>
<th>Value Type URN</th>
<th>Applicable Credential Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Service</td>
<td>oic.sec.crm.pro</td>
<td>All</td>
<td>A CMS initiates re-issuance of credentials nearing expiration. The Server should delete expired credentials to manage storage resources. The Resource Owner Property references the provisioning service. The Server uses its &quot;/oic/sec/cred.rowneruuid&quot; Resource to identify additional key management service that supports this credential refresh method.</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>oic.sec.crm.psk</td>
<td>[1]</td>
<td>The Server performs ad-hoc key refresh by initiating a DTLS connection with the Device prior to credential expiration using a Diffie-Hellman based ciphersuite and the current PSK. The new DTLS MasterSecret value becomes the new PSK. The Server selects the new validity period. The new validity period value is sent to the Device who updates the validity period for the current credential. The Device acknowledges this update by returning a successful response or denies the update by returning a failure response. The Server uses its &quot;/oic/sec/cred.rowneruuid&quot; Resource to identify a key management service that supports this credential refresh method.</td>
</tr>
</tbody>
</table>
| Random PIN           | oic.sec.crm.rdp | [16]                      | The Server performs ad-hoc key refresh following the "oic.sec.crm.psk" approach, but in addition generates a random PIN value that is communicated out-of-band to the remote Device. The current PSK + PIN are hashed to form a new PSK' that is used with the DTLS ciphersuite. I.e. PSK' = SHA256(PSK, PIN). The Server uses its "/oic/sec/cred.rowneruuid" Resource to identify a key management service that supports this credential refresh method. **
| SKDC                 | oic.sec.crm.skdc| [1, 2, 4, 32]              | The Server issues a request to obtain a ticket for the Device. The Server updates the credential using the information contained in the response to the ticket request. The Server uses its "/oic/sec/cred.rowneruuid" Resource to identify the key management service that supports this credential refresh method. The Server uses its "/oic/sec/cred.rowneruuid" Resource to identify a key management service that supports this credential refresh method. **
| PKCS10               | oic.sec.crm.pk10| [8]                       | The Server issues a PKCS#10 certificate request message to obtain a new certificate. The Server uses its "/oic/sec/cred.rowneruuid" Resource to identify the key management service that supports this credential refresh method. The Server uses its "/oic/sec/cred.rowneruuid" Resource to identify a key management service that supports this credential refresh method. **

### 13.3.2.10 Credential Usage

Credential Usage indicates to the Device the circumstances in which a credential should be used. Five values are defined:

- oic.sec.cred.trustca: This certificate is a trust anchor for the purposes of certificate chain validation, as defined in 10.3.
- oic.sec.cred.cert: This credusage is used for certificates for which the Device possesses the private key and uses it for identity authentication in a secure session, as defined in clause 10.4.
- oic.sec.cred.rolecert: This credusage is used for certificates for which the Device possesses the private key and uses to assert one or more roles, as defined in clause 10.4.2.
- oic.sec.cred.mfgtrustca: This certificate is a trust anchor for the purposes of the Manufacturer Certificate Based OTM as defined in clause 7.3.6.
– oic.sec.cred.mfgcert: This certificate is used for certificates for which the Device possesses the private key and uses it for authentication in the Manufacturer Certificate Based OTM as defined in clause 7.3.6.

13.3.3 Key Formatting

13.3.3.1 Symmetric Key Formatting

Symmetric keys shall have the format described in Table 37 and Table 38.

### Table 37 – 128-bit symmetric key

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>16</td>
<td>OCTET</td>
<td>Specifies the number of 8-bit octets following Length</td>
</tr>
<tr>
<td>Key</td>
<td>opaque</td>
<td>OCTET Array</td>
<td>16-byte array of octets. When used as input to a PSK function Length is omitted.</td>
</tr>
</tbody>
</table>

### Table 38 – 256-bit symmetric key

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>32</td>
<td>OCTET</td>
<td>Specifies the number of 8-bit octets following Length</td>
</tr>
<tr>
<td>Key</td>
<td>opaque</td>
<td>OCTET Array</td>
<td>32-byte array of octets. When used as input to a PSK function Length is omitted.</td>
</tr>
</tbody>
</table>

13.3.3.2 Asymmetric Keys

Asymmetric key formatting is not available in this revision of the document.

13.3.3.3 Asymmetric Keys with Certificate

Key formatting is defined by certificate definition.

13.3.3.4 Passwords

Password formatting is not available in this revision of the document.

13.3.4 Credential Refresh Method Details

13.3.4.1 Provisioning Service

The resource owner identifies the provisioning service. If the Server determines a credential requires refresh and the other methods do not apply or fail, the Server will request re-provisioning of the credential before expiration. If the credential is allowed to expire, the Server should delete the Resource.

13.3.4.2 Pre-Shared Key

13.3.4.2.1 Pre-Shared Key General

Using this mode, the current PSK is used to establish a Diffie-Hellman session key in DTLS. The TLS_PRF is used as the key derivation function (KDF) that produces the new (refreshed) PSK.

PSK = TLS_PRF(MasterSecret, Message, length);

– MasterSecret – is the MasterSecret value resulting from the DTLS handshake using one of the above ciphersuites.

– Message is the concatenation of the following values:

  – RM - Refresh method – i.e. "oic.sec.crm.psk"
- Device ID_A is the string representation of the Device ID that supplied the DTLS ClientHello.

- Device ID_B is the Device responding to the DTLS ClientHello message

Length of Message in bytes.

Both Server and Client use the PSK to update the "/oic/sec/cred" Resource's privatedata Property. If Server initiated the credential refresh, it selects the new validity period. The Server sends the chosen validity period to the Client over the newly established DTLS session so it can update the corresponding credential Resource for the Server.

### 13.3.4.2.2 Random PIN

Using this mode, the current unexpired PIN is used to generate a PSK following IETF RFC 2898. The PSK is used during the Diffie-Hellman exchange to produce a new session key. The session key should be used to switch from PIN to PSK mode.

The PIN is randomly generated by the Server and communicated to the Client through an out-of-band method. The OOB method used is out-of-scope.

The pseudo-random function (PBKDF2) defined by IETF RFC 2898. PIN is a shared value used to generate a pre-shared key. The PIN-authenticated pre-shared key (PPSK) is supplied to a DTLS ciphersuite that accepts a PSK.

$$PPSK = PBKDF2(PR, PIN, RM, Device ID, c, dkLen)$$

The PBKDF2 function has the following parameters:

- PRF – Uses the DTLS PRF.
- PIN – Shared between Devices.
- RM - Refresh method – I.e. "oic.sec.crm.rdp"
- Device ID – UUID of the new Device.
- c – Iteration count initialized to 1000, incremented upon each use.
- dkLen – Desired length of the derived PSK in octets.

Both Server and Client use the PPSK to update the "/oic/sec/cred" Resource’s PrivateData Property. If Server initiated the credential refresh, it selects the new validity period. The Server sends the chosen validity period to the Client over the newly established DTLS session so it can update its corresponding credential Resource for the Server.

### 13.3.4.2.3 SKDC

A DTLS session is opened to the Server where the "/oic/sec/cred" Resource has an owneruuid Property value that matches a CMS that implements SKDC functionality and where the Client credential entry supports the oic.sec.crm.skdc credential refresh method. A ticket request message is delivered to the CMS and in response returns the ticket request. The Server updates or instantiates an "/oic/sec/cred" Resource guided by the ticket response contents.

### 13.3.4.2.4 PKCS10

A DTLS session is opened to the Server where the "/oic/sec/cred" Resource has an owneruuid Property value that matches a CMS that supports the oic.sec.crm.pk10 credential refresh method. A PKCS10 formatted message is delivered to the service. After the refreshed certificate is issued, the CMS pushes the certificate to the Server. The Server updates or instantiates an "/oic/sec/cred" Resource guided by the certificate contents.
13.3.4.3 Resource Owner

The Resource Owner Property allows credential provisioning to occur soon after Device onboarding before access to support services has been established. It identifies the entity authorized to manage the "/oic/sec/cred" Resource in response to Device recovery situations.

13.4 Certificate Revocation List

13.4.1 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.r.crl" Resource is defined in Table 39.

Table 39 – Definition of the "oic.r.crl" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/crl</td>
<td>CRLs</td>
<td>oic.r.crl</td>
<td>baseline</td>
<td>Resource containing CRLs for Device certificate revocation</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 40 defines the Properties of "oic.r.crl".

Table 40 – Properties of the "oic.r.crl" Resource

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

13.5 ACL Resources

13.5.1 ACL Resources General

All Resource hosted by a Server are required to match an ACL policy. ACL policies can be expressed using three ACL Resource Types: "/oic/sec/acl2", "/oic/sec/amacl" and "/oic/sec/sacl". The subject (e.g. deviceuuid of the Client) requesting access to a Resource shall be authenticated prior to applying the ACL check. Resources that are available to multiple Clients can be matched using a wildcard subject. All Resources accessible via the unsecured communication endpoint shall be matched using a wildcard subject.

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

ACL structure in Backus-Naur Form (BNF) notation is defined in Table 41:

Table 41 – 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 `<Character>` 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 privilege 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"), RETRIEVE ("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.

### 13.5.3 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:

### Table

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Authority&gt;</code></td>
<td><code>&lt;UUID&gt;</code></td>
</tr>
<tr>
<td><code>&lt;ResourceRef&gt;</code></td>
<td>' (' <code>&lt;OIC_LINK&gt;</code> {',' <code>&lt;OIC_LINK&gt;</code>} ') '</td>
</tr>
<tr>
<td><code>&lt;Permission&gt;</code></td>
<td>(&quot;C&quot;</td>
</tr>
<tr>
<td><code>&lt;Validity&gt;</code></td>
<td><code>&lt;Period&gt;</code> { <code>&lt;Recurrence&gt;</code> }</td>
</tr>
<tr>
<td><code>&lt;Wildcard&gt;</code></td>
<td>'*'</td>
</tr>
<tr>
<td><code>&lt;URI&gt;</code></td>
<td>IETF RFC 3986</td>
</tr>
<tr>
<td><code>&lt;UUID&gt;</code></td>
<td>IETF RFC 4122</td>
</tr>
<tr>
<td><code>&lt;Period&gt;</code></td>
<td>IETF RFC 5545 Period</td>
</tr>
<tr>
<td><code>&lt;Recurrence&gt;</code></td>
<td>IETF RFC 5545 Recurrence</td>
</tr>
<tr>
<td><code>&lt;OIC_LINK&gt;</code></td>
<td>ISO/IEC 30118-1:2018 defined in JSON Schema</td>
</tr>
<tr>
<td><code>&lt;Character&gt;</code></td>
<td>Any UTF8 printable character, excluding NUL</td>
</tr>
</tbody>
</table>
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.r.ace2" 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.r.acl2" Resource's use of the DELETE operation is not in accordance with the OCF Interfaces defined in ISO/IEC 30118-1:2018.

Evaluation of local ACL Resource completes when all ACL Resource have been queried and no entry can be found for the requested Resource for the requestor – e.g. "/oic/sec/acl", "/oic/sec/sacl" and "/oic/sec/amacl" do not match the subject and the requested Resource.

It is possible the AMS has an ACL policy that satisfies a resource access request, but the necessary ACE has not been provisioned to Server. The Server may open a secure connection to the AMS to request ACL provisioning. The Server may use filter criteria that returns a subset of the AMS ACL policy. The AMS shall obtain the Server Device ID using the secure connection context.

The AMS maintains an AMACL policy for Servers it manages. If the Server connects to the AMS to process an "/oic/sec/amacl" Resource. The AMS shall match the AMACL policy and return the Permission Property or an error if no match is found.

If the requested Resource is still not matched, the Server returns an error. The requester should query the Server to discover the configured AMS services. The Client should contact the AMS to request a sacl ("/oic/sec/sacl") Resource. Performing the following operations implement this type of request:

1) Client: Open secure connection to AMS.
2) Client: RETRIEVE /oic/sec/acl2?deviceuuid="XXX...",resources="href"
3) AMS: constructs a "/oic/sec/sacl" Resource that is signed by the AMS and returns it in response to the RETRIEVE command.
4) Client: UPDATE /oic/sec/sacl [{ ...sacl... }]
5) Server: verifies sacl signature using AMS credentials and installs the ACL Resource if valid.
6) Client: retries original Resource access request. This time the new ACL is included in the local ACL evaluation.

The ACL contained in the "/oic/sec/sacl" Resource should grant longer term access that satisfies repeated Resource requests.

"oic.r.acl" Resource is defined in Table 42.

Table 42 – Definition of the "oic.r.acl" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/acl</td>
<td>ACL</td>
<td>oic.r.acl</td>
<td>baseline</td>
<td>Resource for managing access</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 43 defines the Properties of "oic.r.acl".

Table 43 – Properties of the "oic.r.acl" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Access Mode</th>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE List</td>
<td>aclist</td>
<td>oic.sec.ace</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>Access Control Entries in the ACL resource. This Property contains &quot;aces&quot;, an array of &quot;oic.sec.ace1&quot; resources and &quot;aces2&quot;, an array of &quot;oic.sec.ace2&quot; Resources</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>R</td>
<td>RESET</td>
<td>Server shall set to manufacturer defaults.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFOTM</td>
<td>Set by DOTS after successful OTM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFPRO</td>
<td>The AMS (referenced via rowneruuid property) shall update the aclist entries after mutually authenticated secure session is established. Access to NCRs is prohibited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>RFNOP</td>
<td>Access to NCRs is permitted after a matching ACE is found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>SRESET</td>
<td>The DOTS (referenced via devowneruuid Property of &quot;/oic/sec/doxm&quot; Resource) should evaluate the integrity of and may update aclist entries when a secure session is established and the Server and DOTS are authenticated.</td>
</tr>
<tr>
<td>Resource Owner ID</td>
<td>rowneruuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>The resource owner Property (rowneruuid) is used by the Server to reference a service provider trusted by the Server. Server shall verify the service provider is authorized to perform the requested action</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>RESET</td>
<td>Server shall set to the nil uuid value (e.g. &quot;00000000-0000-0000-0000-000000000000&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFOTM</td>
<td>The DOTS should configure the /acl rowneruuid Property when a successful owner transfer session is established.</td>
</tr>
</tbody>
</table>

R: Read
RW: Read Write
R FOTM: Read, from OTM
R FPRO: Read, from PRO
R FNOP: Read, from NOP
R RESET: Read, Set to RESET
R SRESET: Read, Set to SRESET

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
The DOTS (referenced via /doxm devowneruuid Property or the /doxm ownerruuid Property) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the ownerruuid Property does not refer to a valid DOTS the Server shall transition to RESET device state.

Table 44 defines the Properties of "oic.r.ace".

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>resources</td>
<td>oic.oic-link</td>
<td>array</td>
<td>RW</td>
<td>Yes</td>
<td>The application's Resources to which a security policy applies</td>
</tr>
<tr>
<td>Permission</td>
<td>permission</td>
<td>oic.sec.crudntype</td>
<td>bitmask</td>
<td>RW</td>
<td>Yes</td>
<td>Bitmask encoding of CRUDN permission</td>
</tr>
<tr>
<td>Validity</td>
<td>validity</td>
<td>oic.sec.ace/definitions/time-interval</td>
<td>array</td>
<td>RW</td>
<td>No</td>
<td>An array of a tuple of period and recurrence. Each item in this array contains a string representing a period using the IETF RFC 5545 Period, and a string array representing a recurrence rule using the IETF RFC 5545 Recurrence.</td>
</tr>
<tr>
<td>Subject ID</td>
<td>subjectuuid</td>
<td>String</td>
<td>uuid, ***</td>
<td>RW</td>
<td>Yes</td>
<td>A uuid that identifies the Device to which this ACE applies to or &quot;***&quot; for anonymous access.</td>
</tr>
</tbody>
</table>

Table 45 defines the values of "oic.sec.crudntype".

<table>
<thead>
<tr>
<th>Value</th>
<th>Access Policy</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>bx0000,0000 (0)</td>
<td>No permissions</td>
<td>No permissions</td>
<td>N/A</td>
</tr>
<tr>
<td>bx0000,0001 (1)</td>
<td>C</td>
<td>CREATE</td>
<td>N/A</td>
</tr>
<tr>
<td>bx0000,0010 (2)</td>
<td>R</td>
<td>RETREIVE, OBSERVE, DISCOVER</td>
<td>The &quot;R&quot; permission bit covers both the Read permission and the Observe permission.</td>
</tr>
<tr>
<td>bx0000,0100 (4)</td>
<td>U</td>
<td>WRITE, UPDATE</td>
<td>N/A</td>
</tr>
<tr>
<td>bx0000,1000 (8)</td>
<td>D</td>
<td>DELETE</td>
<td>N/A</td>
</tr>
<tr>
<td>bx0001,0000 (16)</td>
<td>N</td>
<td>NOTIFY</td>
<td>The &quot;N&quot; permission bit is ignored in OCF 1.0, since &quot;R&quot; covers the Observe permission. It is documented for future versions</td>
</tr>
</tbody>
</table>

"oic.sec.acl2" Resource is defined in Table 28.


### Table 46 – Definition of the "oic.sec.acl2" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/acl2</td>
<td>ACL2</td>
<td>oic.r.acl2</td>
<td>baseline</td>
<td>Resource for managing access</td>
<td>Security</td>
</tr>
</tbody>
</table>

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

### Table 47 – Properties of the "oic.sec.acl2" Resource

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value Type</th>
<th>Mandatory</th>
<th>Device State</th>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aclist2</td>
<td>array of oic.sec.ace2</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td>The aclist2 Property is an array of ACE records of type &quot;oic.sec.ace2&quot;. The Server uses this list to apply access control to its local resources.</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>RESET R The Server shall set to manufacturer defaults.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM RW The AMS (referenced via rowneruuid property) shall update the aclist entries after mutually authenticated secure session is established. Access to NCRs is prohibited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO RW Access to NCRs is permitted after a matching ACE2 is found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP R The AMS (referenced via devowneruuid Property of &quot;/oic/sec/doxm Resource&quot;) should evaluate the integrity of and may update aclist entries when a secure session is established and the Server and DOTS are authenticated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SRESET RW The DOTS (referenced via devowneruuid Property or rowneruuid Property of &quot;/oic/sec/doxm Resource&quot;) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the rowneruuid Property does not refer to a valid DOTS the Server shall transition to RESET device state.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>uuid</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td>RESET R The DOTS (referenced via devowneruuid Property of &quot;/oic/sec/doxm Resource&quot;) should configure the rowneruuid Property of &quot;/oic/sec/acl2&quot; Resource when a successful owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM RW The DOTS should configure the rowneruuid Property of &quot;/oic/sec/acl2&quot; Resource when a successful owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO R The DOTS should configure the rowneruuid Property of &quot;/oic/sec/acl2&quot; Resource when a successful owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP R The DOTS should configure the rowneruuid Property of &quot;/oic/sec/acl2&quot; Resource when a successful owner transfer session is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SRESET RW The DOTS (referenced via devowneruuid Property or rowneruuid Property of &quot;/oic/sec/doxm Resource&quot;) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the rowneruuid Property does not refer to a valid DOTS the Server shall transition to RESET device state.</td>
</tr>
</tbody>
</table>
Table 48 defines the Properties of "oic.sec.ace2".

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value Type</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject</td>
<td>oic.sec.roletype, oic.sec.didtype, oic.sec.conntype</td>
<td>Yes</td>
<td>The Client is the subject of the ACE when the roles, Device ID, or connection type matches.</td>
</tr>
<tr>
<td>resources</td>
<td>array of oic.sec.ace2.resource-ref</td>
<td>Yes</td>
<td>The application's resources to which a security policy applies</td>
</tr>
<tr>
<td>permission</td>
<td>oic.sec.crudntype.bitmask</td>
<td>Yes</td>
<td>Bitmask encoding of CRUDN permission</td>
</tr>
<tr>
<td>validity</td>
<td>array of oic.sec.time-pattern</td>
<td>No</td>
<td>An array of a tuple of period and recurrence. Each item in this array contains a string representing a period using the IETF RFC 5545 Period, and a string array representing a recurrence rule using the IETF RFC 5545 Recurrence.</td>
</tr>
<tr>
<td>aceid</td>
<td>integer</td>
<td>Yes</td>
<td>An aceid is unique with respect to the array entries in the aclist2 Property.</td>
</tr>
</tbody>
</table>

Table 49 defines the Properties of "oic.sec.ace2.resource-ref".

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value Type</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>href</td>
<td>uri</td>
<td>No</td>
<td>A URI referring to a resource to which the containing ACE applies</td>
</tr>
<tr>
<td>wc</td>
<td>string</td>
<td>No</td>
<td>Refer to Table 23.</td>
</tr>
</tbody>
</table>

Table 50 defines the values of "oic.sec.ace2.resource-ref".

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conntype</td>
<td>string</td>
<td>enum [&quot;auth-crypt&quot;, &quot;anon-clear&quot;]</td>
<td>This Property allows an ACE to be matched based on the connection or message protection type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>auth-crypt</td>
<td>ACE applies if the Client is authenticated and the data channel or message is encrypted and integrity protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>anon-clear</td>
<td>ACE applies if the Client is not authenticated and the data channel or message is not encrypted but may be integrity protected</td>
</tr>
</tbody>
</table>

Local ACL Resources supply policy to a Resource access enforcement point within an OCF stack instance. The OCF framework gates Client access to Server Resources. It evaluates the subject's request using policies contained in ACL resources.

Resources named in the ACL policy can be fully qualified or partially qualified. Fully qualified Resource references include the device identifier in the href Property that identifies the remote Resource Server that hosts the Resource. Partially qualified references mean that the local Resource Server hosts the Resource. If a fully qualified resource reference is given, the Intermediary enforcing access shall have a secure channel to the Resource Server and the
Resource Server shall verify the Intermediary is authorized to act on its behalf as a Resource access enforcement point.

Resource Servers should include references to Device and ACL Resources where access enforcement is to be applied. However, access enforcement logic shall not depend on these references for access control processing as access to Server Resources will have already been granted.

Local ACL Resources identify a Resource Owner service that is authorized to instantiate and modify this Resource. This prevents non-terminating dependency on some other ACL Resource. Nevertheless, it should be desirable to grant access rights to ACL Resources using an ACL Resource.

An ACE or ACE2 entry is called currently valid if the validity period of the ACE or ACE2 entry includes the time of the request. The validity period in the ACE or ACE2 may be a recurring time period (e.g., daily from 1:00-2:00). Matching the resource(s) specified in a request to the resource Property of the ACE or ACE2 is defined in clause 12.2. For example, one way they can match is if the Resource URI in the request exactly matches one of the resource references in the ACE or ACE2 entries.

A request will match an ACE if any of the following are true:

1) The "deviceuuid" Property associated with the secure session matches the "subjectuuid" of the ACE; AND the Resource of the request matches one of the "resources" Property of the ACE; AND the ACE is currently valid.

2) The ACE "subjectuuid" Property contains the wildcard "*" character; AND the Resource of the request matches one of the "resources" Property of the ACE; AND the ACE is currently valid.

3) When authentication uses a symmetric key credential;
   AND the CoAP payload query string of the request specifies a role, which is associated with the symmetric key credential of the current secure session;
   AND the CoAP payload query string of the request specifies a role, which is contained in the "oic.r.cred.creds.roleid" Property of the current secure session;
   AND the resource of the request matches one of the resources Property of the ACE;
   AND the ACE is currently valid.

A request will match an ACE2 if any of the following are true:

1) The ACE2 "subject" Property is of type oic.sec.didtype has a UUID value that matches the "deviceuuid" Property associated with the secure session;
   AND the Resource of the request matches one of the resources Property of the ACE2 oic.sec.ace2.resource-ref;
   AND the ACE2 is currently valid.

2) The ACE2 "subject" Property is of type oic.sec.conntype and has the wildcard value that matches the currently established connection type;
   AND the resource of the request matches one of the resources Property of the ACE2 oic.sec.ace2.resource-ref;
   AND the ACE2 is currently valid.

3) When Client authentication uses a certificate credential;
   AND one of the roleid values contained in the role certificate matches the roleid Property of the ACE2 oic.sec.roletype;
AND the role certificate public key matches the public key of the certificate used to establish
the current secure session;

AND the resource of the request matches one of the array elements of the resources Property
of the ACE2 oic.ace2.resource-ref;

AND the ACE2 is currently valid.

4) When Client authentication uses a certificate credential;

AND the CoAP payload query string of the request specifies a role, which is member of the
set of roles contained in the role certificate;

AND the roleid values contained in the role certificate matches the roleid Property of the
ACE2 oic.ace2.roleid;

AND the role certificate public key matches the public key of the certificate used to establish
the current secure session;

AND the resource of the request matches one of the resources Property of the ACE2
oic.ace2.resource-ref;

AND the ACE2 is currently valid.

5) When Client authentication uses a symmetric key credential;

AND one of the roleid values associated with the symmetric key credential used in the secure
session, matches the roleid Property of the ACE2 oic.ace2.roleid;

AND the resource of the request matches one of the array elements of the resources Property
of the ACE2 oic.ace2.resource-ref;

AND the ACE2 is currently valid.

6) When Client authentication uses a symmetric key credential;

AND the CoAP payload query string of the request specifies a role, which is contained in the
"oic.r.cred.creds.roleid" Property of the current secure session;

AND CoAP payload query string of the request specifies a role that matches the "roleid"
Property of the ACE2 oic.ace2.roleid;

AND the resource of the request matches one of the array elements of the "resources"
Property of the ACE2 oic.ace2.resource-ref;

AND the ACE2 is currently valid.

A request is granted if ANY of the 'matching' ACEs contains the permission to allow the request.
Otherwise, the request is denied.

There is no way for an ACE to explicitly deny permission to a resource. Therefore, if one Device
with a given role should have slightly different permissions than another Device with the same
role, they must be provisioned with different roles.

The Server is required to verify that any hosted Resource has authorized access by the Client
requesting access. The "/oic/sec/acl2" Resource is co-located on the Resource host so that the
Resource request processing should be applied securely and efficiently. See Annex A for
example.

13.6 Access Manager ACL Resource

"oic.r.amacl" Resource is defined in Table 51.
Table 51 – Definition of the "oic.r.amacl" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/amacl</td>
<td>Managed ACL</td>
<td>oic.r.amacl</td>
<td>baseline</td>
<td>Resource for managing access</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 52 defines the Properties of "oic.r.amacl".

Table 52 – Properties of the "oic.r.amacl" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>resources</td>
<td>oic.sec.ace 2.resource-ref</td>
<td>array</td>
<td>RW</td>
<td>Yes</td>
<td>Multiple links to this host's Resources</td>
</tr>
</tbody>
</table>

The AMS should be used to centralize management of access policy, but requires Servers to open a connection to the AMS whenever the named Resources are accessed. See A.2 for example.

13.7 Signed ACL Resource

"oic.r.sacl" Resource is defined in Table 53.

Table 53 – Definition of the "oic.r.sacl" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/sacl</td>
<td>Signed ACL</td>
<td>oic.r.sacl</td>
<td>baseline</td>
<td>Resource for managing access</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 54 defines the Properties of "oic.r.sacl".

Table 54 – Properties of the "oic.r.sacl" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Access Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE List</td>
<td>aclist2</td>
<td>oic.sec.ace2</td>
<td>array</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
<td>Access Control Entries in the ACL Resource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>Server shall set to manufacturer defaults.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>Set by DOTS after successful OTM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>The AMS (referenced via owneruuid property) shall update the aclist entries after mutually authenticated secure session is established. Access to NCRs is prohibited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>Access to NCRs is permitted after a matching ACE is found.</td>
</tr>
</tbody>
</table>

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
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.

Table 55 defines the Properties of "oic.sec.sigtype".

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Unit</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Type</td>
<td>sigtype</td>
<td>String</td>
<td>N/A</td>
<td>N/A</td>
<td>RW</td>
<td>Yes</td>
<td>The string specifying the predefined signature format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.sigtype.jws&quot; – IETF RFC 7515 JSON web signature (JWS) object</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.sigtype.pk7&quot; – IETF RFC 2315 base64-encoded object</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;oic.sec.sigtype.cws&quot; – CBOR-encoded JWS object</td>
</tr>
<tr>
<td>Signature Value</td>
<td>sigvalue</td>
<td>String</td>
<td>N/A</td>
<td>N/A</td>
<td>RW</td>
<td>Yes</td>
<td>The encoded signature</td>
</tr>
</tbody>
</table>

### 13.8 Provisioning Status Resource

The "/oic/sec/pstat" Resource maintains the Device provisioning status. Device provisioning should be Client-directed or Server-directed. Client-directed provisioning relies on a Client device to determine what, how and when Server Resources should be instantiated and updated. Server-directed provisioning relies on the Server to seek provisioning when conditions dictate. Server-directed provisioning depends on configuration of the rowneruuid Property of the "/oic/sec/doxm", "/oic/sec/cred" and "/oic/sec/acl2" Resources to identify the device ID of the trusted DOTS, CMS and AMS services respectively. Furthermore, the "/oic/sec/cred" Resource should be provisioned at ownership transfer with credentials necessary to open a secure connection with appropriate support service.

"oic.r.pstat" Resource is defined in Table 56.

Table 56 – Definition of the "oic.r.pstat" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/pstat</td>
<td>Provisioning Status</td>
<td>oic.r.pstat</td>
<td>baseline</td>
<td>Resource for managing Device provisioning status</td>
<td>Configuration</td>
</tr>
</tbody>
</table>

Table 57 defines the Properties of "oic.r.pstat".
Table 57 – Properties of the "oic.r.pstat" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Access Mode</th>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Onboarding State</td>
<td>dos</td>
<td>oic.sec.dostype</td>
<td>N/A</td>
<td>Yes</td>
<td>RW</td>
<td></td>
<td>Device Onboarding State</td>
</tr>
<tr>
<td>Is Device Operational</td>
<td>isop</td>
<td>Boolean</td>
<td>T/F</td>
<td>Yes</td>
<td>R</td>
<td>RESET</td>
<td>Server shall set to FALSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFOTM Server shall set to FALSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFPRO Server shall set to FALSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RFNOP Server shall set to TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SRESET Server shall set to FALSE</td>
</tr>
<tr>
<td>Current Mode</td>
<td>cm</td>
<td>oic.sec.dpmtype</td>
<td>bitmask</td>
<td>Yes</td>
<td>R</td>
<td>Current Mode</td>
<td></td>
</tr>
<tr>
<td>Target Mode</td>
<td>tm</td>
<td>oic.sec.dpmtype</td>
<td>bitmask</td>
<td>Yes</td>
<td>RW</td>
<td>Target Mode</td>
<td></td>
</tr>
<tr>
<td>Operational Mode</td>
<td>om</td>
<td>oic.sec.pomtype</td>
<td>bitmask</td>
<td>Yes</td>
<td>R</td>
<td>RESET Server shall set to manufacturer default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFOTM Set by DOTS after successful OTM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFPRO Set by CMS, AMS, DOTS after successful authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFNOP Set by CMS, AMS, DOTS after successful authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>SRESET Set by DOTS.</td>
<td></td>
</tr>
<tr>
<td>Supported Mode</td>
<td>sm</td>
<td>oic.sec.pomtype</td>
<td>bitmask</td>
<td>Yes</td>
<td>R</td>
<td>All states Supported provisioning services operation modes</td>
<td></td>
</tr>
<tr>
<td>Device UUID</td>
<td>deviceuuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>RW</td>
<td>All states [DEPRECATED] A uuid that identifies the Device to which the status applies</td>
<td></td>
</tr>
<tr>
<td>Resource Owner ID</td>
<td>owneruuid</td>
<td>String</td>
<td>uuid</td>
<td>Yes</td>
<td>R</td>
<td>RESET Server shall set to the nil uuid value (e.g. &quot;00000000-0000-0000-0000-000000000000&quot;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFOTM The DOTS should configure the owneruuid Property when a successful owner transfer session is established.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>RFPRO n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>RFNOP n/a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>SRESET The DOTS (referenced via devowneruuid Property of &quot;/oic/sec/doxm&quot; Resource) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the owneruuid does not refer to a valid DOTS the Server shall transition to RESET Device state.</td>
<td></td>
</tr>
</tbody>
</table>

The provisioning status Resource "/oic/sec/pstat" is used to enable Devices to perform self-directed provisioning. Devices are aware of their current configuration status and a target configuration objective. When there is a difference between current and target status, the Device
should consult the rowneruuid Property of "/oic/sec/cred" Resource to discover whether any suitable provisioning services exist. The Device should request provisioning if configured to do so. The om Property of "/oic/sec/pstat" Resource will specify expected Device behaviour under these circumstances.

Self-directed provisioning enables Devices to function with greater autonomy to minimize dependence on a central provisioning authority that should be a single point of failure in the OCF Security Domain.

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

**Table 58 – Properties of the "/oic/sec/dostype" Property**

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Mandatory</th>
<th>Access Mode</th>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Onboarding State</td>
<td>s</td>
<td>UINT16</td>
<td>enum (0=RESET, 1=RFOTM, 2=RFPRO, 3=RFNOP, 4=SRESET)</td>
<td>Y</td>
<td>R</td>
<td>RESET</td>
<td>The Device is in a hard reset state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFOTM</td>
<td>Set by DOTS after successful OTM to RFPRO.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFPRO</td>
<td>Set by CMS, AMS, DOTS after successful authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>RFNOP</td>
<td>Set by CMS, AMS, DOTS after successful authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>SRESET</td>
<td>Set by CMS, AMS, DOTS after successful authentication</td>
</tr>
<tr>
<td>Pending state</td>
<td>p</td>
<td>Boolean</td>
<td>T</td>
<td>F</td>
<td>Y</td>
<td>R</td>
<td>All States</td>
</tr>
</tbody>
</table>

In all Device states:

- An authenticated and authorised Client may change the Device state of a Device by updating pstat.dos.s to the desired value. The allowed Device state transitions are defined in Figure 27.
- Prior to updating pstat.dos.s, the Client configures the Device to meet entry conditions for the new Device state. The SVR definitions define the entity (Client or Server) expected to perform the specific SVR configuration change to meet the entry conditions. Once the Client has configured the aspects for which the Client is responsible, it may update pstat.dos.s. The Server then makes any changes for which the Server is responsible, including updating required SVR values, and set pstat.dos.s to the new value.
- The pstat.dos.p Property is read-only by all Clients.
- The Server sets pstat.dos.p to TRUE before beginning the process of updating pstat.dos.s, and sets it back to FALSE when the pstat.dos.s change is completed.

Any requests to update pstat.dos.s while pstat.dos.p is TRUE are denied.

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 the property of "/oic/sec/dostype" Resource 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, the s Property of "/oic/sec/dostype" Resource is read-only by unauthenticated requestors
- After the OTM is successful, the s Property of "/oic/sec/dostype" Resource is read-write by authorized requestors.
- The negotiable Device OC is used to create an authenticated session over which the DOTS directs the Device state to transitions 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 devowneruuuid Property in the /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 /doxm Resource to "true".

When Device state is RFPRO:

- The s Property of "/oic/sec/dostype" Resource 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 RFNOP:

- The /pstat.dos.s Property is read-only by unauthorized requestors and read-write by authorized requestors.
- NCRs, SVRs and core Resources are accessible following normal access processing.
- An authorized may transition to RFPRO. Only the Device owner may transition to SRESET or RESET.

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 s Property of the "/oic/sec/dostype" Resource of "/oic/sec/pstat" Resource.

The certificates that identify and authorize the Device owner are sufficient to re-create minimalist /cred and /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 dos.s Property of the /pstat Resource 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).

"oic.sec.dpmtype" is defined in Table 59.

Table 59 – Definition of the "oic/sec.dpmtype" Property

<table>
<thead>
<tr>
<th>Type Name</th>
<th>Type URN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Provisioning Mode</td>
<td>oic/sec.dpmtype</td>
<td>Device provisioning mode is a 16-bit bitmask describing various provisioning modes</td>
</tr>
</tbody>
</table>

Table 60 and Table 61 define the values of "oic.sec.dpmtype".

Table 60 – Value Definition of the "oic/sec.dpmtype" Property (Low-Byte)

<table>
<thead>
<tr>
<th>Value</th>
<th>Device Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bx0000,0001 (1)</td>
<td>Deprecated</td>
<td></td>
</tr>
<tr>
<td>bx0000,0010 (2)</td>
<td>Deprecated</td>
<td></td>
</tr>
<tr>
<td>bx0000,0100 (4)</td>
<td>Deprecated</td>
<td></td>
</tr>
<tr>
<td>bx0000,1000 (8)</td>
<td>Deprecated</td>
<td></td>
</tr>
<tr>
<td>bx0001,0000 (16)</td>
<td>Deprecated</td>
<td></td>
</tr>
<tr>
<td>bx0010,0000 (32)</td>
<td>Deprecated</td>
<td></td>
</tr>
</tbody>
</table>
| bx0100,0000 (64) | Initiate Software Version Validation | Software version validation requested/pending (1)  
Software version validation complete (0) |
| bx1000,0000 (128) | Initiate Secure Software Update | Secure software update requested/pending (1)  
Secure software update complete (0) |

Table 61 – Value Definition of the "oic/sec.dpmtype" Property (High-Byte)

<table>
<thead>
<tr>
<th>Value</th>
<th>Device Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bx0000,0000 – bx1111,1111</td>
<td>&lt;Reserved&gt;</td>
<td>Reserved for later use</td>
</tr>
</tbody>
</table>

The provisioning operation mode type is an 8-bit mask enumerating the various provisioning operation modes.
"oic.sec.pomtype" is defined in Table 62.

### Table 62 – Definition of the "oic.sec.pomtype" Property

<table>
<thead>
<tr>
<th>Type Name</th>
<th>Type URN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Provisioning</td>
<td>oic.sec.pomtype</td>
<td>Device provisioning operation mode is a 8-bit bitmask describing various</td>
</tr>
<tr>
<td>Operation Mode</td>
<td></td>
<td>provisioning operation modes</td>
</tr>
</tbody>
</table>

Table 63 defines the values of "oic.sec.pomtype".

### Table 63 – Value Definition of the "oic.sec.pomtype" Property

<table>
<thead>
<tr>
<th>Value</th>
<th>Operation Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bx0000,0001 (1)</td>
<td>Server-directed utilizing multiple provisioning</td>
<td>Provisioning related services are placed in different Devices. Hence, a</td>
</tr>
<tr>
<td></td>
<td>services</td>
<td>provisioned Device should establish multiple DTLS sessions for each service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This condition exists when bit 0 is FALSE.</td>
</tr>
<tr>
<td>bx0000,0010 (2)</td>
<td>Server-directed utilizing a single provisioning</td>
<td>All provisioning related services are in the same Device. Hence, instead</td>
</tr>
<tr>
<td></td>
<td>service</td>
<td>of establishing multiple DTLS sessions with provisioning services, a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provisioned Device establishes only one DTLS session with the Device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This condition exists when bit 0 is TRUE.</td>
</tr>
<tr>
<td>bx0000,0100 (4)</td>
<td>Client-directed provisioning</td>
<td>Device supports provisioning service control of this Device's provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operations. This condition exists when bit 1 is TRUE. When this bit is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE this Device controls provisioning steps.</td>
</tr>
<tr>
<td>bx0000,1000(8) –</td>
<td>&lt;Reserved&gt;</td>
<td>Reserved for later use</td>
</tr>
<tr>
<td>bx1000,0000(128)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bx1111,11xx</td>
<td>&lt;Reserved&gt;</td>
<td>Reserved for later use</td>
</tr>
</tbody>
</table>

### 13.9 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 an 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.r.csr" Resource is defined in Table 64.

### Table 64 – Definition of the "oic.r.csr" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/csr</td>
<td>Certificate Signing</td>
<td>oic.r.csr</td>
<td>baseline</td>
<td>The CSR resource contains a Certificate Signing Request for the Device's</td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Request</td>
<td></td>
<td></td>
<td>public key.</td>
<td></td>
</tr>
</tbody>
</table>

Table 65 defines the Properties of "oic.r.csr".

### Table 65 – Properties of the "oic.r.csr" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>csr</td>
<td>String</td>
<td>R</td>
<td>Yes</td>
<td>Contains the signed CSR encoded according to the encoding Property</td>
</tr>
</tbody>
</table>
The Device chooses which public key to use, and may optionally generate a new key pair for this purpose.

In the CSR, the Common Name component of the Subject Name shall contain a string of the format "uuid:X" where X is the Device’s requested UUID in the format defined by IETF RFC 4122. The Common Name, and other components of the Subject Name, may contain other data. If the Device chooses to include additional information in the Common Name component, it shall delimit it from the UUID field by white space, a comma, or a semicolon.

If the Device does not have a pre-provisioned key pair to use, but is capable and willing to generate a new key pair, the Device may begin generation of a key pair as a result of a RETRIEVE of this resource. If the Device cannot immediately respond to the RETRIEVE request due to time required to generate a key pair, the Device shall return an "operation pending" error. This indicates to the Client that the Device is not yet ready to respond, but will be able at a later time. The Client should retry the request after a short delay.

### 13.10 Roles Resource

The roles Resource maintains roles that have been asserted with role certificates, as described in clause 10.4.2. Asserted roles have an associated public key, i.e., the public key in the role certificate. Servers shall only grant access to the roles information associated with the public key of the Client. The roles Resource should be viewed as an extension of the (D)TLS session state. See 10.4.2 for how role certificates are validated.

The roles Resource shall be created by the Server upon establishment of a secure (D)TLS session with a Client, if is not already created. The roles Resource shall only expose a secured OCF Endpoint in the "/oic/res" response. A Server shall retain the roles Resource at least as long as the (D)TLS session exists. A Server shall retain each certificate in the roles Resource at least until the certificate expires or the (D)TLS session ends, whichever is sooner. The requirements of clause 10.3 and 10.4.2 to validate a certificate’s time validity at the point of use always apply. A Server should regularly inspect the contents of the roles resource and purge contents based on a policy it determines based on its resource constraints. For example, expired certificates, and certificates from Clients that have not been heard from for some arbitrary period of time could be candidates for purging.

The roles Resource is implicitly created by the Server upon establishment of a (D)TLS session. In more detail, the RETRIEVE, UPDATE and DELETE operations on the roles Resource shall behave as follows. Unlisted operations are implementation specific and not reliable.

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.

Table 66 – Definition of the "oic.r.roles" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/roles</td>
<td>Roles</td>
<td>oic.r.roles</td>
<td>baseline</td>
<td>Resource containing roles that have previously been asserted to this Server</td>
<td>Security</td>
</tr>
</tbody>
</table>

Table 67 defines the Properties of "oic.r.roles".

Table 67 – Properties of the "oic.r.roles" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles</td>
<td>roles</td>
<td>oic.sec.cred</td>
<td>array</td>
<td>RW</td>
<td>Yes</td>
<td>List of roles previously asserted to this Server</td>
</tr>
</tbody>
</table>

Because "oic.r.roles" shares the "oic.sec.cred" schema with "oic.r.cred", "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.

13.11 Account Resource

The Account Resource specifies the Properties based on IETF RFC 6749 Access Token based account creation. The mechanism to obtain credentials is described in clause 7.5. The Account Resource is used for Device Registration. The Account Resource is instantiated on the OCF Cloud as "oic/sec/account" SVR and is used by cloud-enabled Devices to register with the OCF Cloud. It should be only accessible on a secure channel; non-secure channel should not be able access this Resource.

During the Device Registration process, an OCF Cloud can provide a distinct URI of another OCF Cloud ("redirected-to" OCF Cloud). Both initial and redirected-to OCF Clouds are expected to belong to the same Vendor; they are assumed to have the same UUID and are assumed to have an out-of-band communication mechanism established. Device does not have to perform the Device Registration on the redirected-to OCF Cloud and the OCF Cloud may ignore such attempts. Redirected-to OCF Cloud is expected to accept the Access Token, provided to the Device by the initial OCF Cloud.

The "di", "uid", "refresh_token" and "access_token" Properties of the Account Resource should be securely stored as described in clause 15.
The RETRIEVE operation on OCF Cloud's "/oic/sec/account" Resource is not allowed and the OCF Cloud is expected to reject all attempts to perform such operation.

The UPDATE operation on the OCF Cloud's "/oic/sec/account" Resource behaves as follows:

- A Device intending to register with the OCF Cloud shall send UPDATE with following Properties "di" ("di" Property Value of "/oic/d" Resource), and "accesstoken" as configured by the Mediator ("at" Property Value of "oic.r.coapcloudconf" Resource). The OCF Cloud verifies it is the same "accesstoken" which was assigned to the Mediator for the corresponding "di" Property Value. The "accesstoken" is the permission for the Device to access the OCF Cloud. If the "apn" was included when the Mediator UPDATED the "oic.r.coapcloudconf" Resource, the Device shall also include "authprovider" Property when registering with the OCF Cloud. If no "apn" is specified, then the "authprovider" Property shall not be included in the UPDATE request.

- OCF Cloud returns "accesstoken", "uid", "refreshtoken", "expiresin" It may also return "redirecturi". Received "accesstoken" is to be treated by Device as an Access Token with "Bearer" token type as defined in IETF RFC 6750. This "accesstoken" shall be used for the following Account Session start using "oic/sec/session" SVR. Received "refreshtoken" is to be treated by Device as a Refresh Token as defined in IETF RFC 6749. The Device stores the OCF Cloud's Response values. If "redirecturi" is received, Device shall use received value as a new OCF Cloud URI instead of "cis" Property Value of "oic.r.coapcloudconf" Resource for further connections.

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.r.account " Resource is defined in Table 68.

### Table 68 – Definition of the "oic.r.account" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/account</td>
<td>Account</td>
<td>oic.r.account</td>
<td></td>
<td>Resource used for a device to add itself under a given credential</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 69 defines the Properties of "oic.r.account".

### Table 69 – Properties of the "oic.r.account" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>di</td>
<td>string</td>
<td>uuid</td>
<td>W</td>
<td>Yes</td>
<td>Unique Device identifier</td>
</tr>
<tr>
<td>Auth Provider</td>
<td>authprovider</td>
<td>string</td>
<td>Non-empty string</td>
<td>RW</td>
<td>Yes</td>
<td>The name of Authorization Provider through which Access Token was obtained.</td>
</tr>
<tr>
<td>Access-Token</td>
<td>accesstoken</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
<td>Access-Token used for communication with OCF Cloud after account creation</td>
</tr>
</tbody>
</table>
13.12 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.

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

The RETRIEVE operation on OCF Cloud’s "/oic/sec/session" 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 OCF Cloud’s "/oic/sec/session" Resource:

- The Device connecting to the OCF Cloud shall send an UPDATE request message to the OCF Cloud’s "/oic/sec/session" Resource. The message shall include the "di" Property Value of "/oic/d" Resource and "uid", "login" Value ("true" to establish connection; "false" to disconnect) and "accesstoken" as returned by OCF Cloud during Device Registration. The OCF Cloud verifies it is the same Access Token which was returned to the Device during Device Registration process. If Device was attempting to establish the connection and provided values were verified as correct by the OCF Cloud, OCF Cloud sends a response with remaining lifetime of the associated Access Token ("expiresin" Property Value).

"oic.r.session" Resource is defined in Table 70.

Table 70 – Definition of the "oic.r.session" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (&quot;rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/session</td>
<td>Account Session</td>
<td>oic.r.session</td>
<td>oic.if.baseline</td>
<td>Resource that enables a device to manage its session using login or logout</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 71 defines the Properties of "oic.r.session".

Table 71 – Properties of the "oic.r.session" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>uid</td>
<td>string</td>
<td>uuid</td>
<td>W</td>
<td>Yes</td>
<td>User ID which provided by Device Registration process</td>
</tr>
<tr>
<td>Device ID</td>
<td>di</td>
<td>string</td>
<td>uuid</td>
<td>W</td>
<td>Yes</td>
<td>Unique device id registered for a Device</td>
</tr>
</tbody>
</table>
Access Token | access_token | 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 | expires_in | 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

### 13.13 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 "expires_in" 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 "refresh_token", as returned by OCF Cloud.
- OCF Cloud response is expected to include a "refresh_token", new "access_token", and "expires_in". Received "access_token" 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 "refresh_token" is to be treated by Device as a Refresh Token as defined in IETF RFC 6749. Received "refresh_token" may be the new Refresh Token or the same one as provided by the Device in the UPDATE request. In case when new distinct "refresh_token" is provided by the OCF Cloud, the Device shall discard the old value. The OCF Cloud’s response values "refresh_token", "access_token" and "expires_in" are securely stored on the Device.

"oic.r.tokenrefresh" Resource is defined in Table 72.

#### Table 72 – Definition of the "oic.r.tokenrefresh" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID (“rt” value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/tokenrefresh</td>
<td>Token Refresh</td>
<td>oic.r.tokenrefresh</td>
<td>oic.if.baseline</td>
<td>Resource to manage the access-token using refresh token</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 73 defines the Properties of "oic.r.tokenrefresh".
Table 73 – Properties of the "oic.r.tokenrefresh" Resource

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

13.14 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.r.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.r.doxm" Resource to anonymous requesters, to preserve privacy.

13.15 SVRs, Discoverability and OCF Endpoints
All implemented SVRs shall be "discoverable" (reference ISO/IEC 30118-1:2018, Policy Parameter clause 7.8.2.1.2).

All implemented discoverable SVRs shall expose a Secure OCF Endpoint (e.g. CoAPS) (reference ISO/IEC 30118-1:2018, clause 10).

The "/oic/sec/doxm" Resource shall expose an Unsecure OCF Endpoint (e.g. CoAP) in RFOTM (reference ISO/IEC 30118-1:2018, clause 10).

13.16 Additional Privacy Consideration for Core and SVRs Resources
13.16.1 Additional Privacy Considerations for Core and SVR Resources General
Unique identifiers are a privacy consideration due to their potential for being used as a tracking mechanism. These include the following Resources and Properties:

- "/oic/d" Resource containing the "di" and "piid" Properties.
- "/oic/p" Resource containing the "pi" Property.
- "/oic/sec/doxm" Resource containing the "deviceuuuid" Property.

All identifiers are unique values that are visible to throughout the Device lifecycle by anonymous requestors. This implies any Client Device, including those with malicious intent, are able to reliably obtain identifiers useful for building a log of activity correlated with a specific Platform and Device.

There are two strategies for privacy protection of Devices:
1) Apply an ACL policy that restricts read access to Resources containing unique identifiers
2) Limit identifier persistence to make it impractical for tracking use.
Both techniques can be used effectively together to limit exposure to privacy attacks.

1) A Platform / Device manufacturer should specify a default ACL policy that restricts anonymous requestors from accessing unique identifiers. An OCF Security Domain owner should modify the ACL policy to grant access to authenticated Devices who, presumably, do not present a privacy threat.

2) Servers shall expose a temporary, non-repeated identifier via an OCF Interface when the Device transitions to the RESET Device state. The temporary identifiers are disjoint from and not correlated to the persistent and semi-persistent identifiers. Temporary, non-repeated identifiers shall be:
   a) Disjoint from (i.e. not linked to) the persistent or semi-persistent identifiers
   b) Generated by a function that is pre-image resistant, second pre-image resistant and collision resistant

A new Device seeking deployment needs to inform would-be DOTS providers of the identifier used to begin the onboarding process. However, attackers could obtain the value too and use it for Device tracking throughout the Device’s lifetime.

To address this privacy threat, Servers shall expose a temporary non-repeated identifier via the deviceuuid Property of the "/oic/sec/doxm" Resource to unauthenticated "/oic/res" and "/oic/sec/doxm" Resource RETRIEVE requests when the devowneruuid Property of "/oic/sec/doxm" Resource is the nil-UUID. The Server shall expose a new temporary non-repeated deviceuuid Property of the "/oic/sec/doxm" Resource when the device state transitions to RESET. This ensures the deviceuuid Property of the "/oic/sec/doxm" cannot be used to track across multiple owners.

The devowneruuid Property of "/oic/sec/doxm" Resource is initialized to the nil-UUID upon entering RESET; which is retained until being set to a non-nil-UUID value during RFOTM device state. The device shall supply a temporary, non-repeated deviceuuid Property of "/oic/sec/doxm" Resource to RETRIEVE requests on "/oic/sec/doxm" and "/oic/res" Resources while devowneruuid Property of "/oic/sec/doxm" Resource is the nil-UUID. During the OTM process the DOTS shall UPDATE devowneruuid Property of the "/oic/sec/doxm" Resource to a non-nil UUID value which is the trigger for the Device to expose its persistent or semi-persistent device identifier. Therefore, the Device shall supply deviceuuid Property of "/oic/sec/doxm" Resource in response to RETRIEVE requests while the devowneruuid Property of the "/oic/sec/doxm" Resource is a non-nil-UUID value.

The DOTS or AMS may also provision an ACL policy that restricts access to the "/oic/sec/doxm" Resource such that only authenticated Clients are able to obtain the persistent or semi-persistent device identifier via the deviceuuid Property value of the "/oic/sec/doxm" Resource.

Clients avoid making unauthenticated discovery requests that would otherwise reveal a persistent or semi-persistent identifier using the "/oic/sec/cred" Resource to first establish an authenticated connection. This is achieved by first provisioning a "/oic/sec/cred" Resource entry that contains the Server’s deviceuuid Property value of the "/oic/sec/doxm" Resource.

The di Property in the "/oic/d" Resource shall mirror that of the deviceuuid Property of the "/oic/sec/doxm" Resource. The DOTS should provision an ACL policy that restricts access to the"/oic/d" resource such that only authenticated Clients are able to obtain the di Property of "/oic/d" Resource. See clause 13.1 for deviceuuid Property lifecycle requirements.

Servers should expose a temporary, non-repeated, piid Property of "/oic/p" Resource Value upon entering RESET Device state. Servers shall expose a persistent value via the piid Property of
"/oic/p" Property when the DOTS sets devowneruuid Property to a non-nil-UUID value. An ACL policy on the "/oic/d" Resource should protect the piid Property of "/oic/p" Resource from being disclosed to unauthenticated requestors.

Servers shall expose a temporary, non-repeated, pi Property value upon entering RESET Device state. Servers shall expose a persistent or semi-persistent platform identifier value via the pi Property of the "/oic/p" Resource when onboarding sets devowneruuid Property to a non-nil-UUID value. An ACL policy on the "/oic/p" Resource should protect the pi Property from being disclosed to unauthenticated requestors.

Table 74 depicts Core Resource Properties Access Modes given various Device States.

Table 74 – Core Resource Properties Access Modes given various Device States

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Property title</th>
<th>Property name</th>
<th>Value type</th>
<th>Access Mode</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>oic.wk.p</td>
<td>Platform ID</td>
<td>pi</td>
<td>oic.types-schema.uuid</td>
<td>All States</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server shall construct a temporary random UUID (The temporary value shall not overwrite the persistent pi internally). Server sets to its persistent value after secure Owner Transfer session is established.</td>
</tr>
<tr>
<td>oic.wk.d</td>
<td>Protocol Independent Identifier</td>
<td>piid</td>
<td>oic.types-schema.uuid</td>
<td>All States</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server should construct a temporary random UUID when entering RESET state.</td>
</tr>
<tr>
<td>oic.wk.d</td>
<td>Device Identifier</td>
<td>di</td>
<td>oic.types-schema.uuid</td>
<td>All States</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/d di shall mirror the value contained in /doxm deviceuuid in all device states.</td>
</tr>
</tbody>
</table>

Four identifiers are thought to be privacy sensitive:

- "/oic/d" Resource containing the "di" and "piid" Properties.
- "/oic/p" Resource containing the "pi" Property.
- "/oic/sec/doxm" Resource containing the "deviceuuid" Property.

There are three strategies for privacy protection of Devices:

1) Apply access control to restrict read access to Resources containing unique identifiers. This ensures privacy sensitive identifiers do not leave the Device.
2) Limit identifier persistence to make it impractical for tracking use. This ensures privacy sensitive identifiers are less effective for tracking and correlation.
3) Confidentiality protect the identifiers. This ensures only those authorized to see the value can do so.

These techniques can be used to limit exposure to privacy attacks. For example:

- ACL policies that restrict anonymous requestors from accessing persistent / semi-persistent identifiers can be created.
- A temporary identifier can be used instead of a persistent or semi-persistent identifier to facilitate onboarding.
- Persistent and semi-persistent identifiers can be encrypted before sending them to another Device.
A temporary, non-repeated identifier shall be:

1) Disjoint from (i.e. not linked to) the persistent or semi-persistent identifiers
2) Generated by a function that is pre-image resistant, second pre-image resistant and collision resistant

NOTE This requirement is met through a vendor attestation certification mechanism.

### 13.16.2 Privacy Protecting the Device Identifiers

The "di" Property Value of the "/oic/d" Resource shall mirror that of the "deviceuuid" Property of the "/oic/sec/doxm" Resource. The Device should use a new, temporary non-repeated identifier in place of the "deviceuuid" Property Value of "/oic/sec/doxm" Resource upon entering the RESET Device state. This value should be exposed while the "devowneruuid" Property has a nil UUID value. The Device should expose its persistent (or semi-persistent) "deviceuuid" Property value of the "/oic/sec/doxm" Resource after the DOTS sets the "devowneruuid" Property to a non-nil-UUID value. The temporary identifier should not change more frequently than once per Device state transition to RESET.

Subsequent to the "devowneruuid" being UPDATED to a non-nil UUID:

- If constructing a CRUDN response for any Resource that contains the "deviceuuid" and/or "di" Property values:
  - The Device should include its persistent (or semi-persistent) "deviceuuid" (or "di") Property value only if responding to an authenticated requestor and the "deviceuuid" (or "di") value is confidentiality protected.
  - The Device should use a temporary non-repeated "deviceuuid" (or "di") Property value if responding to an unauthenticated requestor.
- The AMS should provision an ACL policy on the "/oic/sec/doxm" and "/oic/d" resources to further protect the "deviceuuid" and "di" Properties from being disclosed unnecessarily.

See 13.2 for deviceuuid Property lifecycle requirements.

NOTE A Client Device can avoid disclosing its persistent (or semi-persistent) identifiers by avoiding unnecessary discovery requests. This is achieved by provisioning a "/oic/sec/cred" Resource entry that contains the Server's deviceuuid Property value. The Client establishes a secure connection to the Server straight away.

### 13.16.3 Privacy Protecting the Protocol Independent Device Identifier

The Device should use a new, temporary non-repeated identifier in place of the "piid" Property Value of "/oic/d" Resource upon entering the RESET Device state. If a temporary, non-repeated value has been generated, it should be used while the "devowneruuid" Property has the nil UUID value. The Device should use its persistent "piid" Property value after the DOTS sets the "devowneruuid" Property to a non-nil-UUID value. The temporary identifier should not change more frequently than once per Device state transition to RESET.

Subsequent to the "devowneruuid" being UPDATED to a non-nil UUID:

- If constructing a CRUDN response for any Resource that contains the "piid" Property value:
  - The Device should include its persistent "piid" Property value only if responding to an authenticated requestor and the "piid" value is confidentiality protected.
  - The Device should include a temporary non-repeated "piid" Property value if responding to an unauthenticated requestor.
- The AMS should provision an ACL policy on the "/oic/d" Resource to further protect the piid Property of "/oic/p" Resource from being disclosed unnecessarily.
13.16.4 Privacy Protecting the Platform Identifier

The Device should use a new, temporary non-repeated identifier in place of the "pi" Property Value of the "/oic/p" Resource upon entering the RESET Device state. This value should be exposed while the "devowneruuid" Property has a nil UUID value. The Device should use its persistent (or semi-persistent) "pi" Property value after the DOTS sets the "devowneruuid" Property to a non-nil-UUID value. The temporary identifier should not change more frequently than once per Device state transition to RESET.

Subsequent to the "devowneruuid" being UPDATED to a non-nil UUID:

- If constructing a CRUDN response for any Resource that contains the "pi" Property value:
  - The Device should include its persistent (or semi-persistent) "pi" Property value only if responding to an authenticated requestor and the "pi" value is confidentiality protected.
  - The Device should include a temporary non-repeated "pi" Property value if responding to an unauthenticated requestor.
  - The AMS should provision an ACL policy on the "/oic/p" Resource to protect the pi Property from being disclosed unnecessarily.

13.17 Easy Setup Resource Device State

This clause only applies to a new Device that uses Easy Setup for ownership transfer as defined in OCF Wi-Fi Easy Setup. Easy Setup has no impact to new Devices that have a different way of connecting to the network i.e. DOTS and AMS don't use a Soft AP to connect to non-Easy Setup Devices.

Figure 39 shows an example of Soft AP and Easy Setup Resource in different Device states.

Device enters RFOTM Device state, Soft AP may be accessible in RFOTM and RFPRO Device's state.

While it is reasonable for a user to expect that power cycling a new Device will turn on the Soft AP for Easy Setup during the initial setup, since that is potentially how it behaved on first boot, it is a security risk to make this the default behaviour of a device that remains unenrolled beyond a reasonable period after first boot.

Therefore, the Soft AP for Easy Setup has several requirements to improve security:
– Time availability of Easy Setup Soft AP should be minimised, and shall not exceed 30 minutes after Device factory reset RESET or first power boot, or when user initiates the Soft AP for Easy Setup.

– If a new Device tried and failed to complete Easy Setup Enrolment immediately following the first boot, or after a factory reset, it may turn the Easy Setup Soft AP back on automatically for another 30 minutes upon being power cycled, provided that the power cycle occurs within 3 hours of first boot or the most recent factory reset. If the user has initiated the Easy Setup Soft AP directly without a factory reset, it is not necessary to turn it back on if it was on immediately prior to power cycle, because the user obviously knows how to initiate the process manually.

– After 3 hours from first boot or factory reset without successfully enrolling the device, the Soft AP should not turn back on for Easy Setup until another factory reset occurs, or the user initiates the Easy Setup Soft AP directly.

– Easy Setup Soft AP may stay enabled during RFNOP, until the Mediator instructs the new Device to connect to the Enroller.

– The Easy Setup Soft AP shall be disabled when the new Device successfully connects to the Enroller.

– Once a new Device has successfully connected to the Enroller, it shall not turn the Easy Setup Soft AP back on for Easy Setup Enrolment again unless the Device is factory reset, or the user initiates the Easy Setup Soft AP directly.

– Just Works OTM shall not be enabled on Devices which support Easy Setup.

– The Soft AP shall be secured (e.g. shall not expose an open AP).

– The Soft AP shall support a passphrase for connection by the Mediator, and the passphrase shall be between 8 and 64 ASCII printable characters. The passphrase may be printed on a label, sticker, packaging etc., and may be entered by the user into the Mediator device.

– The Soft AP should not use a common passphrase across multiple Devices. Instead, the passphrase may be sufficiently unique per device, to prevent guessing of the passphrase by an attacker with knowledge of the Device type, model, manufacturer, or any other information discoverable through Device’s exposed interfaces.

The Enrollee shall support WPA2 security (i.e. shall list WPA2 in the "swat" Property of the "/example/WiFiConfResURI" Resource), for potential selection by the Mediator in connecting the Enrollee to the Enroller. The Mediator should select the best security available on the Enroller, for use in connecting the Enrollee to the Enroller.

The Enrollee may not expose any interfaces (e.g. web server, debug port, NCRs, etc.) over the Soft AP, other than SVRs, and Resources required for Wi-Fi Easy Setup.

The "/example/EasySetupResURI" Resource should not be discoverable in RFOTM or SRESET state. After ownership transfer process is completed with the DOTS, and the Device enters in RFPRO Device state, the "/example/EasySetupResURI" may be Discoverable. The DOTS may be hosted on the Mediator Device.

The OTM CoAPS session may be used by Mediator for connection over Soft AP for ownership transfer and initial Easy Setup provisioning. SoftAP or regular network connection may be used by AMS for "/oic/sec/acl2" Resource provisioning in RFPRO state. The CoAPS session authentication and encryption is already defined in the Security spec.

In RFPRO state, AMS should configure ACL2 Resource on the Device with ACE2 for following Resources to be only configurable by the Mediator Device with permission to UPDATE or RETRIEVE access:

– /example/EasySetupResURI
An ACE2 granting RETRIEVE or UPDATE access to the Easy Setup Resource

```
{  
    "subject": { "uuid": "<insert-UUID-of-Mediator>" },  
    "resources": [  
        { "href": "/example/EasySetupResURI" },  
        { "href": "/example/WifiConfResURI" },  
        { "href": "/example/DevConfResURI" },  
    ],  
    "permission": 6 // RETRIEVE (2) or UPDATE and RETRIEVE(6)  
}
```

ACE2 may be re-configured after Easy Setup process. These ACE2s should be installed prior to the Mediator performing any RETRIEVE/UPDATE operations on these Resources.

In RFPRO or RFNOP, the Mediator should discover /EasySetupResURI Resources and UPDATE these Resources. The AMS may UPDATE /EasySetupResURI resources in RFNOP Device state.
14 Security Hardening Guidelines/Execution Environment Security

14.1 Preamble

This is an informative clause. Many TGs in OCF have security considerations for their protocols and environments. These security considerations are addressed through security mechanisms specified in the security documents for OCF. However, effectiveness of these mechanisms depends on security robustness of the underlying hardware and software Platform. This clause defines the components required for execution environment security.

14.2 Execution Environment Elements

14.2.1 Execution Environment Elements General

Execution environment within a computing Device has many components. To perform security functions in a robustness manner, each of these components has to be secured as a separate dimension. For instance, an execution environment performing AES cannot be considered secure if the input path entering keys into the execution engine is not secured, even though the partitions of the CPU, performing the AES encryption, operate in isolation from other processes. Different dimensions referred to as elements of the execution environment are listed below. To qualify as a secure execution environment (SEE), the corresponding SEE element must qualify as secure.

- (Secure) Storage
- (Secure) Execution engine
- (Trusted) Input/output paths
- (Secure) Time Source/clock
- (Random) number generator
- (Approved) cryptographic algorithms
- Hardware Tamper (protection)

NOTE Software security practices (such as those covered by OWASP) are outside scope of this document, as development of secure code is a practice to be followed by the open source development community. This document will however address the underlying Platform assistance required for executing software. Examples are secure boot and secure software upgrade.

Each of the elements above are described in the clauses 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7.

14.2.2 Secure Storage

14.2.2.1 Secure Storage General

Secure storage refers to the physical method of housing sensitive or confidential data ("Sensitive Data"). Such data could include but not be limited to symmetric or asymmetric private keys, certificate data, OCF Security Domain access credentials, or personal user information. Sensitive Data requires that its integrity be maintained, whereas Critical Sensitive Data requires that both its integrity and confidentiality be maintained.

It is strongly recommended that IoT Device makers provide reasonable protection for Sensitive Data so that it cannot be accessed by unauthorized Devices, groups or individuals for either malicious or benign purposes. In addition, since Sensitive Data is often used for authentication and encryption, it must maintain its integrity against intentional or accidental alteration.

A partial list of Sensitive Data is outlined in Table 75:
Table 75 – Examples of Sensitive Data

<table>
<thead>
<tr>
<th>Data</th>
<th>Integrity protection</th>
<th>Confidentiality protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner PSK (Symmetric Keys)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Service provisioning keys</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asymmetric Private Keys</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Data and Signed Hashes</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Public Keys</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Access credentials (e.g. SSID, passwords, etc.)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ECDH/ECDH Dynamic Shared Key</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Root CA Public Keys</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Device and Platform IDs</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Easy Setup Resources</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OCF Cloud URL</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>OCF Cloud Identity</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Access Token</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Exact method of protection for secure storage is implementation specific, but typically combinations of hardware and software methods are used.

14.2.2.2 Hardware Secure Storage

Hardware secure storage is recommended for use with critical Sensitive Data such as symmetric and asymmetric private keys, access credentials, and personal private data. Hardware secure storage most often involves semiconductor-based non-volatile memory ("NVRAM") and includes countermeasures for protecting against unauthorized access to Critical Sensitive Data.

Hardware-based secure storage not only stores Sensitive Data in NVRAM, but also provides protection mechanisms to prevent the retrieval of Sensitive Data through physical and/or electronic attacks. It is not necessary to prevent the attacks themselves, but an attempted attack should not result in an unauthorized entity successfully retrieving Sensitive Data.

Protection mechanisms should provide JIL Moderate protection against access to Sensitive Data from attacks that include but are not limited to:

1) Physical decapping of chip packages to optically read NVRAM contents
2) Physical probing of decapped chip packages to electronically read NVRAM contents
3) Probing of power lines or RF emissions to monitor voltage fluctuations to discern the bit patterns of Critical Sensitive Data
4) Use of malicious software or firmware to read memory contents at rest or in transit within a microcontroller
5) Injection of faults that induce improper Device operation or loss or alteration of Sensitive Data

14.2.2.3 Software Storage

It is generally NOT recommended to rely solely on software and unsecured memory to store Sensitive Data even if it is encrypted. Critical Sensitive Data such as authentication and encryption keys should be housed in hardware secure storage whenever possible.
Sensitive Data stored in volatile and non-volatile memory shall be encrypted using acceptable algorithms to prevent access by unauthorized parties through methods described in 14.2.2.2.

14.2.2.4 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.r.cred" Resource entries, since this opens up an identity spoofing opportunity.

6) Device vendor understands that it is the Device vendor’s responsibility to ensure the Device meets security requirements for its intended uses. As an example, IoTivity is a reference implementation intended to be used as a basis for a product, but IoTivity has not undergone 3rd party security review, penetration testing, etc. Any Device based on IoTivity should undergo appropriate penetration testing and security review prior to sale or deployment.

7) Device vendor agrees to publish the expected support lifetime for the Device to OCF and to consumers. Changes should be made to a public and accessible website. Expectations should be clear as to what will be supported and for how long the Device vendor expects to support security updates to the software, operating system, drivers, networking, firmware and hardware of the device.

8) Device vendor has not implemented test or debug interfaces on the Device which are operable or which can be enabled which might present an attack vector on the Device which circumvents the interface-level security or access policies of the Device.

9) Device vendor understands that if an application running on the Device has access to cryptographic elements such as the private keys or Ownership Credential, then those elements have become vulnerable. If the Device vendor is implementing a Bridge, an OBT, or a Device with access to the Internet beyond the local network, the execution of critical functions should take place within a Trusted or Secure Execution Environment (TEE/SEE).

10) Any PINS or fixed passphrases used for onboarding, Wi-Fi Easy Setup, SoftAP management or access, or other security-critical function, should be sufficiently unique (do not duplicate passphrases. The creation of these passphrases or PINS should not be algorithmically deterministic nor should they use insufficient entropy in their creation.

11) Ensure that there are no remaining "VENDOR_TODO" items in the source code.
12) If the implementation of this document uses the "Just Works" onboarding method, understand that there is a man-in-the-middle vulnerability during the onboarding process where a malicious party could intercept messages between the device being onboarded and the OBT and could persist, acting as an intermediary with access to message traffic, during the lifetime of that onboarded device. The recommended best practice would be to use an alternate ownership transfer method (OTM) instead of "Just Works".

13) It is recommended that at least one static and dynamic analysis tool\(^1\) be applied to any proposed major production release of the software before its release, and any vulnerabilities resolved.

14) To avoid a malicious device being able to covertly join an OCF Security Domain, implementers of any OBT may eliminate completely autonomous sequences where a device is brought into the OCF Security Domain without any authorization by the owner. Consider either including a confirmation with the OCF Security Domain owner/operator (e.g. "Do you want to add 'LIGHTBULB 80' from manufacturer 'GenericLightingCo'? Yes/No/Cancel?") or a confirmation with a security policy (e.g. an enterprise policy where the OCF Security Domain admin can bulk-onboard devices).

14.2.3 Secure execution engine

Execution engine is the part of computing Platform that processes security functions, such as cryptographic algorithms or security protocols (e.g. DTLS). Securing the execution engine requires the following:

- Isolation of execution of sensitive processes from unauthorized parties/ processes. This includes isolation of CPU caches, and all of execution elements that needed to be considered as part of trusted (crypto) boundary.

- Isolation of data paths into and out of execution engine. For instance, both unencrypted but sensitive data prior to encryption or after decryption, or cryptographic keys used for cryptographic algorithms, such as decryption or signing. See clause 14.2.4 for more details.

14.2.4 Trusted input/output paths

Paths/ ports used for data entry into or export out of trusted/ crypto-boundary needs to be protected. This includes paths into and out secure execution engine and secure memory.

Path protection can be both hardware based (e.g. use of a privileged bus) or software based (using encryption over an untrusted bus).

14.2.5 Secure clock

Many security functions depend on time-sensitive credentials. Examples are time stamped Kerberos tickets, OAUTH tokens, X.509 certificates, OSCP response, software upgrades, etc. Lack of secure source of clock can mean an attacker can modify the system clock and fool the validation mechanism. Thus an SEE needs to provide a secure source of time that is protected from tampering. Trustworthiness from security robustness standpoint is not the same as accuracy. Protocols such as NTP can provide rather accurate time sources from the network, but are not immune to attacks. A secure time source on the other hand can be off by seconds or minutes depending on the time-sensitivity of the corresponding security mechanism. Secure time source can be external as long as it is signed by a trusted source and the signature validation in the local Device is a trusted process (e.g. backed by secure boot).

14.2.6 Approved algorithms

An important aspect of security of the entire ecosystem is the robustness of publicly vetted and peer-reviewed (e.g. NIST-approved) cryptographic algorithms. Security is not achieved by obscurity of the cryptographic algorithm. To ensure both interoperability and security, not only

---

\(^1\) A general discussion of analysis tools can be found here: https://www.ibm.com/developerworks/library/se-static/
widely accepted cryptographic algorithms must be used, but also a list of approved cryptographic
functions must be specified explicitly. As new algorithms are NIST approved or old algorithms are
deprecated, the list of approved algorithms must be maintained by OCF. All other algorithms
(even if they deemed stronger by some parties) must be considered non-approved.

The set of algorithms to be considered for approval are algorithms for

- Hash functions
- Signature algorithms
- Encryption algorithms
- Key exchange algorithms
- Pseudo Random functions (PRF) used for key derivation

This list will be included in this or a separate security robustness rules document and must be
followed for all security specifications within OCF.

14.2.7 Hardware tamper protection

Various levels of hardware tamper protection exist. We borrow FIPS 140-2 terminology (not
requirements) regarding tamper protection for cryptographic module

- Production-grade (lowest level): this means components that include conformal sealing
  coating applied over the module’s circuitry to protect against environmental or other physical
damage. This does not however require zeroization of secret material during physical
maintenance. This definition is borrowed from FIPS 140-2 security level 1.
- Tamper evident/proof (mid-level): This means the Device shows evidence (through covers,
  enclosures, or seals) of an attempted physical tampering. This definition is borrowed from
  FIPS 140-2 security level 2.
- Tamper resistance (highest level), this means there is a response to physical tempering that
  typically includes zeroization of sensitive material on the module. This definition is borrowed
  from FIPS 140-2 security level 3.

It is difficult of specify quantitative certification test cases for accreditation of these levels.
Content protection regimes usually talk about different tools (widely available, specialized and
professional tools) used to circumvent the hardware protections put in place by manufacturing. If
needed, OCF can follow that model, if and when OCF engage in distributing sensitive key
material (e.g. PKI) to its members.

14.3 Secure Boot

14.3.1 Concept of software module authentication

In order to ensure that all components of a Device are operating properly and have not been
tampered with, it is best to ensure that the Device is booted properly. There may be multiple
stages of boot. The end result is an application running on top an operating system that takes
advantage of memory, CPU and peripherals through drivers.

The general concept is that each software module is invoked only after cryptographic integrity
verification is complete. The integrity verification relies on the software module having been
hashed (e.g. SHA_1, SHA_256) and then signed with a cryptographic signature algorithm with
(e.g. RSA), with a key that only a signing authority has access to.

Figure 40 depicts software module authentication.
After the data is signed with the signer’s signing key (a private key), the verification key (the public key corresponding to the private signing key) is provided for later verification. For lower level software modules, such as bootloaders, the signatures and verification keys are inserted inside tamper proof memory, such as one-time programmable memory or TPM. For higher level software modules, such as application software, the signing is typically performed according to the PKCS#7 format IETF RFC 2315, where the signedData format includes both indications for signature algorithm, hash algorithm as well as the signature verification key (or certificate). Secure boot does not require use of PKCS#7 format.

Figure 41 depicts verification software module.

As shown in Figure 42, the verification module first decrypts the signature with the verification key (public key of the signer). The verification module also calculates a hash of the data and then compares the decrypted signature (the original) with the hash of data (actual) and if the two values match, the software module is authentic.
14.3.2 Secure Boot process

Depending on the Device implementation, there may be several boot stages. Typically, in a PC/Linux type environment, the first step is to find and run the BIOS code (first-stage bootloader) to find out where the boot code is and then run the boot code (second-stage boot loader). The second stage bootloader is typically the process that loads the operating system (Kernel) and transfers the execution to the where the Kernel code is. Once the Kernel starts, it may load external Kernel modules and drivers.

When performing a secure boot, it is required that the integrity of each boot loader is verified before executing the boot loader stage. As mentioned, while the signature and verification key for the lowest level bootloader is typically stored in tamper-proof memory, the signature and verification key for higher levels should be embedded (but attached in an easily accessible manner) in the data structures software.

14.3.3 Robustness Requirements

14.3.3.1 Robustness General

To qualify as high robustness secure boot process, the signature and hash algorithms shall be one of the approved algorithms, the signature values and the keys used for verification shall be stored in secure storage and the algorithms shall run inside a secure execution environment and the keys shall be provided the SEE over trusted path.

14.3.3.2 Next steps

Develop a list of approved algorithms and data formats

14.4 Attestation

14.5 Software Update

14.5.1 Overview:

The Device lifecycle does not end at the point when a Device is shipped from the manufacturer; the distribution, retailing, purchase, installation/onboarding, regular operation, maintenance and end-of-life stages for the Device remain outstanding. It is possible for the Device to require
update during any of these stages, although the most likely times are during onboarding, regular
operation and maintenance. The aspects of the software include, but are not limited to, firmware,
operating system, networking stack, application code, drivers, etc.

14.5.2 Recognition of Current Differences
Different manufacturers approach software update utilizing a collection of tools and strategies:
over-the-air or wired USB connections, full or partial replacement of existing software, signed and
verified code, attestation of the delivery package, verification of the source of the code, package
structures for the software, etc.

It is recommended that manufacturers review their processes and technologies for compliance
with industry best-practices that a thorough security review of these takes place and that periodic
review continue after the initial architecture has been established.

This document applies to software updates as recommended to be implemented by Devices; it
does not have any bearing on the above-mentioned alternative proprietary software update
mechanisms.

14.5.3 Software Version Validation
Setting the Initiate Software Version Validation bit in the "/oic/sec/pstat.tm" Property (see
Table 57 defines the Properties of "oic.r.pstat".

Table 57 of 13.8) indicates a request to initiate the software version validation process, the
process whereby the Device validates the software (including firmware, operating system, Device
drivers, networking stack, etc.) against a trusted source to see if, at the conclusion of the check,
the software update process will need to be triggered (see clause 14.5.4). When the Initiate
Software Version Validation bit of "/oic/sec/pstat.tm" is set to 1 (TRUE) by a sufficiently privileged
Client, the Device sets the "/oic/sec/pstat.cm" Initiate Software Version Validation bit to 0 and
initiates a software version check. Once the Device has determined if an update is available, it
sets the Initiate Software Version Validation bit in the "/oic/sec/pstat.cm" Property to 1 (TRUE) if
an update is available or 0 (FALSE) if no update is available. To signal completion of the
Software Version Validation process, the Device sets the Initiate Software Version Validation bit
in the "/oic/sec/pstat.cm" Property back to 0 (FALSE). If the Initiate Software Version Validation
bit of "/oic/sec/pstat.tm" is set to 0 (FALSE) by a Client, it has no effect on the validation process.

14.5.4 Software Update
Setting the Initiate Secure Software Update bit in the "/oic/sec/pstat.tm" Property (see Table 57
defines the Properties of "oic.r.pstat".

Table 57 of 13.8) indicates a request to initiate the software update process. When the Initiate
Secure Software Update bit of "/oic/sec/pstat.tm" is set to 1 (TRUE) by a sufficiently privileged
Client, the Device sets the "/oic/sec/pstat.cm" Initiate Software Version Validation bit to 0 and
initiates a software update process. Once the Device has completed the software update process,
it sets the Initiate Secure Software Update bit in the "/oic/sec/pstat.cm" Property to 1 (TRUE)
if/when the software was successfully updated or 0 (FALSE) if no update was performed. To
signal completion of the Secure Software Update process, the Device sets the Initiate Secure
Software Update bit in the "/oic/sec/pstat.tm" Property back to 0 (FALSE). If the Initiate Secure
Software Update bit of "/oic/sec/pstat.tm" is set to 0 (FALSE) by a Client, it has no effect on the
update process.

14.5.5 Recommended Usage
The Initiate Secure Software Update bit of "/oic/sec/pstat.tm" should only be set by a Client after
the Initiate Software Version Validation check is complete.
The process of updating Device software may involve state changes that affect the Device Operational State ("/oic/sec/pstat.dos"). Devices with an interest in the Device(s) being updated should monitor "/oic/sec/pstat.dos" and be prepared for pending software update(s) to affect Device state(s) prior to completion of the update.

The Device itself may indicate that it is autonomously initiating a software version check/update or that a check/update is complete by setting the pstat.tm and pstat.cm Initiate Software Version Validation and Secure Software Update bits when starting or completing the version check or update process. As is the case with a Client-initiated update, Clients can be notified that an autonomous version check or software update is pending and/or complete by observing pstat resource changes.

14.6 Non-OCF Endpoint interoperability

14.7 Security Levels

Security Levels are a way to differentiate Devices based on their security criteria. This need for differentiation is based on the requirements from different verticals such as industrial and healthcare and may extend into smart home. This differentiation is distinct from Device classification (e.g. IETF RFC 7228)

These categories of security differentiation may include, but is not limited to:

1) Security Hardening
2) Identity Attestation
3) Certificate/Trust
4) Onboarding Technique
5) Regulatory Compliance
   a) Data at rest
   b) Data in transit
6) Cipher Suites – Crypto Algorithms & Curves
7) Key Length
8) Secure Boot/Update

In the future security levels can be used to define interoperability.

The following applies to the OCF Security Specification 1.1:

The current document does not define any other level beyond Security Level 0. All Devices will be designated as Level 0. Future versions may define additional levels.

Additional comments:

- The definition of a given security level will remain unchanged between versions of the document.
- Devices that meet a given level may, or may not, be capable of upgrading to a higher level.
- Devices may be evaluated and re-classified at a higher level if it meets the requirements of the higher level (e.g. if a Device is manufactured under the 1.1 version of the document, and a later document version defines a security level 1, the Device could be evaluated and classified as level 1 if it meets level 1 requirements).
- The security levels may need to be visible to the end user.
14.8 Security Profiles

14.8.1 Security Profiles General

Security Profiles are a way to differentiate OCF Devices based on their security criteria. This need for differentiation is based on the requirements from different verticals such as industrial and health care and may extend into smart home. This differentiation is distinct from device classification (e.g., IETF RFC 7228).

These categories of security differentiation may include, but is not limited to:

1) Security Hardening and assurances criteria
2) Identity Attestation
3) Certificate/Trust
4) Onboarding Technique
5) Regulatory Compliance
   a) Data at rest
   b) Data in transit
6) Cipher Suites – Crypto Algorithms & Curves
7) Key Length
8) Secure Boot/Update

Each Security Profile definition must specify the version or versions of the OCF Security Specification(s) that form a baseline set of normative requirements. The profile definition may include security requirements that supersede baseline requirements (not to relax security requirements).

Security Profiles have the following properties:

- A given profile definition is not specific to the version of the document that defines it. For example, the profile may remain constant for subsequent OCF Security Specification versions.
- A specific OCF Device and platform combination may be used to satisfy the security profile.
- Profiles may have overlapping criteria; hence it may be possible to satisfy multiple profiles simultaneously.
- An OCF Device that satisfied a profile initially may be re-evaluated at a later time and found to satisfy a different profile (e.g., if a device is manufactured under the 1.1 version of the document, and a later document version defines a security profile Black, the device could be evaluated and classified as profile Black if it meets profile Black requirements).
- A machine-readable representation of compliance results specifically describing profiles satisfied may be used to facilitate OCF Device onboarding. (e.g., a manufacturer certificate or manifest may contain security profiles attributes).

14.8.2 Identification of Security Profiles (Normative)

14.8.2.1 Security Profiles in Prior Documents

OCF Devices conforming to versions of the OCF Security Specifications where Security Profiles Resource was not defined may be presumed to satisfy the "sp-baseline-v0" profile (defined in 14.8.3.3) or may be regarded as unspecified. If Security Profile is unspecified, the Client may use the OCF Security Specification version to characterize expected security behaviour.

14.8.2.2 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 Specification.
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 76 – Definition of the "oic.sec.sp" Resource

<table>
<thead>
<tr>
<th>Fixed URI</th>
<th>Resource Type Title</th>
<th>Resource Type ID &quot;(rt&quot; value)</th>
<th>OCF Interfaces</th>
<th>Description</th>
<th>Related Functional Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>/oic/sec/sp</td>
<td>Security Profile Resource Definition</td>
<td>oic.r.sp</td>
<td>oic.if.baseline</td>
<td>Resource specifying supported and current security profile(s)</td>
<td>Discoverable</td>
</tr>
</tbody>
</table>

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

### Table 77 – Properties of the "oic.sec.sp" Resource

<table>
<thead>
<tr>
<th>Property Title</th>
<th>Property Name</th>
<th>Value Type</th>
<th>Value Rule</th>
<th>Access Mode</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Security Profiles</td>
<td>supportedprofiles</td>
<td>ocfSecurityProfileOID</td>
<td>array</td>
<td>RW</td>
<td>Yes</td>
<td>Array of supported Security Profiles (e.g. &quot;1.3.6.1.4.1.51414.0.0.2.0&quot;, &quot;1.3.6.1.4.1.51414.0.0.3.0&quot;)</td>
</tr>
<tr>
<td>SecurityProfile</td>
<td>currentprofile</td>
<td>ocfSecurityProfileOID</td>
<td>N/A</td>
<td>RW</td>
<td>Yes</td>
<td>Currently active Security Profile (e.g. &quot;1.3.6.1.4.1.51414.0.0.3.0&quot;)</td>
</tr>
</tbody>
</table>

The following OIDs are defined to uniquely identify Security Profiles. Future Security Profiles or changes to existing Security Profiles may result in a new ocfSecurityProfileOID.

```plaintext
id-OCF OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) OCF(51414) }

id-ocfSecurity OBJECT IDENTIFIER ::= { id-OCF 0 }

id-ocfSecurityProfile ::= { id-ocfSecurity 0 }

sp-unspecified ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 0 } --The Security Profile is not specified
sp-baseline ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 1 } --This specifies the OCF Baseline Security Profile(s)
sp-black ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 2 } --This specifies the OCF Black Security Profile(s)
sp-blue ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 3 } --This specifies the OCF Blue Security Profile(s)
sp-purple ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 4 } --This specifies the OCF Purple Security Profile(s)

sp-unspecified-v0 ::= ocfSecurityProfileOID {id-sp-unspecified 0}
sp-baseline-v0 ::= ocfSecurityProfileOID {id-sp-baseline 0}
sp-black-v0 ::= ocfSecurityProfileOID {id-sp-black 0}
sp-blue-v0 ::= ocfSecurityProfileOID {id-sp-blue 0}
sp-purple-v0 ::= ocfSecurityProfileOID {id-sp-purple 0}

ocfSecurityProfileOID ::= UTF8String
```


14.8.3  Security Profiles

14.8.3.1  Security Profiles General

The Security Profiles Resource shall be pre-populated with manufacturer default values (Refer to the Security Profile clauses for additional details).

The OCF Conformance criteria may require vendor attestation that establishes the expected environment in which the OCF Device is hosted (Refer to the Security Profile clauses for specific requirements).

14.8.3.2  Security Profile Unspecified (sp-unspecified-v0)

The Security Profile "sp-unspecified-v0" is reserved for future use.

14.8.3.3  Security Profile Baseline v0 (sp-baseline-v0)

The Security Profile "sp-baseline-v0" is defined for all OCF Security Specification versions where the "/oic/sec/sp" Resource is defined. All Devices shall include the "sp-baseline-v0" OID in the "supportedprofiles" Property of the "/oic/sec/sp" Resource.

It indicates the OCF Device satisfies the normative security requirements for this document.

When a device supports the baseline profile, the "supportedprofiles" Property shall contain sp-baseline-v0, represented by the OID string "1.3.6.1.4.1.51414.0.0.1.0", and may contain other profiles.

When a manufacturer makes sp-baseline-v0 the default, by setting the "currentprofile" Property to "1.3.6.1.4.1.51414.0.0.1.0", the "supportedprofiles" Property shall contain sp-baseline-v0.

14.8.3.4  Security Profile Black (sp-black-v0)

14.8.3.4.1  Black Profile General

The need for Security Profile Black v0 is to support devices and manufacturers who wish to certify their devices meeting this specific set of security criteria. A Device may satisfy the Black requirements as well as requirements of other profiles, the Black Security Profile is not necessarily mutually exclusive with other Security Profiles unless those requirements conflict with the explicit requirements of the Black Security Profile.

14.8.3.4.2  Devices Targeted for Security Profile Black v0

Security Profile Black devices could include any device a manufacturer wishes to certify at this profile, but healthcare devices and industrial devices with additional security requirements are the initial target. Additionally, manufacturers of devices at the edge of the network (or fog), or devices with exceptional profiles of trust bestowed upon them, may wish to certify at this profile; these types of devices may include, but are not limited to the following:

- Bridges (Mapping devices between ecosystems handling virtual devices from different ecosystems)
- Resource Directories (Devices trusted to manage OCF Security Domain resources)
- Remote Access (Devices which have external access but can also act within the OCF Security Domain)
- Healthcare Devices (Devices with specific requirements for enhanced security and privacy)
- Industrial Devices (Devices with advanced management, security and attestation requirements)
14.8.3.4.3 Requirements for Certification at Security Profile Black (Normative)

Every device with "currentprofile" Property of the "/oic/sec/sp" Resource designating a Security Profile of "sp-black-v0", as defined in clause 14.8.2, must support each of the following:

- Onboarding via OCF Rooted Certificate Chain, including PKI chain validation
- Support for AES 128 encryption for data at rest and in transit.
- Hardening minimums: manufacturer assertion of secure credential storage
- In 14) in enumerated item #10 “The "/oic/sec/cred" Resource should contain credential(s) if required by the selected OTM” is changed to require the credential be stored: “The "/oic/sec/cred" Resource shall contain credential(s).”
- The OCF Device shall include an X.509v3 OCF Compliance Extension (clause 9.4.2.2.4) in its certificate and the extension's 'securityProfile' field shall contain sp-black-v0 represented by the ocfSecurityProfileOID string, "1.3.6.1.4.1.51414.0.0.2.0".

When a device supports the black profile, the "supportedprofiles" Property shall contain sp-black-v0, represented by the OID string "1.3.6.1.4.1.51414.0.0.2.0", and may contain other profiles.

When a manufacturer makes sp-black-v0 the default, by setting the "currentprofile" Property to "1.3.6.1.4.1.51414.0.0.2.0", the "supportedprofiles" Property shall contain sp-black-v0.

The OCF Rooted Certificate Chain and PKI is defined by and structured within a framework described in the supporting documents:

- Certificate Profile (See 9.4.2)

14.8.3.5 Security Profile Blue v0 (sp-blue-v0)

14.8.3.5.1 Blue Profile General

The Security Profile Blue is used when manufacturers issue platform certificates for platforms containing manufacturer-embedded keys. Compatibility with interoperable trusted platforms is anticipated using certificate extensions defined by the Trusted Computing Group (TCG). OCF Security Domain owners evaluate manufacturer supplied certificates and attributed data to determine an appropriate OCF Security Profile that is configured for OCF Devices at onboarding. OCF Devices may satisfy multiple OCF Security Profiles. The OCF Security Domain owner may configure deployments using the Security Profile as OCF Security Domain partitioning criteria.

Certificates issued to Blue Profile Devices shall be issued by a CA conforming to the CA Vetting Criteria defined by OCF.

14.8.3.5.2 Platforms and Devices for Security Profile Blue v0

The OCF Security Profile Blue anticipates an ecosystem where platform vendors may differ from OCF Device vendor and where platform vendors may implement trusted platforms that may conform to industry standards defining trusted platforms. The OCF Security Profile Blue specifies mechanisms for linking platforms with OCF Device(s) and for referencing quality assurance criteria produced by OCF conformance operations. The OCF Security Domain owner evaluates these data when an OCF Device is onboarded into the OCF Security Domain. Based on this evaluation the OCF Security Domain owner determines which Security Profile may be applied during OCF Device operation. All OCF Device types may be considered for evaluation using the OCF Security Profile Blue.

14.8.3.5.3 Requirements for Certification at Security Profile Blue v0

The OCF Device satisfies the Blue profile v0 (sp-blue-v0) when all of the security normative for this document version are satisfied and the following additional criteria are satisfied.
OCF Blue profile defines the following OCF Device quality assurances:

- The OCF Conformance criteria shall require vendor attestation that the conformant OCF Device was hosted on one or more platforms that satisfies OCF Blue platform security assurances and platform security and privacy functionality requirements.
- The OCF Device achieving OCF Blue Security Profile compliance will be registered by OCF and published by OCF in a machine readable format.
- The OCF Blue Security Profile compliance registry may be digitally signed by an OCF owned signing key.
- The OCF Device shall include an X.509v3 OCF Compliance Extension (clause 9.4.2.2.4) in its certificate and the extension's 'securityProfile' field shall contain sp-blue-v0 represented by the ocfSecurityProfileOID string, "1.3.6.1.4.1.51414.0.0.3.0".
- The OCF Device shall include an X.509v3 OCF CPL Attributes Extension (clause 9.4.2.2.7) in its certificate.
- The OBT shall perform a look up of the certification status of the OCF Device using the OCF CPL Attributes Extension values and verify that the sp-blue-v0 OID is listed in the extension's "securityprofiles" field.

OCF Blue profile defines the following OCF Device security functionality:

- OCF Device(s) shall be hosted on a platform where a cryptographic and secure storage functions are hardened by the platform.
- OCF Device(s) hosted on a platform shall expose accompanying manufacturer credentials using the "/oic/sec/cred" Resource where the "credusage" Property contains the value "oic.sec.cred.mfgcert".
- OCF Device(s) that are hosted on a TCG-defined trusted platform should use an IEEE802.1AR IDevID and should verify the "TCG Endorsement Key Credential". All TCG-defined manufacturer credentials may be identified by the "oic.sec.cred.mfgcert" value of the "credusage" Property of the "/oic/sec/cred" Resource. They may be used in response to selection of the "oic.sec.doxm.mfgcert" owner transfer method.
- OCF Device(s) shall use AES128 equivalent minimum protection for transmitted data. (See NIST SP 800-57).
- OCF Device(s) shall use AES128 equivalent minimum protection for stored data. (See NIST SP 800-57).
- OCF Device(s) should use AES256 equivalent minimum protection for stored data. (See NIST SP 800-57).
- OCF Device(s) should protect the "/oic/sec/cred" resource using the platform provided secure storage.
- OCF Device(s) shall protect trust anchors (aka policy defining trusted CAs and pinned certificates) using platform provided secure storage.
- OCF Device(s) should check certificate revocation status for locally issued certificates.
- OCF OBTs (aka DOTS) shall check certificate revocation status for all certificates in manufacturer certificate path(s) if available. If a certificate is revoked, certificate validation fails and the connection is refused. The DOTS may disregard revocation status results if unavailable.

OCF Blue profile defines the following platform security assurances:

- Platforms implementing cryptographic service provider (CSP) functionality and secure storage functionality should be evaluated with a minimum FIPS140-2 Level 2 or Common Criteria EAL Level 2.
Platforms implementing trusted platform functionality should be evaluated with a minimum Common Criteria EAL Level 1.

OCF Blue profile defines the following platform security and privacy functionality:

- The Platform shall implement cryptographic service provider (CSP) functionality.
- Platform CSP functionality shall include cryptographic algorithms, random number generation, secure time.
- The Platform shall implement AES128 equivalent protection for transmitted data. (See NIST SP 800-57).
- The Platform shall implement AES128 and AES256 equivalent protection for stored data. (See NIST SP 800-57).
- Platforms hosting OCF Device(s) should implement a platform identifier following IEEE802.1AR or Trusted Computing Group (TCG) specifications.
- Platforms based on Trusted Computing Group (TCG) platform definition that host OCF Device(s) should supply TCG-defined manufacture certificates; also known as "TCG Endorsement Key Credential" (which complies with IETF RFC 5280) and "TCG Platform Credential" (which complies with IETF RFC 5755).

When a device supports the blue profile, the "supportedprofiles" Property shall contain sp-blue-v0, represented by the OID string "1.3.6.1.4.1.51414.0.0.3.0", and may contain other profiles.

When a manufacturer makes sp-blue-v0 the default, by setting the "currentprofile" Property to "1.3.6.1.4.1.51414.0.0.3.0", the "supportedprofiles" Property shall contain sp-blue-v0.

During onboarding, while the device state is RFOTM, the DOTS may update the "currentprofile" Property to one of the other values found in the "supportedprofiles" Property.

### 14.8.3.6 Security Profile Purple v0 (sp-purple-v0)

Every device with the "/oic/sec/sp" Resource designating "sp-purple-v0", as defined in clause 14.8.2 must support following minimum requirements

- Hardening minimums: secure credential storage, software integrity validation, secure update.
- If a Certificate is used, the OCF Device shall include an X.509v3 OCF Compliance Extension (clause 9.4.2.2.4) in its certificate and the extension's 'securityProfile' field shall contain sp-purple-v0 represented by the ocfSecurityProfileOID string, "1.3.6.1.4.1.51414.0.0.3.0"
- The OCF Device shall include a X.509v3 OCFCPLAttributes Extension (clause 9.4.2.2.7) in its End-Entity Certificate when manufacturer certificate is used.

Security Profile Purple has following optional security hardening requirements that the device can additionally support.

- Hardening additions: secure boot, hardware backed secure storage
- The OCF Device shall include a X.509v3 OCFSecurityClaims Extension (clause 9.4.2.2.6) in its End-Entity Certificate and it shall include corresponding OIDs to the hardening additions implemented and attested by the vendor. If there is no additional support for hardening requirements, X.509v3 OCFSecurityClaims Extension shall be omitted.

For software integrity validation, OCF Device(s) shall provide the integrity validation mechanism for security critical executables such as cryptographic modules or secure service applications, and they should be validated before the execution. The key used for validating the integrity must be pinned at the least to the validating software module.

For secure update, OCF Device(s) shall be able to update its firmware in a secure manner.
For secure boot, OCF Device(s) shall implement the BIOS code (first-stage bootloader on ROM) to be executed by the processor on power-on, and secure boot parameters to be provisioned by tamper-proof memory. Also OCF Device(s) shall provide software module authentication for the security critical executables and stop the boot process if any integrity of them is compromised.

For hardware backed secure storage, OCF Device(s) shall store sensitive data in non-volatile memory ("NVRAM") and prevent the retrieval of sensitive data through physical and/or electronic attacks.

More details on security hardening guidelines for software integrity validation, secure boot, secure update, and hardware backed secure storage are described in 14.3, 14.5 and 14.2.2.2.

Certificates issued to Purple Profile Devices shall be issued by a CA conforming to the CA Vetting Criteria defined by OCF.

When a device supports the purple profile, the "supportedprofiles" Property shall contain sp-purple-v0, represented by the OID string "1.3.6.1.4.1.51414.0.0.4.0", and may contain other profiles.

When a manufacturer makes sp-purple-v0 the default, by setting the "currentprofile" Property to "1.3.6.1.4.1.51414.0.0.4.0", the "supportedprofiles" Property shall contain sp-purple-v0.
15 Device Type Specific Requirements

15.1 Bridging Security

15.1.1 Universal Requirements for Bridging to another Ecosystem

The Bridge shall go through OCF ownership transfer as any other onboardee would.

The software of an Bridge shall be field updatable. (This requirement need not be tested but can be certified via a vendor declaration.)

Each VOD shall be onboarded by an OCF OBT. Each Virtual Bridged Device should be provisioned as appropriate in the Bridged Protocol. In other words, VODs and Virtual Bridged Devices are treated the same way as physical Devices. They are entities that have to be provisioned in their network.

Each VOD shall implement the behaviour required by ISO/IEC 30118-1:2018 and this document. Each VOD shall perform authentication, access control, and encryption according to the security settings it received from the OCF OBT. Each Virtual Bridged Device shall implement the security requirements of the Bridged Protocol.

In addition, in order to be considered secure from an OCF perspective, the Bridge Platform shall use appropriate ecosystem-specific security options for communication between the Virtual Bridged Devices instantiated by the Bridge and Bridged Devices. This security shall include mutual authentication, and encryption and integrity protection of messages in the bridged ecosystem.

A VOD may authenticate itself to the DOTS using the Manufacturer Certificate Based OTM (see clause 7.3.6) with the Manufacturer Certificate and corresponding private key of the Bridge which instantiated that VOD.

A VOD may authenticate itself to the OCF Cloud (see clause 10.5.2) using the Manufacturer Certificate and corresponding private key of the Bridge which instantiated that VOD.

15.1.2 Additional Security Requirements specific to Bridged Protocols

15.1.2.1 Additional Security Requirements specific to the AllJoyn Protocol

For AllJoyn translator, an OCF OBT shall be able to block the communication of all OCF Devices with all Bridged Devices that don’t communicate securely with the Bridge, by using the Bridge Device’s "oic.r.securemode" Resource specified in ISO/IEC 30118-3:2018

15.1.2.2 Additional Security Requirements specific to the Bluetooth LE Protocol

A Bridge shall block the communication of all OCF Devices with all Bridged Devices that don’t communicate securely with the Bridge.

15.1.2.3 Additional Security Requirements specific to the oneM2M Protocols

The Bridge shall implement oneM2M application access control as defined in the oneM2M Release 3 Specifications.

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don’t communicate securely with the Bridge.

15.1.2.4 Additional Security Requirements specific to the U+ Protocol

A Bridge shall block the communication of all OCF Devices with all Bridged Devices that don’t communicate securely with the Bridge.
15.1.2.5 Additional Security Requirements specific to the Z-Wave Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.

15.1.2.6 Additional Security Requirements specific to the Zigbee Protocol

An Bridge shall block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge.
Annex A
(informative)
Access Control Examples

Example OCF ACL Resource

Figure A-1 shows how a "/oic/sec/acl2" Resource could be configured to enforce an example access policy on the Server.

```json
{

    "aclist2": [

        // Subject with ID ...01 should access two named Resources with access mode "CRUDN" (Create, Retrieve, Update, Delete and Notify)

        "subject": {"uuid": "XXXX----XX01"},

        "resources": [

            {"href": "/oic/sh/light/1"},
            {"href": "/oic/sh/temp/0"}

        ],

        "permission": 31, // 31 dec = 0b0001 1111 which maps to ---N DURC

        "validity": [

            // The period starting at 18:00:00 UTC, on January 1, 2015 and ending at 07:00:00 UTC on January 2, 2015

            "period": ["20150101T180000Z/20150102T070000Z"],

            // Repeats the {period} every week until the last day of Jan. 2015.

            "recurrence": ["RRULE:FREQ=WEEKLY;UNTIL=20150131T070000Z"]

        ],

        "aceid": 1

    ]

    // An ACL provisioning and management service should be identified as the resource owner

    "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"

}
```

Figure A-1 – Example "/oic/sec/acl2" Resource

Example AMS

Figure A-2 demonstrates how the "/oic/sec/amacl" Resource should be configured to achieve this objective.

```json
{

    "resources": [

        // If the (Subject) wants to access the /oic/sh/light/1 Resource at host1 and an Amacl was supplied then use the sacl validation credential to enforce access.

        {"href": "/oic/sh/light/1"},

        // If the (Subject) wants to access the /oma/3 Resource at host2 and an AM sacl was supplied then use the sacl validation credential to enforce access.

        {"href": "/oma/3"},

    ]

}
```
// If the (Subject) wants to access any local Resource and an Amacl was supplied then use
// the sacl validation credential to enforce access.
{"wc": "***"]
}

Figure A-2 Example "/oic/sec/amacl" Resource
Annex B  
(Informative)  
Execution Environment Security Profiles  

Given that IoT verticals and Devices will not be of uniform capabilities, a one-size-fits all security robustness requirements meeting all IOT applications and services will not serve the needs of OCF, and security profiles of varying degree of robustness (trustworthiness), cost and complexity have to be defined. To address a large ecosystem of vendors, the profiles can only be defined as requirements and the exact solutions meeting those requirements are specific to the vendors’ open or proprietary implementations, and thus in most part outside scope of this document.

To align with the rest of OCF documents, where Device classifications follow IETF RFC 7228 (Terminology for constrained node networks) methodology, we limit the number of security profiles to a maximum of 3 (see Table B.1). However, our understanding is OCF capabilities criteria for each of 3 classes will be more fit to the current IoT chip market than that of IETF.

Given the extremely low level of resources at class 0, our expectation is that class 0 Devices are either capable of no security functionality or easily breakable security that depend on environmental (e.g. availability of human) factors to perform security functions. This means the class 0 will not be equipped with an SEE.

Table B.1 – OCF Security Profile

<table>
<thead>
<tr>
<th>Platform class</th>
<th>SEE</th>
<th>Robustness level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>High</td>
</tr>
</tbody>
</table>

NOTE This analysis acknowledges that these Platform classifications do not take into consideration of possibility of security co-processor or other hardware security capability that augments classification criteria (namely CPU speed, memory, storage).
Annex C
(normative)
Resource Type definitions

C.1 List of Resource Type definitions

Table C.1 contains the list of defined security resources in this document.

<table>
<thead>
<tr>
<th>Friendly Name (informative)</th>
<th>Resource Type (rt)</th>
<th>Clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control List</td>
<td>oic.r.acl</td>
<td>C.3</td>
</tr>
<tr>
<td>Access Control List 2</td>
<td>oic.r.acl2</td>
<td>C.4</td>
</tr>
<tr>
<td>Account</td>
<td>oic.r.account</td>
<td>C.2</td>
</tr>
<tr>
<td>Account Session</td>
<td>oic.r.session</td>
<td>C.13</td>
</tr>
<tr>
<td>Account Token Refresh</td>
<td>oic.r.tokenrefresh</td>
<td>C.15</td>
</tr>
<tr>
<td>Certificate Revocation</td>
<td>oic.r.crl</td>
<td>C.7</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>oic.r.crl</td>
<td>C.8</td>
</tr>
<tr>
<td>Credential</td>
<td>oic.r.cred</td>
<td>C.6</td>
</tr>
<tr>
<td>Device owner transfer method</td>
<td>oic.r.doxm</td>
<td>C.9</td>
</tr>
<tr>
<td>Device Provisioning Status</td>
<td>oic.r.pstat</td>
<td>C.10</td>
</tr>
<tr>
<td>Managed Access Control</td>
<td>oic.r.acl2</td>
<td>C.5</td>
</tr>
<tr>
<td>Roles</td>
<td>oic.r.pstat</td>
<td>C.11</td>
</tr>
<tr>
<td>Security Profile</td>
<td>oic.r.sp</td>
<td>C.14</td>
</tr>
<tr>
<td>Signed Access Control List</td>
<td>oic.r.sacl</td>
<td>C.12</td>
</tr>
</tbody>
</table>

C.2 Account Token

C.2.1 Introduction

Sign-up using generic account provider.

C.2.2 Well-known URI

/oic/sec/account

C.2.3 Resource type

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

C.2.4 OpenAPI 2.0 definition

```json
{
    "swagger": "2.0",
    "info": {
        "title": "Account Token",
        "version": "20190111",
        "license": {
            "name": "OCF Data Model License",
            "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/account": {
    "post": {
      "description": "Sign-up using generic account provider.
      "parameters": [
        {
          "$ref": "#/parameters/interface"},
        {
          "name": "body",
          "in": "body",
          "required": true,
          "schema": { "$ref": "#/definitions/Account-request" },
          "x-example":
          {
            "di": "9cfbeb8e-5a1e-4d1c-9d01-00c04fd430c8",
            "authprovider": "github",
            "accesstoken": "8802f2eaf85e147a936"
          }
        }
      ],
      "responses": {
        "204": {
          "description": "2.04 Changed respond with required and optional information\n",
          "x-example":
          {
            "rt": ["oic.r.account"],
            "accesstoken": "0f3d9f7fe5491d54077d",
            "refreshrequest": "00fe4644a6be5324ec",
            "expiresin": "3600",
            "uid": "123e4567-e89b-12d3-456d-6e313b71d9f",
            "redirecturi": "coaps+tcp://example.com:443",
            "schema": { "$ref": "#/definitions/Account-response" }
          }
        }
      }
    },
    "delete": {
      "description": "Delete a device. This also removes all resources in the device on cloud
      example: /oic/account?di=9cfbeb8e-5a1e-4d1c-9d01-00c04fd430c8&accesstoken=0f3d9f7fe5491d54077d
      "parameters": [
        {
          "$ref": "#/parameters/interface"}
      ],
      "responses": {
        "202": {
          "description": "2.02 Deleted response informing the device is successfully deleted.\n"
        }
      }
    }
  },
  "parameters": {
    "interface": {
      "in": "query",
      "name": "if",
      "type": "string",
      "enum": ["oic.if.baseline"]
    }
  },
  "definitions": {
    "Account-request": {
      "properties": {
        "authprovider": {
          "description": "The name of Authorization Provider through which Access Token was obtained",
          "type": "string"
        }
      }
    }
  }
}
"accesstoken": {
  "description": "Access-Token used for communication with OCF Cloud after account creation",
  "pattern": "(?![\$][\s*])+",
  "type": "string"
},
"di": {
  "description": "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}$",
  "type": "string"
}
},
"type": "object",
"required": ["di", "accesstoken"]
},
"Account-response": {
"properties": {
  "expiresin": {
    "description": "Access-Token remaining life time in seconds (-1 if permanent)",
    "readOnly": true,
    "type": "integer"
  },
  "rt": {
    "description": "Resource Type of the Resource",
    "items": {
      "maxLength": 64,
      "type": "string",
      "enum": ["oic.r.account"]
    },
    "minItems": 1,
    "maxItems": 1,
    "readOnly": true,
    "type": "array"
  },
  "refreshtoken": {
    "description": "Refresh token can be used to refresh the Access Token before getting expired",
    "pattern": "(?![\$][\s*])+",
    "readOnly": true,
    "type": "string"
  },
  "uid": {
    "description": "Format pattern according to IETF RFC 4122.",
    "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
    "type": "string"
  },
  "accesstoken": {
    "description": "Access-Token used for communication with cloud after account creation",
    "pattern": "(?![\$][\s*])+",
    "type": "string"
  },
  "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"
  },
  "redirecturi": {
    "description": "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.",
    "readOnly": true,
    "type": "string"
  },
  "i": {
    "description": "The interface set supported by this resource",
    "items": {
      "enum": ["$$
"
C.2.5 Property definition

Table C.2 defines the Properties that are part of the "oic.r.account" Resource Type.

**Table C.2 – The Property definitions of the Resource with type "rt" = "oic.r.account".**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>di</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>authprovider</td>
<td>string</td>
<td>No</td>
<td>Read Write</td>
<td>The name of Authorization Provider through which Access Token was obtained</td>
</tr>
<tr>
<td>accesstoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Access-Token used for communication with OCF Cloud after account creation</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>refreshtoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Only</td>
<td>Refresh token can be used to refresh the Access Token before getting expired</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource</td>
</tr>
<tr>
<td>accesstoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Access-Token used for communication with cloud after account creation</td>
</tr>
<tr>
<td>uid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>expiresin</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td>Access-Token remaining life time in seconds</td>
</tr>
</tbody>
</table>
C.2.6 CRUDN behaviour

Table C.3 defines the CRUDN operations that are supported on the "oic.r.account" Resource Type.

Table C.3 – The CRUDN operations of the Resource with type "rt" = "oic.r.account".

<table>
<thead>
<tr>
<th></th>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>post</td>
<td></td>
<td>delete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C.3 Access Control List

C.3.1 Introduction

This Resource specifies the local access control list. When used without query parameters, all the ACE entries are returned. When used with a subjectuuid, only the ACEs with the specified subjectuuid are returned. If subjectuuid and Resources are specified, only the ACEs with the specified subjectuuid and Resource hrefs are returned.

C.3.2 Well-known URI

/oic/sec/acl

C.3.3 Resource type

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

C.3.4 OpenAPI 2.0 definition

```json
{
"swagger": "2.0",
"info": {
  "title": "Access Control List",
  "version": "v1.1-20161213",
  "license": {
    "name": "OCF Data Model License",
    "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4cfbce8bdc4ba/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/acl": {
    "get": {
      "description": "This Resource specifies the local access control list. When used without query parameters, all the ACE entries are returned. When used with a subjectuuid, only the ACEs with the specified subjectuuid are returned. If subjectuuid and Resources are specified, only the ACEs with the specified subjectuuid and Resource hrefs are returned."
    },
    "parameters": [
      {"$ref": "#/parameters/interface"},
      {"$ref": "#/parameters/ace-filtered-uuid"},
      {"$ref": "#/parameters/ace-filtered-resources"}
    ],
    "responses": {
      "200": {
        "description": "",
        "x-example": {
          "rt": ["oic.r.acl"],
          "aclist": {
            "aces": [
              {
                "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
                "resources": [
                  {"href": "coaps://IP-ADDR/temp", "rel": "some-rel", "rt": ["oic.r.temperature"], "if": ["oic.if.a"]},
                  {"href": "coaps://IP-ADDR/temp", "rel": "some-rel", "rt": ["oic.r.temperature"], "if": ["oic.if.a"]}
                ],
                "permission": 31,
                "validity": [
                  {"period": "20160101T180000Z/20170102T070000Z", "recurrence": ["DSTART:XXXXX", "RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1"]}
                ]
              },
              {"subjectuuid": "de305d54-75b4-431b-adb2-eb6b9e546014",
                "owneruuid": "de305d54-75b4-431b-adb2-eb6b9e546014",
                "schema": { "$ref": "#/definitions/Acl" }
              },
              "400": {
                "description": "The request is invalid."}
            ]
          },
          "post": {
            "description": "Updates the ACL Resource with the provided values. ACEs provided in the update not currently in the ACL are added. ACEs that already exist in the ACL are ignored.
Note that for the purposes of update, equivalency is determined by comparing the ACE subjectuuid, permission, string comparisons of all validity elements, and string comparisons of all
Resource
hrefs.

"parameters": [
   {"$ref": "/#/parameters/interface"},
   {"name": "body", "in": "body", "required": true, "schema": { "$ref": "/#/definitions/Acl" }, "x-example": {
      "aclist": [
         "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9", "resources": [
            { "href": "coaps://IP-ADDR/temp", "rel": "some-rel", "rt": ["oic.r.temperature"], "if": ["oic.if.a"] },
            { "href": "coaps://IP-ADDR/temp", "rel": "some-rel", "rt": ["oic.r.temperature"], "if": ["oic.if.s"] },
         ]
      },
      "permission": 31,
      "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-eb6b9e5a546014" }
],
"responses": {
   "400": { "description" : "The request is invalid." },
   "201": { "description" : "The ACL entry/entries is/are created." },
   "204": { "description" : "The ACL entry/entries is/are updated." }
}
"delete": {
   "description": "Deletes ACL entries.
When DELETE is used without query parameters, all the
ACE entries are deleted. When DELETE is used with a subjectuuid, only the ACEs with the
specified subjectuuid are deleted. If subjectuuid and Resources are specified, only the ACEs with
the specified subjectuuid and Resource hrefs are deleted.
"parameters": [
   {"$ref": "/#/parameters/interface"},
   {"$ref": "/#/parameters/ace-filtered-uuid"},
   {"$ref": "/#/parameters/ace-filtered-resources"}
],
"responses": {
   "200": { }
"description": "The matching ACEs or the entire ACL Resource has been successfully deleted.",
"400": {
"description": "The request is invalid.
}
},
"parameters": {
"interface": {
"in": "query",
"name": "if",
"type": "string",
"enum": ["oic.if.baseline"]
}
},
"ace-filtered-uuid": {
"in": "query",
"name": "subjectuuid",
"required": false,
"type": "string",
"description": "Only applies to ACEs with the specified subject UUID.",
"x-example": "se61c3e6b-9c54-4b81-8ce5-f9039cd04d9"
}
},
"ace-filtered-resources": {
"in": "query",
"name": "resources",
"required": false,
"type": "string",
"description": "Only applies to ACEs with the specified subjectuuid | and Resources href.",
"x-example": "coaps://IP-ADDR/temp"
}
},
"definitions": {
"Acl": {
"properties": {
"roweruuid": {
"description": "The value identifies the unique Resource owner Format pattern according to IETF RFC 4122.",
"pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
"type": "string"
},
"rt": {
"description": "Resource Type of the Resource.",
"items": {
"maxLength": 64,
"type": "string",
"enum": ["oic.r.acl"]
},
"minItems": 1,
"readOnly": true,
"type": "array"
},
"aclist": {
"description": "Subject-based Access Control Entries in the ACL Resource.",
"properties": {
"aces": {
"properties": {
"permission": {
"description": "Bitmask encoding of CRUDN permission
The 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."],
}"type": "string",
"enum": ["allow", "deny", "n"],
"def": "true""]
}
}
"maximum": 31,
"minimum": 0,
"type": "integer"
},
"resources": [
  "description": "References the application's Resources to which a security policy applies."
],
"items": [
  "properties": [
    "anchor": {
      "description": "This is used to override the context URI e.g. override the URI of the containing collection.",
      "format": "uri",
      "maxLength": 256,
      "type": "string"
    },
    "di": {
      "description": "The Device ID
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"
    },
    "eps": {
      "description": "the Endpoint information of the target Resource.",
      "items": [
        "properties": [
          "ep": {
            "description": "Transport Protocol Suite + Endpoint Locator.",
            "format": "uri",
            "type": "string"
          },
          "pri": {
            "description": "The priority among multiple Endpoints.",
            "minimum": 1,
            "type": "integer"
          }
        ],
        "type": "object"
      ],
      "type": "array"
    },
    "href": {
      "description": "This is the target URI, it can be specified as a Relative Reference or fully-qualified URI.",
      "format": "uri",
      "maxLength": 256,
      "type": "string"
    },
    "if": {
      "description": "The interface set supported by this Resource.",
      "items": [
        "enum": [
          "oic.if.baseline",
          "oic.if.ll",
          "oic.if.b",
          "oic.if.rw",
          "oic.if.a",
          "oic.if.s"
        ],
        "type": "string"
      ],
      "minItems": 1,
      "type": "array"
    },
    "ins": {
      "description": "The instance identifier for this web link in an array of web links - used in collections.",
      "type": "integer"
    },
    "p": {
      "description": "The priority among multiple Endpoints.",
      "minimum": 1,
      "type": "integer"
    }
  ],
  "type": "object"
"description": "Specifies the framework policies on the Resource referenced by the target URI.",
"properties": {
  "bm": {
    "description": "Specifies the framework policies on the Resource referenced by the target URI for e.g. observable and discoverable.",
    "type": "integer"
  }
},
"required": [
  "bm"
],
"type": "object"
},
"rel": {
  "description": "The relation of the target URI referenced by the link to the context URI.",
  "oneOf": [
    {
      "default": ["hosts"],
      "items": {
        "maxLength": 64,
        "type": "string"
      },
      "minItems": 1,
      "type": "array"
    },
    {
      "default": "hosts",
      "maxLength": 64,
      "type": "string"
    }
  ]
},
"rt": {
  "description": "Resource Type of the Resource.",
  "items": {
    "maxLength": 64,
    "type": "string"
  },
  "minItems": 1,
  "type": "array"
},
"title": {
  "description": "A title for the link relation. Can be used by the UI to provide a context.",
  "maxLength": 64,
  "type": "string"
},
"type": {
  "default": "application/cbor",
  "description": "A hint at the representation of the Resource referenced by the target URI. This represents the media types that are used for both accepting and emitting.";
  "items": {
    "maxLength": 64,
    "type": "string"
  },
  "minItems": 1,
  "type": "array"
}
],
"required": [
  "href",
  "rt",
  "if"
],
"type": "array"
"subjectuuid": {  
  "anyOf": [
    {
      "description": "The id of the Device to which the ace applies to or \"*\" for anonymous access.",
      "pattern": "\"*\"",
      "type": "string"
    },
    {
      "description": "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"
    }
  ],

  "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"
    }
  }
}

"aces": {
  "description": "The interface set supported by this Resource.",
  "$ref": "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-schema.json#/definitions/n"
},

"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.",
  "$ref": "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-schema.json#/definitions/"
C.3.5 Property definition

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

Table C.4 – The Property definitions of the Resource with type "rt" = "oic.r.acl".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aclist</td>
<td>object: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>Subject-based Access Control Entries in the ACL Resource.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>The value identifies the unique Resource owner. Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
</tbody>
</table>

C.3.6 CRUDN behaviour

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

Table C.5 – The CRUDN operations of the Resource with type "rt" = "oic.r.acl".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td>delete</td>
<td></td>
<td>observe</td>
</tr>
</tbody>
</table>

C.4 Access Control List-2

C.4.1 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
C.4.2 Well-known URI
/oic/sec/acl2

C.4.3 Resource type
The Resource Type is defined as: "oic.r.acl2".

C.4.4 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/e28a9e0a92e17042ba3e83661e4c0fbc8bdc4ba/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. 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."
      },
      "responses": {
        "200": {
          "description": "",
          "x-example": {
            "rt": ["oic.r.acl2"],
            "aclist2": [
              {
                "aceid": 1,
                "subject": {
                  "authority": "484b8a51-ch23-46c0-a5f1-b4aebc50be",
                  "role": "SOME_STRING"
                },
                "resources": [
                  {
                    "href": "/light",
                    "rt": ["oic.r.light"],
                    "if": ["oic.if.baseline", "oic.if.a"]
                  },
                  {
                    "href": "/door",
                    "rt": ["oic.r.door"],
                    "if": ["oic.if.baseline", "oic.if.a"]
                  }
                ],
                "permission": 24
              }
            ]
          }
        }
      }
    }
  }
}
"resources": [
  {
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.baseline", "oic.if.a"]
  },
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.baseline", "oic.if.a"]
  }
],
"permission": 24,
"aceid": 3,
"subject": {"conntype": "anon-clear"},
"resources": [
  {
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.baseline", "oic.if.a"]
  },
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.baseline", "oic.if.a"]
  }
],
"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": { "$ref": "/definitions/Acl2" }
},
"post": {
  "description": "Updates the ACL Resource with the provided ACEs.\n  A new ACL Resource is created if one does not currently exist.\n  New ACEs provided in the update with aceid(s) already in the ACL completely replace the ACE(s) in the ACL Resource.\n  New ACEs provided in the update without aceid properties are added and assigned unique aceids in the ACL Resource.\n  ",
  "parameters": [{$ref": "/parameters/interface"},
                 {"$ref": "/parameters/ace-filtered"},
                 {"name": "body",
                  "in": "body",
                  "required": true,
                  "schema": { "$ref": "/definitions/Acl2-Update" },
                  "x-example": {
                    "aclist2": [
                      {"aceid": 1,
                       "href": "/light",
                       "rt": ["oic.r.light"],
                       "if": ["oic.if.baseline", "oic.if.a"]
                      },
                      {"href": "/door",
                       "rt": ["oic.r.door"],
                       "if": ["oic.if.baseline", "oic.if.a"]
                      }
                    ],
                    "permission": 24,
                    "aceid": 3,
                    "subject": {"conntype": "anon-clear"},
                    "resources": [
                      {"href": "/light",
                       "rt": ["oic.r.light"],
                       "if": ["oic.if.baseline", "oic.if.a"]
                      },
                      {"href": "/door",
                       "rt": ["oic.r.door"],
                       "if": ["oic.if.baseline", "oic.if.a"]
                      }
                    ],
                    "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": { "$ref": "/definitions/Acl2" }
                }
  ]
}
"subject": {
  "authority": "484b8a51-cb23-46c0-a5f1-b4aebe50ebe",
  "role": "SOME_STRING"
},
"resources": [
  {
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.baseline", "oic.if.a"]
  },
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.baseline", "oic.if.a"]
  }
],
"permission": 24,
"aceid": 3,
"subject": {
  "uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
},
"resources": [
  {
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.baseline", "oic.if.a"]
  },
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.baseline", "oic.if.a"]
  }
],
"permission": 24,
"rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
],
"responses": {
  "400": {
    "description": "The request is invalid."
  },
  "201": {
    "description": "The ACL entry is created."
  },
  "204": {
    "description": "The ACL entry is updated."
  }
}
}]
},
"delete": {
  "description": "Deletes ACL entries.\nWhen DELETE is used without query parameters, all the
ACE entries are deleted.\nWhen DELETE is used with a query parameter, only the ACEs matching
the\nspecified parameter are deleted.\n",
"parameters": [
  {"$ref": "/parameters/interface"},
  {"$ref": "/parameters/ace-filtered"}
],
"responses": {
  "200": {
    "description": "The matching ACEs or the entire ACL Resource has been successfully
deleted."
  },
  "400": {
    "description": "The request is invalid."
  }
}
}
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  },
  "ace-filtered": {
    "in": "query",
    "name": "aceid",
    "required": false,
    "type": "integer",
    "description": "Only applies to the ACE with the specified aceid.",
    "x-example": 2112
  }
},
"definitions": {
  "Acl2": {
    "properties": {
      "owneruuid": {
        "description": "The value identifies the unique Resource owner\nFormat pattern according to IETF RFC 4122.",
        "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
        "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. This is the target URI, it can be specified as a Relative Reference or fully-qualified URI.",
  "format": "uri",
  "maxLength": 256,
  "type": "string"
},
"if": {
  "description": "When present, the ACE only applies when the if (interface) matches. The interface set supported by this Resource.",
  "items": {
    "enum": [
      "oic.if.baseline",
      "oic.if.ll",
      "oic.if.b",
      "oic.if.rw",
      "oic.if.r",
      "oic.if.a",
      "oic.if.s"
    ],
    "type": "string"
  },
  "minItems": 1,
  "type": "array"
},
"rt": {
  "description": "When present, the ACE only applies when the rt (Resource type) matches. Resource Type of the Resource.",
  "items": {
    "maxLength": 64,
    "type": "string"
  },
  "minItems": 1,
  "type": "array"
},
"wc": {
  "description": "A wildcard matching policy.",
  "pattern": "^[\-\+\*]$",
  "type": "string"
},
"type": "object"
},
"type": "array"
},
"subject": {
  "anyOf": [
    {
      "description": "This is the Device identifier.",
      "properties": {
        "uuid": {
          "description": "A UUID Device ID. Format pattern according to IETF RFC 4122.",
          "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
          "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"
        }
      },
      "required": [
        "authority"
      ],
      "type": "object"
    }
  ]
}

"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"
    },
    "required": [
      "aceid",
      "resources",
      "permission",
      "subject"
    ],
    "type": "object"
"type": "array",
"n": {
  "$ref": 
  "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-schemas.json#/definitions/n"
},
"id": {
  "$ref": 
  "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-schemas.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
      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\n            The 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\n            \nThis
is the target URI, it can be specified as a Relative Reference or fully-qualified URI.

```
"format": "uri",
"maxLength": 256,
"type": "string"
}`, 
"if": { 
"description": "When present, the ACE only applies when the if (interface) matches
The interface set supported by this Resource.",
"items": { 
"enum": [ 
"oic.if.baseline",
"oic.if.ll",
"oic.if.b",
"oic.if.rw",
"oic.if.r",
"oic.if.s",
"oic.if.s"
],
"type": "string"
},
"minItems": 1,
"type": "array"
},
"rt": { 
"description": "When present, the ACE only applies when the rt (Resource type) matches
Resource Type of the Resource.",
"items": { 
"maxLength": 64,
"type": "string"
},
"minItems": 1,
"type": "array"
},
"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"
},
"subject": { 
"anyOf": [ 
"description": "This is the Device identifier.",
"properties": { 
"uuid": { 
"description": "A UUID Device ID
 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 "
  },
  "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"
  }
},
"required": [
  "period"
],
"type": "array"}
C.4.5 Property definition

Table C.6 defines the Properties that are part of the "oic.r.acl2" Resource Type.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aclist2</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Write</td>
<td>Access Control Entries in the ACL Resource.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>No</td>
<td>Read Write</td>
<td>The value identifies the unique Resource owner. Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>aclist2</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>Access Control Entries in the ACL Resource.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>The value identifies the unique Resource owner. Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
</tbody>
</table>

C.4.6 CRUDN behaviour

Table C.7 defines the CRUDN operations that are supported on the "oic.r.acl2" Resource Type.

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td>delete</td>
<td>observe</td>
<td></td>
</tr>
</tbody>
</table>
C.5 Managed Access Control

C.5.1 Introduction

This Resource specifies the host Resources with access permission that is managed by an AMS.

C.5.2 Well-known URI

/oic/sec/amacl

C.5.3 Resource type

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

C.5.4 OpenAPI 2.0 definition

```
{
  "swagger": "2.0",
  "info": {
    "title": "Managed Access Control",
    "version": "20190111",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/amacl": {
      "get": {
        "description": "This Resource specifies the host Resources with access permission that is managed by an AMS.",
        "parameters": [
          {$ref: "/parameters/interface"}
        ],
        "responses": {
          "200": {
            "description": "",
            "x-example": {
              "rt": ["oic.r.amacl"],
              "resources": [
                {
                  "href": "/temp",
                  "rt": ["oic.r.temperature"],
                  "if": ["oic.if.baseline", "oic.if.a"]
                },
                {
                  "href": "/temp",
                  "rt": ["oic.r.temperature"],
                  "if": ["oic.if.baseline", "oic.if.s"]
                }
              ]
            }
          },
          ""nt": ["oic.r.amacl"],
          "resources": [
            {
              "$ref": "/parameters/interface",
              "name": "body",
              "in": "body",
              "description": "Sets the new amacl data."
            }
          ]
        }
```
"required": true,
"schema": { "$ref": "#/definitions/Amacl" },
"x-example":
{
  "resources": [
  {
    "href": "/temp",
    "rt": ["oic.r.temperature"],
    "if": ["oic.if.baseline", "oic.if.a"]
  },
  {
    "href": "/temp",
    "rt": ["oic.r.temperature"],
    "if": ["oic.if.baseline", "oic.if.s"]
  }
  ],
  "responses": {
    "400": {
      "description": "The request is invalid."
    },
    "201": {
      "description": "The AMACL entry is created."
    },
    "204": {
      "description": "The AMACL entry is updated."
    }
  }
},
"put": {
  "description": "Creates the new acl data."
  "parameters": [{
    "$ref": "#/parameters/interface"},
    {
      "name": "body",
      "in": "body",
      "required": true,
      "schema": { "$ref": "#/definitions/Amacl" },
      "x-example":
      {
        "resources": [
        {
          "href": "/temp",
          "rt": ["oic.r.temperature"],
          "if": ["oic.if.baseline", "oic.if.a"]
        },
        {
          "href": "/temp",
          "rt": ["oic.r.temperature"],
          "if": ["oic.if.baseline", "oic.if.s"]
        }
        ],
        "responses": {
          "400": {
            "description": "The request is invalid."
          },
          "201": {
            "description": "The AMACL entry is created."
          }
        }
      }
    }
  }
},
"delete": {
  "description": "Deletes the acl data."
  "parameters": [ ]
}
"parameters": [
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  },
  "subject": {
    "in": "query",
    "description": "Delete the ACE identified by the string matching the subject value.\n",
    "type": "string",
    "name": "subject"
  }
],
"responses": {
  "200": {
    "description": "The ACE instance or the the entire AMAACL Resource has been successfully deleted."
  },
  "400": {
    "description": "The request is invalid."  
  }
}
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "Amacl": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource.\n",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.amacl"]
        },
        "minItems": 1,
        "maxItems": 1,
        "readOnly": true,
        "type": "array"  
      },
      "n": {
        "$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"  
      },
      "resources": {
        "description": "Multiple links to this host's Resources.\n",
        "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 URL, it can be specified as a Relative Reference or fully-qualified URL."",
              "format": "uri",
              "maxLength": 256,
              "type": "string"  
            },
            "if": {
              "description": "When present, the ACE only applies when the if (interface) matches\nThe interface set supported by this Resource."",
              "20": {  
                "items": ["oic.if.baseline",...
C.5.5 Property definition

Table C.8 defines the Properties that are part of the "oic.r.amacl" Resource Type.

Table C.8 – The Property definitions of the Resource with type "rt" = "oic.r.amacl".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resources</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>Multiple links to this host's Resources.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
</tbody>
</table>
C.5.6 CRUDN behaviour

Table C.9 defines the CRUDN operations that are supported on the "oic.r.amacl" Resource Type.

Table C.9 – The CRUDN operations of the Resource with type "rt" = "oic.r.amacl".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>put</td>
<td>get</td>
<td>post</td>
<td>delete</td>
<td>observe</td>
</tr>
</tbody>
</table>

C.6 Credential

C.6.1 Introduction

This Resource specifies credentials a Device may use to establish secure communication.

Retrieves the credential data.

When used without query parameters, all the credential entries are returned.

When used with a query parameter, only the credentials matching the specified parameter are returned.

Note that write-only credential data will not be returned.

C.6.2 Well-known URI

/oic/sec/cred

C.6.3 Resource type

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

C.6.4 OpenAPI 2.0 definition

```json
{
   "swagger": "2.0",
   "info": {
      "title": "Credential",
      "version": "v1.0-20181031",
      "license": {
         "name": "OCF Data Model License",
         "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/cred": {
         "get": {
            "description": "This Resource specifies credentials a Device may use to establish secure communication.
Retrieves the credential data.
When used without query parameters, all the credential entries are returned.
When used with a query parameter, only the credentials matching the specified parameter are returned.
Note that write-only credential data will not be returned.
",
            "parameters": [
               {"$ref": "#/parameters/interface"},
               {"$ref": "#/parameters/cred-filtered-credid"},
               {"$ref": "#/parameters/cred-filtered-subjectuuid"}
            ]
         }
      }
   }
}
```
"responses": {
  "200": {
    "description": "",
    "x-example": {
      "rt": ["oic.r.cred"],
      "creds": [
        {
          "credid": 55,
          "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
          "roleid": {
            "authority": "484b8a51-cb23-46c0-a5f1-b4aebe50ebe",
            "role": "SOME_STRING"
          },
          "credtype": 32,
          "publicdata": {
            "encoding": "oic.sec.encoding.base64",
            "data": "BASE-64-ENCODED-VALUE"
          },
          "privateData": {"encoding": "oic.sec.encoding.base64",
          "data": "BASE-64-ENCODED-VALUE"}
          "period": "20160101T180000Z/20170102T070000Z",
          "crms": [ "oic.sec.crm.pk10" ]
        },
        {
          "credid": 56,
          "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
          "roleid": {
            "authority": "484b8a51-cb23-46c0-a5f1-b4aebe50ebe",
            "role": "SOME_STRING"
          },
          "credtype": 1,
          "publicdata": {
            "encoding": "oic.sec.encoding.base64",
            "data": "BASE-64-ENCODED-VALUE"
          },
          "privateData": {"encoding": "oic.sec.encoding.base64",
          "data": "BASE-64-ENCODED-VALUE"}
          "period": "20160101T180000Z/20170102T070000Z",
          "crms": [ "oic.sec.crm.pk10" ]
        }
      ],
      "rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
    }
  },
  "400": {
    "description": "The request is invalid."
  }
},
"post": {
  "description": "Updates the credential Resource with the provided credentials. \n  Credentials provided in the update with credid(s) not currently in the credential..."
Credentials provided in the update with credid(s) already in the credential Resource are added.

Credentials provided in the update without credid(s) properties are added and assigned unique credid(s) in the credential Resource.

```
parameters:
  - $ref: "/parameters/interface"
  - name: "body"
  - in: "body"
  - required: true,
  - schema: { $ref: "/definitions/Cred-Update" },
  - x-example:
    - "creds": [
      { "credid": 55,
        "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
        "roleid": { "authority": "484b8a51-cb23-46c0-a5f1-b4aebe50ebe",
                    "role": "SOME_STRING" },
        "credtype": 32,
        "publicdata": { "encoding": "oic.sec.encoding.base64",
                         "data": "BASE-64-ENCODED-VALUE" },
        "privatedata": { "encoding": "oic.sec.encoding.base64",
                         "data": "BASE-64-ENCODED-VALUE",
                         "handle": 4 },
        "optionaldata": { "revstat": false,
                          "encoding": "oic.sec.encoding.base64",
                          "data": "BASE-64-ENCODED-VALUE" },
        "period": "20160101T180000Z/20170102T070000Z",
        "crms": [ "oic.sec.crm.pk10" ] },
      { "credid": 56,
        "subjectuuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
        "roleid": { "authority": "484b8a51-cb23-46c0-a5f1-b4aebe50ebe",
                    "role": "SOME_STRING" },
        "credtype": 1,
        "publicdata": { "encoding": "oic.sec.encoding.base64",
                         "data": "BASE-64-ENCODED-VALUE" },
        "privatedata": { "encoding": "oic.sec.encoding.base64",
                         "data": "BASE-64-ENCODED-VALUE",
                         "handle": 4 },
        "optionaldata": { "revstat": false,
                          "encoding": "oic.sec.encoding.base64",
                          "data": "BASE-64-ENCODED-VALUE" },
        "period": "20160101T180000Z/20170102T070000Z",
        "crms": [ "oic.sec.crm.pk10" ] },
      { "rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9" }
    ],
  responses:
    - 400: 
```

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved

191
"description" : "The request is invalid."
},
"201": {
  "description" : "The credential entry is created."
},
"204": {
  "description" : "The credential entry is updated."
}
"
delete": {
  "description": "Deletes credential entries. When DELETE is used without query parameters,
the cred entries are deleted. When DELETE is used with a query parameter, only the entries
matching the query parameter are deleted."
  "parameters": {
    "$ref": "/parameters/interface",
    "$ref": "/parameters/cred-filtered-credid",
    "$ref": "/parameters/cred-filtered-subjectuuid"
  },
  "responses": {
    "400": {
      "description" : "The request is invalid."
    },
    "204": {
      "description" : "The specific credential(s) or the the entire credential Resource has
been successfully deleted."
    }
  }
  "interface" : {
    "in" : "query",
    "name" : "if",
    "type" : "string",
    "enum" : ["oic.if.baseline"]
  },
  "cred-filtered-credid" : {
    "in" : "query",
    "name" : "credid",
    "required" : false,
    "type" : "integer",
    "description" : "Only applies to the credential with the specified credid."
  },
  "cred-filtered-subjectuuid" : {
    "in" : "query",
    "name" : "subjectuuid",
    "required" : false,
    "type" : "string",
    "description" : "Only applies to credentials with the specified subject UUID."
  }
  "definitions": {
    "Cred" : {
      "properties": {
        "rowneruuid" : {
          "description": "Format pattern according to IETF RFC 4122."
        },
        "rt" : {
          "description": "Resource Type of the Resource.",
          "items": {
            "maxLength": 64,
            "type": "string",
            "enum": ["oic.r.cred"]
          }
        }
      }
    }
  }
}
"readOnly": true,
"type": "array",
"uniqueItems": true
"n": {
  "$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"
},
"creds": {
  "description": "List of credentials available at this Resource.",
  "items": {
    "properties": {
      "credid": {
        "description": "Local reference to a credential Resource.",
        "type": "integer"
      },
      "credtype": {
        "description": "Representation of this credential's type
Credential Types - Cred type encoded as a bitmask.0 - Empty credential used for testing1 - Symmetric pair-wise key2 - Symmetric group key4 - Asymmetric signing key8 - Asymmetric signing key with certificate16 - PIN or password32 - Asymmetric encryption key.",
        "maximum": 63,
        "minimum": 0,
        "type": "integer"
      },
      "credusage": {
        "description": "A string that provides hints about how/where the cred is used
The type of credusage.oic.sec.cred.trustca - Trust certificateoic.sec.cred.cert - Certificateoic.sec.cred.rolecert - Role Certificateoic.sec.cred.mfgtrustca - Manufacturer Certificateoic.sec.cred.mfgcert - Manufacturer Certificate.",
        "enum": [
          "oic.sec.cred.trustca",
          "oic.sec.cred.cert",
          "oic.sec.cred.rolecert",
          "oic.sec.cred.mfgtrustca",
          "oic.sec.cred.mfgcert"
        ],
        "type": "string"
      },
      "crms": {
        "description": "The refresh methods that may be used to update this credential.",
        "items": {
          "description": "Each enum represents a method by which the credentials are refreshed.oic.sec.crm.pro - Credentials refreshed by a provisioning serviceoic.sec.crm.rdp - Credentials refreshed by a key agreement protocol and random PINoic.sec.crm.psk - Credentials refreshed by a key agreement protocoloic.sec.crm.skdc - Credentials refreshed by a key distribution serviceoic.sec.crm.pk10 - Credentials refreshed by a PKCS#10 request to a CA.",
          "enum": [
            "oic.sec.crm.pro",
            "oic.sec.crm.psk",
            "oic.sec.crm.rdp",
            "oic.sec.crm.skdc",
            "oic.sec.crm.pk10"
          ],
          "type": "string"
        }
      }
    }
  }
},
"optionaldata": {
  "description": "Credential revocation status information\nOptional credential contents describes revocation status for this credential.",
  "properties": {
    "data": {
      "description": "The encoded structure."
    }
  }
}
"type": "string",
"encoding": {
  "description": "A string specifying the encoding format of the data contained in
  the optdata.",
  "x-detail-desc": [
    "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
    "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
    "oic.sec.encoding.base64 - Base64 encoded object.",
    "oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain.",
    "oic.sec.encoding.der - Encoding for DER encoded certificate.",
    "oic.sec.encoding.raw - Raw hex encoded data."
  ],
  "enum": [
    "oic.sec.encoding.jwt",
    "oic.sec.encoding.cwt",
    "oic.sec.encoding.base64",
    "oic.sec.encoding.pem",
    "oic.sec.encoding.der",
    "oic.sec.encoding.raw"
  ],
  "type": "string"
},
"revstat": {
  "description": "Revocation status flag - true = revoked.",
  "type": "boolean"
},
"period": {
  "description": "String with RFC5545 Period.",
  "type": "string"
},
"privateData": {
  "description": "Private credential information
  Credential Resource non-public
  contents.",
  "properties": {
    "data": {
      "description": "The encoded value.",
      "maxLength": 3072,
      "type": "string"
    },
    "encoding": {
      "description": "A string specifying the encoding format of the data contained in
      the privdata\oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding\oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding\oic.sec.encoding.base64 - Base64 encoded object\oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain\oic.sec.encoding.der - Encoding for DER encoded certificate\oic.sec.encoding.raw - Raw hex encoded data.",
      "enum": [
        "oic.sec.encoding.jwt",
        "oic.sec.encoding.cwt",
        "oic.sec.encoding.base64",
        "oic.sec.encoding.pem",
        "oic.sec.encoding.der",
        "oic.sec.encoding.raw"
      ],
      "type": "string"
    },
    "handle": {
      "description": "Handle to a key storage Resource.",
      "type": "integer"
    }
  },
  "required": [
    "data",
    "encoding"
  ],
  "type": "object"
"publicdata": {
  "description": "Public credential information."
},
"properties": {
  "data": {
    "description": "The encoded value."
  },
  "encoding": {
    "description": "A string specifying the encoding format of the data contained in
    the pubdata\oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding\oic.sec.encoding.cwt -
    RFC CBOR web token (CWT) encoding\oic.sec.encoding.base64 - Base64 encoded
    object\oic.sec.encoding.uri - URI reference\oic.sec.encoding.pem - Encoding for PEM encoded
    certificate or chain\oic.sec.encoding.der - Encoding for DER encoded
    certificate\oic.sec.encoding.raw - Raw hex encoded data."
  },
  "enum": [
    "oic.sec.encoding.jwt",
    "oic.sec.encoding.cwt",
    "oic.sec.encoding.base64",
    "oic.sec.encoding.uri",
    "oic.sec.encoding.pem",
    "oic.sec.encoding.der",
    "oic.sec.encoding.raw"
  ],
  "type": "string"
},
"roleid": {
  "description": "The role this credential possesses\nSecurity 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."
  },
  "role": {
    "description": "The ID of the role being identified."
  }
},
"required": [
  "role"
],
"type": "object"
},
"subjectuuid": {
  "anyOf": [
    {
      "description": "The id of the Device, which the cred entry applies to or \"\"*
      "pattern": "\"\$",
      "type": "string"
    },
    {
      "description": "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"
    }]
}
"description": "The interface set supported by this Resource.",
"items": [
  "enum": [
    "oic.if.baseline"
  ],
  "type": "string"
],
"minItems": 1,
"readOnly": true,
"type": "array"
},
"type": "object",
"required": ["creds", "owneruuid"]
},
"Cred-Update": {
  "properties": {
    "owneruuid": {
      "description": "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"
    },
    "creds": {
      "description": "List of credentials available at this Resource.",
      "items": {
        "properties": {
          "cr_id": {
            "description": "Local reference to a credential Resource.",
            "type": "integer"
          },
          "credtype": {
            "description": "Representation of this credential\'s type\nCredential Types - Cred type encoded as a bitmask.
 0 - Empty credential used for testing
 1 - Symmetric pair-wise key
 2 - Symmetric group key
 4 - Asymmetric signing key
 8 - Asymmetric signing key with certificate
16 - PIN or password
32 - Asymmetric encryption key.",
            "maximum": 63,
            "minimum": 0,
            "type": "integer"
          },
          "credusage": {
            "description": "A string that provides hints about how/where the cred is used\nThe type of credusage.oic.sec.cred.trustca - Trust certificate\n  oic.sec.cred.rolecert - Role Certificate\n  oic.sec.cred.mfgtrustca - Manufacturer Certificate Trust\n  oic.sec.cred.mfgcert - Manufacturer Certificate.",
            "enum": [
              "oic.sec.cred.trustca",
              "oic.sec.cred.cert",
              "oic.sec.cred.rolecert",
              "oic.sec.cred.mfgtrustca",
              "oic.sec.cred.mfgcert"
            ],
            "type": "string"
          },
          "crms": {
            "description": "The refresh methods that may be used to update this credential.",
            "items": {
              "description": "Each enum represents a method by which the credentials are refreshed.
  oic.sec.crm.pro - Credentials refreshed by a provisioning service\n  oic.sec.crm.rdp - Credentials refreshed by a key agreement protocol and random PIN\n  oic.sec.crm.psk - Credentials refreshed by a key agreement protocol\n  oic.sec.crm.skdc - Credentials refreshed by a key distribution service\n  oic.sec.crm.pk10 - Credentials refreshed by a PKCS#10 request to a CA.",
            "enum": [
              "oic.sec.crm.pro",
              "oic.sec.crm.psk",
              "oic.sec.crm.rdp",
              "oic.sec.crm.skdc",
              "oic.sec.crm.pk10"
            ],
            "type": "string"
          }
        }
      }
    }
  }
}
"optionaldata": {
    "description": "Credential revocation status information
Optional credential contents describes revocation status for this credential.",
    "properties": {
        "data": {
            "description": "The encoded structure.",
            "type": "string"
        },
        "encoding": {
            "description": "A string specifying the encoding format of the data contained in the optdata.",
            "x-detail-desc": [
                "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
                "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
                "oic.sec.encoding.base64 - Base64 encoded object.",
                "oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain.",
                "oic.sec.encoding.der - Encoding for DER encoded certificate.",
                "oic.sec.encoding.raw - Raw hex encoded data."
            ],
            "enum": [
                "oic.sec.encoding.jwt",
                "oic.sec.encoding.cwt",
                "oic.sec.encoding.base64",
                "oic.sec.encoding.pem",
                "oic.sec.encoding.der",
                "oic.sec.encoding.raw"
            ],
            "type": "string"
        },
        "revstat": {
            "description": "Revocation status flag - true = revoked.",
            "type": "boolean"
        }
    },
    "required": [
        "revstat"
    ],
    "type": "object"
},

"privatedata": {
    "description": "Private credential information
Credential Resource non-public contents.",
    "properties": {
        "data": {
            "description": "The encoded value.",
            "maxLength": 3072,
            "type": "string"
        },
        "encoding": {
            "description": "A string specifying the encoding format of the data contained in the privdata.",
            "x-detail-desc": [
                "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
                "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
                "oic.sec.encoding.base64 - Base64 encoded object.",
                "oic.sec.encoding.uri - URI reference.",
                "oic.sec.encoding.handle - Data is contained in a storage sub-system referenced using a handle.",
                "oic.sec.encoding.raw - Raw hex encoded data."
            ],
            "enum": [
                "oic.sec.encoding.jwt",
                "oic.sec.encoding.cwt",
                "oic.sec.encoding.base64",
                "oic.sec.encoding.uri",
                "oic.sec.encoding.handle"
            ],
            "type": "string"
        }
    }
}
"oic.sec.encoding.raw",
  "type": "string"
},
  "handle": {
    "description": "Handle to a key storage Resource.",
    "type": "integer"
  }
},
  "required": [
  "encoding"
],
  "type": "object"
},
  "publicdata": {
    "properties": {
    "data": {
      "description": "The encoded value.",
      "maxLength": 3072,
      "type": "string"
    },
    "encoding": {
      "description": "Public credential information
A string specifying the encoding
format of the data contained in the pubdata.",
      "x-detail-desc": [
        "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
        "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
        "oic.sec.encoding.base64 - Base64 encoded object.",
        "oic.sec.encoding.uri - URI reference.",
        "oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain.",
        "oic.sec.encoding.der - Encoding for DER encoded certificate.",
        "oic.sec.encoding.raw - Raw hex encoded data."
      ],
      "enum": [
        "oic.sec.encoding.jwt",
        "oic.sec.encoding.cwt",
        "oic.sec.encoding.base64",
        "oic.sec.encoding.uri",
        "oic.sec.encoding.pem",
        "oic.sec.encoding.der",
        "oic.sec.encoding.raw"
      ],
      "type": "string"
    }
  },
  "type": "object"
],
  "roleid": {
    "description": "The role this credential possesses
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"
  },
  "subjectuuid": {
    "anyOf": [
      {"description": "The id of the Device, which the cred entry applies to or "/**/"
for wildcard identity."}]}
C.6.5 Property definition

Table C.10 defines the Properties that are part of the "oic.r.cred" Resource Type.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>No</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>creds</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Write</td>
<td>List of credentials available at this Resource.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
</tbody>
</table>
C.6.6 CRUDN behaviour

Table C.11 defines the CRUDN operations that are supported on the "oic.r.cred" Resource Type.

Table C.11 – The CRUDN operations of the Resource with type "rt" = "oic.r.cred".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td>delete</td>
<td></td>
<td>observe</td>
</tr>
</tbody>
</table>

C.7 Certificate Revocation

C.7.1 Introduction

This Resource specifies certificate revocation lists as X.509 objects.

C.7.2 Well-known URI

/​oic​/sec/crl

C.7.3 Resource type

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

C.7.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Certificate Revocation",
    "version": "v1.0-20150819",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/crl" : {
      "get": {
        "description": "This Resource specifies certificate revocation lists as X.509 objects.\n",
        "parameters": {
          "$ref": "#/parameters/interface"
        },
        "responses": {
          "200": {
            "description": "",
            "x-example": {
              "rt": ["oic.r.crl"],
              "crlid": 1,
              "thisupdate": "2016-04-12T23:20:50.52Z",
              "crldata": "Base64ENCODEDCRL"
            },
            "schema": { "$ref": "#/definitions/Crl" }
          }
        }
      }
    }
  }
}
```
"description": "Updates the CRL data.\n",
"parameters": [
{"$ref": "/#/parameters/interface"},

  "name": "body",
  "in": "body",
  "required": true,
  "schema": { "$ref": "/#/definitions/Crl-Update" },
  "x-example": {
    "crlid": 1,
    "thisupdate": "2016-04-12T23:20:50.52Z",
    "crldata": "Base64ENCODEDCRL"
  }
],
"responses": {
  "400": {
    "description": "The request is invalid."
  },
  "204": {
    "description": "The CRL entry is updated."
  }
}
"parameters": {
  "interface": {
    "in": "query",
    "name": "$if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "Crl": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource.",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.crl"]
        },
        "minItems": 1,
        "readOnly": true,
        "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"
      },
      "crldata": {
        "description": "Base64 BER encoded CRL data.",
        "type": "string"
      },
      "crlid": {
        "description": "Local reference to a CRL Resource.",
        "type": "integer"
      },
      "thisupdate": {
        "description": "UTC time of last CRL update.",
        "type": "string"
      }
    }
  }
}
"if": {
  "description": "The interface set supported by this Resource.",
  "items": {
    "enum": [
      "oic.if.baseline"
    ],
    "type": "string"
  },
  "minItems": 1,
  "readOnly": true,
  "type": "array"
}
"type": "object",
"required": ["crlid", "thisupdate", "crldata"]
},
"Crl-Update": {
  "properties": {
    "crldata": {
      "description": "Base64 BER encoded CRL data.",
      "type": "string"
    },
    "crlid": {
      "description": "Local reference to a CRL Resource.",
      "type": "integer"
    },
    "thisupdate": {
      "description": "UTC time of last CRL update.",
      "type": "string"
    }
  },
  "type": "object"
}
}

C. 7.5 Property definition
Table C.12 defines the Properties that are part of the "oic.r.crl" Resource Type.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crldata</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Base64 BER encoded CRL data.</td>
</tr>
<tr>
<td>thisupdate</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>UTC time of last CRL update.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>crlid</td>
<td>integer</td>
<td>Yes</td>
<td>Read Write</td>
<td>Local reference to a CRL Resource.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>crldata</td>
<td>string</td>
<td>Read Write</td>
<td>Base64 BER encoded CRL data.</td>
<td></td>
</tr>
</tbody>
</table>
C.7.6 CRUDN behaviour

Table C.13 defines the CRUDN operations that are supported on the "oic.r.crl" Resource Type.

Table C.13 – The CRUDN operations of the Resource with type "rt" = "oic.r.crl".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td>observe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C.8 Certificate Signing Request

C.8.1 Introduction

This Resource specifies a Certificate Signing Request.

C.8.2 Well-known URI

/oic/sec/csr

C.8.3 Resource type

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

C.8.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Certificate Signing Request",
    "version": "v1.0-20150819",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e40fbce8bdc4ba/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/csr": {
      "get": {
        "description": "This Resource specifies a Certificate Signing Request.
        "parameters": {
          "$ref": "#/parameters/interface"
        },
        "responses": {
          "200": {
            "description": "",
            "x-example": {
              "rt": ["oic.r.csr"],
              "encoding": "oic.sec.encoding.pem",
              "csr": "PENCODEDCSR"
            }
          },
          "404": {
            "description": "The Device does not support certificates and generating CSRs."
          }
        }
      }
    }
  }
}
```
"503": {
  "description": "The Device is not yet ready to return a response. Try again later."
}
],
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "Csr": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource.",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.csr"]
        },
        "minItems": 1,
        "readOnly": true,
        "type": "array"
      },
      "encoding": {
        "description": "A string specifying the encoding format of the data contained in CSR.",
        "x-detail-desc": {
          "oic.sec.encoding.pem - Encoding for PEM encoded CSR.",
          "oic.sec.encoding.der - Encoding for DER encoded CSR."
        },
        "enum": [
          "oic.sec.encoding.pem",
          "oic.sec.encoding.der"
        ],
        "readOnly": true,
        "type": "string"
      },
      "n": {
        "$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"
      },
      "csr": {
        "description": "Signed CSR in ASN.1 in the encoding specified by the encoding property.",
        "maxLength": 3072,
        "readOnly": true,
        "type": "string"
      },
      "if": {
        "description": "The interface set supported by this Resource.",
        "items": {
          "enum": ["oic.if.baseline"
        },
        "type": "string"
      },
      "minItems": 1,
      "readOnly": true,
      "type": "array"
    }
  }
}
C.8.5 Property definition

Table C.14 defines the Properties that are part of the "oic.r.csr" Resource Type.

Table C.14 – The Property definitions of the Resource with type "rt" = "oic.r.csr".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>encoding</td>
<td>string</td>
<td>Yes</td>
<td>Read Only</td>
<td>A string specifying the encoding format of the data contained in CSR.</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>csr</td>
<td>string</td>
<td>Yes</td>
<td>Read Only</td>
<td>Signed CSR in ASN.1 in the encoding specified by the encoding property.</td>
</tr>
</tbody>
</table>

C.8.6 CRUDN behaviour

Table C.15 defines the CRUDN operations that are supported on the "oic.r.csr" Resource Type.

Table C.15 – The CRUDN operations of the Resource with type "rt" = "oic.r.csr".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td></td>
<td></td>
<td></td>
<td>observe</td>
</tr>
</tbody>
</table>

C.9 Device Owner Transfer Method

C.9.1 Introduction

This Resource specifies properties needed to establish a Device owner.

C.9.2 Well-known URI

/oic/sec/doxm

C.9.3 Resource type

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

C.9.4 OpenAPI 2.0 definition

```
{"swagger": "2.0",
 "info": {
```
"title": "Device Owner Transfer Method",
"version": "v1.0-20181001",
"license": {
  "name": "OCF Data Model License",
  "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbc8bdc4ba/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/doxm": {
    "get": {
      "description": "This Resource specifies properties needed to establish a Device owner.\n",
      "parameters": [
        {"$ref": "/#/parameters/interface"}
      ],
      "responses": {
        "200": {
          "description": "",
          "x-example": {
            "rt": ["oic.r.doxm"],
            "oxms": [ 0, 2, 3 ],
            "oxmsel": 0,
            "sct": 16,
            "owned": true,
            "deviceuuid": "de305d54-75b4-431b-adb2-eb6b9e546014",
            "devowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
            "rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
          }
        },
        "400": {
          "description": ""
        }
      }
    },
    "post": {
      "description": "Updates the DOXM Resource data.\n",
      "parameters": [
        {"$ref": "/#/parameters/interface"},
        {"name": "body",
         "in": "body",
         "required": true,
         "schema": { "$ref": "/#definitions/Doxm-Update" },
         "x-example": {
           "oxmsel": 0,
           "owned": true,
           "deviceuuid": "de305d54-75b4-431b-adb2-eb6b9e546014",
           "devowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9",
           "rowneruuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"
         }
      },
      "responses": {
        "400": {
          "description": "The request is invalid."
        },
        "204": {
          "description": "The DOXM entry is updated."
        }
      }
    }}}}
"interface": {
  "in": "query",
  "name": "if",
  "type": "string",
  "enum": ["oic.if.baseline"]
},
"definitions": {
  "Doxm": {
    "properties": {
      "owneruuid": {
        "description": "Format pattern according to IETF RFC 4122.",
        "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
        "type": "string"
      },
      "oxms": {
        "description": "List of supported owner transfer methods.",
        "items": {
          "description": "The Device owner transfer methods that may be selected at Device onboarding. Each value indicates a specific Owner Transfer method: 0 - Numeric OTM identifier for the Just-Works method (oic.sec.doxm.jw) 1 - Numeric OTM identifier for the random PIN method (oic.sec.doxm.rdp) 2 - Numeric OTM identifier for the manufacturer certificate method (oic.sec.doxm.mfgcert) 3 - Numeric OTM identifier for the decap method (oic.sec.doxm.dcap) (deprecated).",
          "type": "integer"
        },
        "readOnly": true,
        "type": "array"
      },
      "deviceuuid": {
        "description": "The uuid formatted identity of the Device\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}$",
        "type": "string"
      },
      "owned": {
        "description": "Ownership status flag.",
        "type": "boolean"
      },
      "n": {
        "$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"
      },
      "oxmsel": {
        "description": "The selected owner transfer method used during on-boarding\nThe Device owner transfer methods that may be selected at Device on-boarding. Each value indicates a specific Owner Transfer method: 0 - Numeric OTM identifier for the Just-Works method (oic.sec.doxm.jw) 1 - Numeric OTM identifier for the random PIN method (oic.sec.doxm.rdp) 2 - Numeric OTM identifier for the manufacturer certificate method (oic.sec.doxm.mfgcert) 3 - Numeric OTM identifier for the decap method (oic.sec.doxm.dcap) (deprecated).",
        "type": "integer"
      },
      "sct": {
        "description": "Bitmask encoding of supported credential types\nCredential Types - Cred type encoded as a bitmask: 0 - Empty credential used for testing 1 - Symmetric pair-wise key 2 - Symmetric group key 4 - Asymmetric signing key 8 - Asymmetric signing key with certificate 16 - PIN or
password32 - Asymmetric encryption key.

    "maximum": 63,
    "minimum": 0,
    "type": "integer",
    "readOnly": true
},

"rt": {
    "description": "Resource Type of the Resource.",
    "items": {
        "maxLength": 64,
        "type": "string",
        "enum": ["oic.r.doxm"]
    },
    "minItems": 1,
    "readOnly": true,
    "type": "array"
},

"if": {
    "description": "The interface set supported by this Resource.",
    "items": {
        "enum": ["oic.if.baseline"
    },
    "minItems": 1,
    "readOnly": true,
    "type": "array"
}

"type": "object",
"required": ["oxms", "oxmsel", "sct", "owned", "deviceuuid", "devowneruuid", "rowneruuid""]

"Doxm-Update": {
    "properties": {
        "rowneruuid": {
            "description": "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}$",
            "type": "string"
        },
        "devowneruuid": {
            "description": "Format pattern according to IETF RFC 4122.",
            "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
            "type": "string"
        },
        "deviceuuid": {
            "description": "The uuid formatted identity of the Device\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"
        },
        "owned": {
            "description": "Ownership status flag.",
            "type": "boolean"
        },
        "oxmsel": {
            "description": "The selected owner transfer method used during on-boarding\nThe Device owner transfer methods that may be selected at Device on-boarding. Each value indicates a specific Owner Transfer method0 - Numeric OTM identifier for the Just-Works method (oic.sec.doxm.jw)1 - Numeric OTM identifier for the random PIN method (oic.sec.doxm.rdp)2 - Numeric OTM identifier for the manufacturer certificate method (oic.sec.doxm.mfgcert)3 - Numeric OTM identifier for the decap method (oic.sec.doxm.dcap) (deprecated).",
            "type": "integer"
        }
    },
    "type": "object"}
### Property Definition

Table C.16 defines the Properties that are part of the "oic.r.doxm" Resource Type.

**Table C.16 – The Property definitions of the Resource with type "rt" = "oic.r.doxm".**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>owned</td>
<td>boolean</td>
<td>Yes</td>
<td>Read Write</td>
<td>Ownership status flag.</td>
</tr>
<tr>
<td>oxmsel</td>
<td>integer</td>
<td>Yes</td>
<td>Read Write</td>
<td>The selected owner transfer method used during on-boarding. The Device owner transfer methods that may be selected at Device on-boarding. Each value indicates a specific Owner Transfer method: 0 - Numeric OTM identifier for the Just-Works method (oic.sec.doxm.jw) 1 - Numeric OTM identifier for the random PIN method (oic.sec.doxm.rdp) 2 - Numeric OTM identifier for the manufacturer certificate method (oic.sec.doxm.mfgcert) 3 - Numeric OTM identifier for the decap method (oic.sec.doxm.dcap) (deprecated).</td>
</tr>
<tr>
<td>deviceuuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>The uuid formatted identity of the Device. Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td>List of supported owner transfer methods.</td>
</tr>
<tr>
<td>oxms</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Only</td>
<td></td>
</tr>
<tr>
<td>devowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>sct</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td>Bitmask encoding of...</td>
</tr>
<tr>
<td>supported credential types</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credential Types - Cred type encoded as a bitmask. 0 - Empty credential used for testing 1 - Symmetric pair-wise key 2 - Symmetric group key 4 - Asymmetric signing key 8 - Asymmetric signing key with certificate 16 - PIN or password 32 - Asymmetric encryption key.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>rowneruuid</th>
<th>string</th>
<th>Read Write</th>
<th>Format pattern according to IETF RFC 4122.</th>
</tr>
</thead>
<tbody>
<tr>
<td>owned</td>
<td>boolean</td>
<td>Read Write</td>
<td>Ownership status flag.</td>
</tr>
<tr>
<td>oxmsel</td>
<td>integer</td>
<td>Read Write</td>
<td>The selected owner transfer method used during on-boarding. The Device owner transfer methods that may be selected at Device on-boarding. Each value indicates a specific Owner Transfer method 0 - Numeric OTM identifier for the Just-Works method (oic.sec.doxm.jw) 1 - Numeric OTM identifier for the random PIN method (oic.sec.doxm.rdp) 2 - Numeric OTM identifier for the manufacturer certificate method (oic.sec.doxm.mfgcert) 3 - Numeric OTM identifier for the decap method (oic.sec.doxm.dcap) (deprecated).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>devowneruuid</th>
<th>string</th>
<th>Read Write</th>
<th>Format pattern according to IETF RFC 4122.</th>
</tr>
</thead>
<tbody>
<tr>
<td>deviceuuid</td>
<td>string</td>
<td>Read Write</td>
<td>The uuid formatted identity of the Device Format pattern according to IETF RFC 4122.</td>
</tr>
</tbody>
</table>
C.9.6 CRUDN behaviour

Table C.17 defines the CRUDN operations that are supported on the "oic.r.doxm" Resource Type.

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td></td>
<td></td>
<td>observe</td>
</tr>
</tbody>
</table>

C.10 Device Provisioning Status

C.10.1 Introduction

This Resource specifies Device provisioning status.

C.10.2 Well-known URI

/oic/sec/pstat

C.10.3 Resource type

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

C.10.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Device Provisioning Status",
    "version": "v1.0-20191001",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbcc8bdc4ba/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/pstat": {
      "get": {
        "description": "This Resource specifies Device provisioning status.\n",
        "parameters": [
          {"$ref": "/parameters/interface"}
        ],
        "responses": {
          "200": {
            "description": "",
            "x-example": {
              "rt": ["oic.r.pstat"],
              "dos": {"s": 3, "p": true},
              "isop": true,
              "cm": 8,
              "tm": 60,
              "cm": 2,
              "sm": 7,
              "rowneruuid": "de305d54-75b4-431b-adb2-eb6b9e546014"
            },
            "schema": { "$ref": "/definitions/Pstat" }
          },
          "400": { "description": "The request is invalid." }
        }
      }
    }
  }
}
```
"post": {
  "description": "Sets or updates Device provisioning status data.\n",
  "parameters": [
    { "$ref": "#/parameters/interface" },
    {
      "name": "body",
      "in": "body",
      "required": true,
      "schema": { "$ref": "#/definitions/Pstat-Update" },
      "x-example": {
        "dos": { "s": 3 },
        "tm": 60,
        "om": 2,
        "rowneruuid": "de305d54-75b4-431b-adb2-eb6b9e546014"
      }
    }
  ],
  "responses": {
    "400": {
      "description": "The request is invalid."
    },
    "204": {
      "description": "The PSTAT entry is updated."
    }
  }
},

"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},

"definitions": {
  "Pstat": {
    "properties": {
      "rowneruuid": {
        "description": "The UUID formatted identity of the Resource owner\nFormat pattern according to IETF RFC 4122.\n",
        "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.pstat"]
        },
        "minItems": 1,
        "readOnly": true,
        "type": "array"
      },
      "om": {
        "description": "Current operational mode\nDevice provisioning operation may be server directed or client (aka provisioning service) directed. The value is a bitmask encoded as integer and indicates the provisioning operation modes1 - Server-directed utilizing multiple provisioning services2 - Server-directed utilizing a single provisioning service3 - Client-directed provisioning8 - Unused16 - Unused32 - Unused64 - Unused128 - Unused.\n",
        "maximum": 7,
        "minimum": 1,
        "type": "integer"
      },
      "cm": {
        "description": "Current Device provisioning mode\nDevice provisioning mode maintains a bitmask of the possible provisioning states of a Device. The value can be either 8 or 16 character
in length. If its only 8 characters it represents the lower byte value1 - Manufacturer reset state2
- Device pairing and owner transfer state4 - Unused8 - Provisioning of credential management
services16 - Provisioning of access management services32 - Provisioning of local ACLs64 - Initiate
Software Version Validation128 - Initiate Secure Software Update.

 maximum": 255,
 "minimum": 0,
 "type": "integer",
 "readOnly": true
 },
 "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"
 },
 "isop": {
 "description": "true indicates Device is operational.",
 "readOnly": true,
 "type": "boolean"  
 },
 "tm": {
 "description": "Target Device provisioning mode
Device provisioning mode maintains a
bitmask of the possible provisioning states of a Device. The value can be either 8 or 16 character
in length. If its only 8 characters it represents the lower byte value1 - Manufacturer reset state2
- Device pairing and owner transfer state4 - Unused8 - Provisioning of credential management
services16 - Provisioning of access management services32 - Provisioning of local ACLs64 - Initiate
Software Version Validation128 - Initiate Secure Software Update.

 maximum": 255,
 "minimum": 0,
 "type": "integer"
 },
 "sm": {
 "description": "Supported operational modes
Device provisioning operation may be server
directed or client (aka provisioning service) directed. The value is a bitmask encoded as integer
and indicates the provisioning operation mode1 - Server-directed utilizing multiple provisioning
services2 - Server-directed utilizing a single provisioning service4 - Client-directed provisioning8
- Unused16 - Unused32 - Unused64 - Unused128 - Unused.

 maximum": 7,
 "minimum": 1,
 "type": "integer",
 "readOnly": true
 },
 "dos": {
 "description": "Device on-boarding state
Device operation state machine.",
 "properties": {
 "p": {
 "default": true,
 "description": "'p' is TRUE when the 's' state is pending until all necessary changes
to Device Resources are complete.",
 "readOnly": true,
 "type": "boolean"
 },
 "s": {
 "description": "The current or pending operational state.",
 "x-detail-desc": [
 "0 - RESET - Device reset state.",
 "1 - RFOTM - Ready for Device owner transfer method state.",
 "2 - RFPRO - Ready for Device provisioning state.",
 "3 - RFNOP - Ready for Device normal operation state.",
 "4 - SRESET - The Device is in a soft reset state."]
 },
 "maximum": 4,
 "minimum": 0,
 "type": "integer"
 }  
 },
 "required": [  
}
"s": {  
    "type": "object"  
  },

"if": {  
  "description": "The interface set supported by this Resource.",  
  "items": {  
    "enum": [  
      "oic.if.baseline"  
    ],  
    "type": "string"  
  },  
  "minItems": 1,  
  "readOnly": true,  
  "type": "array"  
},

  "type": "object",  
  "required": ["dos", "isop", "cm", "tm", "om", "sm", "rowneruuid"]

"Pstat-Update": {  
  "properties": {  
    "rowneruuid": {  
      "description": "The UUID formatted identity of the Resource owner
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"  
    },  
    "om": {  
      "description": "Current operational mode\nDevice provisioning operation may be server directed or client (aka provisioning service) directed. The value is a bitmask encoded as integer and indicates the provisioning operation modes1 - Server-directed utilizing multiple provisioning services2 - Server-directed utilizing a single provisioning service4 - Client-directed provisioning8 - Unused16 - Unused32 - Unused64 - Unused128 - Unused.",  
      "maximum": 7,  
      "minimum": 1,  
      "type": "integer"  
    },  
    "tm": {  
      "description": "Target Device provisioning mode\nDevice provisioning mode maintains a bitmask of the possible provisioning states of a Device. The value can be either 8 or 16 character in length. If its only 8 characters it represents the lower byte value1 - Manufacturer reset state2 - Device pairing and owner transfer state4 - Unused6 - Provisioning of credential management services16 - Provisioning of access management services32 - Provisioning of local ACLs64 - Initiate Software Version Validation128 - Initiate Secure Software Update.",  
      "maximum": 255,  
      "minimum": 0,  
      "type": "integer"  
    },  
    "dos": {  
      "description": "Device on-boarding state\nDevice operation state machine.",  
      "properties": {  
        "p": {  
          "default": true,  
          "description": "p is TRUE when the 's' state is pending until all necessary changes to Device Resources are complete.",  
          "readOnly": true,  
          "type": "boolean"  
        },  
        "s": {  
          "description": "The current or pending operational state.",  
          "x-detail-desc": [  
            "0 - RESET - Device reset state.",  
            "1 - RFOTM - Ready for Device owner transfer method state.",  
            "2 - RFPRO - Ready for Device provisioning state.",  
            "3 - RFNOP - Ready for Device normal operation state.",  
            "4 - SRESET - The Device is in a soft reset state."  
          ],  
          "maximum": 4,  
          "minimum": 0,  
          "type": "integer"  
        }  
      }  
    }  
  }  
}
C.10.5 Property definition

Table C.18 defines the Properties that are part of the "oic.r.pstat" Resource Type.

Table C.18 – The Property definitions of the Resource with type "rt" = "oic.r.pstat".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos</td>
<td>object: see schema</td>
<td>No</td>
<td>Read Write</td>
<td>Device on-boarding state, Device operation state machine.</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>No</td>
<td>Read Write</td>
<td>The UUID formatted identity of the Resource owner Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>tm</td>
<td>integer</td>
<td>No</td>
<td>Read Write</td>
<td>Target Device provisioning mode, Device provisioning mode maintains a bitmask of the possible provisioning states of a Device. The value can be either 8 or 16 character in length. If it's only 8 characters it represents the lower byte value1 - Manufacturer reset state2 - Device pairing and owner transfer state4 - Unused8 - Provisioning of credential management</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Access</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>om</td>
<td>integer</td>
<td>No</td>
<td>Read Write</td>
<td>Current operational mode. Device provisioning operation may be server directed or client (aka provisioning service) directed. The value is a bitmask encoded as integer and indicates the provisioning operation modes: 1 - Server-directed utilizing multiple provisioning services, 2 - Server-directed utilizing a single provisioning service, 4 - Client-directed provisioning, 8 - Unused, 16 - Unused, 32 - Unused, 64 - Unused, 128 - Unused.</td>
</tr>
<tr>
<td>isop</td>
<td>boolean</td>
<td>Yes</td>
<td>Read Only</td>
<td>true indicates Device is operational.</td>
</tr>
<tr>
<td>cm</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td>Current Device provisioning mode. Device provisioning mode maintains a bitmask of the</td>
</tr>
<tr>
<td>sm</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>-----</td>
<td>-----------</td>
<td></td>
</tr>
</tbody>
</table>

Supported operational modes
Device provisioning operation may be server directed or client (aka provisioning service) directed. The value is a bitmask encoded as integer and indicates the provisioning operation modes:

- **1** - Server-directed
- **2** - Client-directed
- **4** - Device-directed
- **8** - Manufacturer reset state
- **16** - Device pairing state
- **32** - Owner transfer state
- **64** - Unused state
- **128** - Provisioning of credential management services
- **256** - Provisioning of access management services
- **512** - Provisioning of local ACLs
- **1024** - Initiate Software Version Validation
- **2048** - Initiate Secure Software Update.
<table>
<thead>
<tr>
<th>Mode</th>
<th>Data Type</th>
<th>Access</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>om</td>
<td>integer</td>
<td>Yes</td>
<td>Read Write</td>
<td>Current operational mode Device provisioning operation may be server-directed or client-directed (aka provisioning service) directed. The value is a bitmask encoded as integer and indicates the provisioning operation modes: 1 - Server-directed utilizing multiple provisioning services, 2 - Server-directed utilizing a single provisioning service, 4 - Client-directed provisioning, 8 - Unused, 16 - Unused, 32 - Unused, 64 - Unused, 128 - Unused.</td>
</tr>
<tr>
<td>tm</td>
<td>integer</td>
<td>Yes</td>
<td>Read Write</td>
<td>Target Device provisioning mode Device provisioning mode maintains a bitmask of the possible provisioning states of a Device. The value can be</td>
</tr>
</tbody>
</table>
either 8 or 16 character in length. If it's only 8 characters it represents the lower byte value.
- Manufacturer reset state
- Device pairing and owner transfer state
- Unused
- Provisioning of credential management services
- Provisioning of access management services
- Provisioning of local ACLs
- Initiate Software Version Validation
- Initiate Secure Software Update.

<table>
<thead>
<tr>
<th>id</th>
<th>multiple types: see schema</th>
<th>No</th>
<th>Read Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
</tr>
<tr>
<td>dos</td>
<td>object: see schema</td>
<td>Yes</td>
<td>Read Write</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
</tr>
<tr>
<td>rowneruuid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
</tr>
</tbody>
</table>

C.10.6 CRUDN behaviour

Table C.19 defines the CRUDN operations that are supported on the "oic.r.pstat" Resource Type.

Table C.19 – The CRUDN operations of the Resource with type "rt" = "oic.r.pstat".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
</table>

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
C.11 Asserted Roles

C.11.1 Introduction

This Resource specifies roles that have been asserted.

C.11.2 Well-known URI

/oic/sec/roles

C.11.3 Resource type

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

C.11.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Asserted Roles",
    "version": "v1.0-20170323",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/roles" : {
      "get": {
        "description": "This Resource specifies roles that have been asserted.
        
        "parameters": ["$ref": "/parameters/interface"
      ],
      "responses": {
        "200": {
          "description": "",
          "x-example": {
            "roles": [
              {
                "credid": 1,
                "credtype": 8,
                "subjectuuid": "00000000-0000-0000-0000-000000000000",
                "publicdata": {
                  "encoding": "oic.sec.encoding.pem",
                  "data": "PEMENCODEDROLECERT"
                },
                "optionaldata": {
                  "revstat": false,
                  "encoding": "oic.sec.encoding.pem",
                  "data": "PEMENCODEDISSUERCERT"
                }
              },
              {
                "credid": 2,
                "credtype": 8,
                "subjectuuid": "00000000-0000-0000-0000-000000000000",
                "publicdata":
              }
            ]
          }
        }
      }
    }
  }
}
```
"post": {
  "description": "Update the roles Resource, i.e., assert new roles to this server.
New role certificates that match an existing certificate (i.e., publicdata and optionaldata are the same) are not added to the Resource (and 204 is returned). The provided credid values are ignored, the Resource assigns its own.
",
  "parameters": [
    {
      "$ref": "#/parameters/interface",
      "name": "body",
      "in": "body",
      "required": true,
      "schema": {
        "$ref": "#/definitions/Roles-update" }
    },
    {
      "roles": [
        {
          "credid": 1,
          "credtype": 8,
          "subjectuuid": "00000000-0000-0000-0000-000000000000",
          "publicdata": {
            "encoding": "oic.sec.encoding.pem",
            "data": "PEMENCODEDROLECERT"
          },
          "optionaldata": {
            "revstat": false,
            "encoding": "oic.sec.encoding.pem",
            "data": "PEMENCODEDISSUERCERT"
          }
        },
        {
          "credid": 2,
          "credtype": 8,
          "subjectuuid": "00000000-0000-0000-0000-000000000000",
          "publicdata": {
            "encoding": "oic.sec.encoding.pem",
            "data": "PEMENCODEDROLECERT"
          },
          "optionaldata": {
            "revstat": false,
            "encoding": "oic.sec.encoding.pem",
            "data": "PEMENCODEDISSUERCERT"
          }
        }
      ]
    }
  ]
}


```json
"responses": {
  "400": {
    "description": "The request is invalid."
  },
  "204": {
    "description": "The roles entry is updated."
  }
},
"delete": {
  "description": "Deletes roles Resource entries.
  When DELETE is used without query parameters, all the roles entries are deleted.
  When DELETE is used with a query parameter, only the entries matching
  the query parameter are deleted.
  
  Parameters:
  - interface
    - in: "query",
    - name: "if",
    - type: "string",
    - enum: ["oic.if.baseline"]
  - roles-filtered
    - in: "query",
    - name: "credid",
    - required: false,
    - type: "integer",
    - description: "Only applies to the credential with the specified credid."

  Responses:
  - 200: {
    "description": "The specified or all roles Resource entries have been successfully deleted."
  },
  - 400: {
    "description": "The request is invalid."
  }
},
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  },
  "roles-filtered": {
    "in": "query",
    "name": "credid",
    "required": false,
    "type": "integer",
    "description": "Only applies to the credential with the specified credid."
  }
},
"definitions": {
  "Roles": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource."
      },
      "maxLength": 64,
      "type": "string",
      "enum": ["oic.r.roles"]
    },
    "minItems": 1,
    "readOnly": true,
    "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"
  }
}
```
"roles": {  
  "description": "List of role certificates.",

  "items": {  
    "properties": {  
      "credid": {  
        "description": "Local reference to a credential Resource.",
        "type": "integer"
      },

      "credtype": {  
        "description": "Representation of this credential's type\nCredential Types - Cred
type encoded as a bitmask.0 - Empty credential used for testing1 - Symmetric pair-wise key2 -
Symmetric group key4 - Asymmetric signing key8 - Asymmetric signing key with certificate16 - PIN or
password32 - Asymmetric encryption key.",
        "maximum": 63,
        "minimum": 0,
        "type": "integer"
      },

      "credusage": {  
        "description": "A string that provides hints about how/where the cred is used\nThe type of credusage.oic.sec.cred.trustca - Trust certificateoic.sec.cred.cert -
Certificateoic.sec.cred.rolecert - Role Certificateoic.sec.cred.mfgtrustca - Manufacturer
Certificate Trust Anchoroic.sec.cred.mfgcert - Manufacturer Certificate.",
        "enum": [  
          "oic.sec.cred.trustca",
          "oic.sec.cred.cert",
          "oic.sec.cred.rolecert",
          "oic.sec.cred.mfgtrustca",
          "oic.sec.cred.mfgcert"
        ],
        "type": "string"
      },

      "crms": {  
        "description": "The refresh methods that may be used to update this credential.",
        "items": {  
          "description": "Each enum represents a method by which the credentials are
refreshed.oic.sec.crm.pro - Credentials refreshed by a provisioning serviceoic.sec.crm.rdp -
Credentials refreshed by a key agreement protocol and random PINoic.sec.crm.psk - Credentials
refreshed by a key agreement protocoloic.sec.crm.skdc - Credentials refreshed by a key distribution
serviceoic.sec.crm.pk10 - Credentials refreshed by a PKCS\#10 request to a CA.",
          "enum": [  
            "oic.sec.crm.pro",
            "oic.sec.crm.psk",
            "oic.sec.crm.rdp",
            "oic.sec.crm.skdc",
            "oic.sec.crm.pk10"
          ],
          "type": "string"
        },

        "type": "array"
      },

      "optionaldata": {  
        "description": "Credential revocation status information\nOptional credential contents describes revocation status for this credential.",
        "properties": {  
          "data": {  
            "description": "This is the encoded structure.",
            "type": "string"
          },

          "encoding": {  
            "description": "A string specifying the encoding format of the data contained in
the optdata.",
            "x-detail-desc": [  
              "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
              "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
              "oic.sec.encoding.base64 - Base64 encoded object.",
              "oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain.",
              "oic.sec.encoding.der - Encoding for DER encoded certificate.",
              "oic.sec.encoding.raw - Raw hex encoded data."
            ],
            "enum": [

"oic.sec.encoding.jwt",
"oic.sec.encoding.cwt",
"oic.sec.encoding.base64",
"oic.sec.encoding.pem",
"oic.sec.encoding.der",
"oic.sec.encoding.raw"
],
"type": "string"
},
"revstat": {
  "description": "Revocation status flag - true = revoked.",
  "type": "boolean"
}
},
"required": [
"revstat"
],
"type": "object"
},
"period": {
  "description": "String with RFC5545 Period.",
  "type": "string"
}]
},
"privateData": {
  "description": "Private credential information\nCredential Resource non-public contents.",
  "properties": {
    "data": {
      "description": "The encoded value.",
      "maxLength": 3072,
      "type": "string"
    },
    "encoding": {
      "description": "A string specifying the encoding format of the data contained in
the privdata.",
      "x-detail-desc": [
        "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
        "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
        "oic.sec.encoding.base64 - Base64 encoded object.",
        "oic.sec.encoding.uri - URI reference.",
        "oic.sec.encoding.handle - Data is contained in a storage sub-system
referenced using a handle.",
        "oic.sec.encoding.raw - Raw hex encoded data."
      ],
      "enum": [
        "oic.sec.encoding.jwt",
        "oic.sec.encoding.cwt",
        "oic.sec.encoding.base64",
        "oic.sec.encoding.uri",
        "oic.sec.encoding.handle",
        "oic.sec.encoding.raw"
      ],
      "type": "string"
    },
    "handle": {
      "description": "Handle to a key storage Resource.",
      "type": "integer"
    }
  },
  "required": [
    "encoding"
  ],
  "type": "object"
},
"publicData": {
  "description": "Public credential information.",
  "properties": {
    "data": {
      "description": "This is the encoded value.",
      "maxLength": 3072,
      "type": "string"
    }
  }
}
"encoding": {
    "description": "A string specifying the encoding format of the data contained in
the pubdata."
},
"encoding": {
    "description": "The role this credential possesses
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"]
},
"roleid": {
    "description": "The id of the Device, which the cred entry applies to or "*"
for wildcard identity.",
    "pattern": "^\*$",
    "type": "string"
},
"subjectuuid": {
    "anyOf": [
        {
            "description": "Format pattern according to IETF RFC 4122.",
            "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
            "type": "string"
        }
    ]
},
"if": {
    "description": "The interface set supported by this Resource.",
    "items": {
        "enum": ["oic.sec.encoding.jwt", "oic.sec.encoding.cwt", "oic.sec.encoding.base64", "oic.sec.encoding.uri", "oic.sec.encoding.pem", "oic.sec.encoding.der", "oic.sec.encoding.raw"]
    }
}
"oic.if.baseline"
},
  "type": "string"
},
  "minItems": 1,
  "readOnly": true,
  "type": "array"
}
}
"type": "object",
"required": ["roles"]
},
"Roles-update" : {
  "properties": {
    "roles": {
      "description": "List of role certificates.",
      "items": {
        "properties": {
          "credid": {
            "description": "Local reference to a credential Resource."
          },
          "type": "integer"
        },
        "credtype": {
          "description": "Representation of this credential's type\nCredential Types - Cred
type encoded as a bitmask.0 - Empty credential used for testing1 - Symmetric pair-wise key2 -
Symmetric group key4 - Asymmetric signing key8 - Asymmetric signing key with certificate16 - PIN or
password32 - Asymmetric encryption key.\n",
          "maximum": 63,
          "minimum": 0,
          "type": "integer"
        },
        "credusage": {
          "description": "A string that provides hints about how/where the cred is used\nThe
type of credusage.oic.sec.cred.trustca - Trust certificate.oic.sec.cred.cert -
Certificate.oic.sec.cred.rolecert - Role Certificate.oic.sec.cred.mfgtrustca - Manufacturer
Certificate Trust Anchor.oic.sec.cred.mfgcert - Manufacturer Certificate.\n",
          "enum": ["oic.sec.cred.trustca", "oic.sec.cred.cert", "oic.sec.cred.rolecert", "oic.sec.cred.mfgtrustca", "oic.sec.cred.mfgcert"],
          "type": "string"
        },
        "crems": {
          "description": "The refresh methods that may be used to update this credential.\n",
          "items": {
            "description": "Each enum represents a method by which the credentials are
refreshed.oic.sec.crm.pro - Credentials refreshed by a provisioning service.oic.sec.crm.rdp -
Credentials refreshed by a key agreement protocol and random PIN.oic.sec.crm.psk - Credentials
refreshed by a key agreement protocol.oic.sec.crm.skdc - Credentials refreshed by a key distribution
service.oic.sec.crm.pk10 - Credentials refreshed by a PKCS#10 request to a CA."
          },
          "type": "array"
        },
        "optionaldata": {
          "description": "Credential revocation status information\nOptional credential
contents describes revocation status for this credential."
        },
        "properties": {
          "data": {
            "description": "This is the encoded structure."
          },
          "type": "string"
        }
      }
    }
  }
}
"encoding": { ""description": "A string specifying the encoding format of the data contained in the optdata."
},

"revstat": { 
  ""description": "Revocation status flag - true = revoked."
},

"period": { ""description": "String with RFC5545 Period."
},

"privatedata": { 
  ""description": "Private credential information
Credential Resource non-public contents."
},

"data": { ""description": "The encoded value."
},

"encoding": { ""description": "A string specifying the encoding format of the data contained in
the privdata."
},
"required": [ 
  "encoding"
],
"type": "object"
}
,"publicdata": {
  "description": "Public credential information.",
  "properties": {
    "data": {
      "description": "The encoded value.",
      "maxLength": 3072,
      "type": "string"
    }
  }
},
"encoding": {
  "description": "A string specifying the encoding format of the data contained in
the pubdata.",
  "x-detail-desc": [ 
    "oic.sec.encoding.jwt - RFC7517 JSON web token (JWT) encoding.",
    "oic.sec.encoding.cwt - RFC CBOR web token (CWT) encoding.",
    "oic.sec.encoding.base64 - Base64 encoded object.",
    "oic.sec.encoding.uri - URI reference.",
    "oic.sec.encoding.pem - Encoding for PEM encoded certificate or chain.",
    "oic.sec.encoding.der - Encoding for DER encoded certificate.",
    "oic.sec.encoding.raw - Raw hex encoded data."
  ]
},
"required": [ 
    "role"
]
},
"type": "object"
}
,"roleid": {
  "description": "The role this credential possesses
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"
},
"subjectuuid": {
  "anyOf": [ 
    { 
      "description": "The id of the Device, which the cred entry applies to or \"*\"
for wildcard identity.",
      "pattern": "\"*\"$",
      "type": "string"
    },
    { 
      "description": "Format pattern according to IETF RFC 4122.",
      "pattern": "\^[a-fA-F0-9]{8}-\^[a-fA-F0-9]{4}-\^[a-fA-F0-9]{4}-\^[a-fA-F0-9]{4}-\^[a-fA- 
F0-9]{12}$\"",
      "type": "string"
    }
  ]
}
C.11.5 Property definition

Table C.20 defines the Properties that are part of the "oic.r.roles" Resource Type.

Table C.20 – The Property definitions of the Resource with type "rt" = "oic.r.roles".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>List of role certificates.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>roles</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>List of role certificates.</td>
</tr>
</tbody>
</table>

C.11.6 CRUDN behaviour

Table C.21 defines the CRUDN operations that are supported on the "oic.r.roles" Resource Type.

Table C.21 – The CRUDN operations of the Resource with type "rt" = "oic.r.roles".

Create Read Update Delete Notify
get    post    delete    observe

C.12 Signed Access Control List

C.12.1 Introduction

This Resource specifies a signed ACL object.

C.12.2 Well-known URI

/oic/sec/sacl

C.12.3 Resource type

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

C.12.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
```
"title": "Signed Access Control List",
"version": "v1.0-20150819",
"license": {
"name": "OCF Data Model License",
"url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/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/sacl": {
"get": {
"description": "This Resource specifies a signed ACL object.",
"parameters": [
{"$ref": "#/parameters/interface"}
],
"responses": {
"200": {
"description": "",
"x-example": {
"rt": ["oic.r.sacl"],
"aclist2": {
"aceid": 1,
"subject": {"uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9"},
"resources": [
{"href": "/temp",
"rt": ["oic.r.temperature"],
"if": ["oic.if.baseline", "oic.if.a"]
},
{"href": "/temp",
"rt": ["oic.r.temperature"],
"if": ["oic.if.baseline", "oic.if.s"]
]
},
"permission": 31,
"validity": {
"period": "20160101T180000Z/20170102T070000Z",
"recurrence": ["DSTART:XXXXX",
"RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1"]
}
},
"period": "20160101T180000Z/20170102T070000Z",
"recurrence": ["DSTART:XXXXX",
"RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1"]
}
},
"aceid": 2,
"subject": {
"authority": "484b8a51-db23-46c0-a5f1-b4aebe50ebe",
"role": "SOME_STRING"
},
"resources": [
{"href": "/light",
"rt": ["oic.r.light"],
"if": ["oic.if.baseline", "oic.if.a"]
},
{"href": "/door",
"rt": ["oic.r.door"],
"if": ["oic.if.baseline", "oic.if.a"]
}
]
"rt": ["oic.r.temperature"],
"if": ["oic.if.baseline", "oic.if.a"]
},
"permission": 15
],
"signature": {
"sigtype": "oic.sec.sigtype.pk7",
"sigvalue": "ENCODING-SIGNATURE-VALUE"
},
"schema": { "$ref": "#/definitions/Sacl" }
},
"post": {
"description": "Sets the acl Resource data.\n",
"parameters": [
{$ref": "/#/parameters/interface"},
{
"name": "body",
"in": "body",
"required": true,
"schema": { "$ref": "/#/definitions/Sacl" },
"x-example": {
"aclist2": [
{ "aceid": 1,
"subject": {"uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d0d49"},
"resources": [ {
"href": "/temp",
"rt": ["oic.r.temperature"],
"if": ["oic.if.baseline", "oic.if.a"]
},
{ "href": "/temp",
"rt": ["oic.r.temperature"],
"if": ["oic.if.baseline", "oic.if.s"]
}]
},
"permission": 31,
"validity": [ { "period": "20160101T180000Z/20170102T070000Z",
"recurrence": [ "DSTART:XXXXXXXX",
"RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONT=1" ]
}]
},
"aceid": 2,
"subject": { 
"authority": "4848a51-cb23-46c0-a5f1-b4aebe50ebe",
"role": "SOME_STRING"
},
"resources": [ {
"href": "/light",
"rt": ["oic.r.light"],
"if": ["oic.if.baseline", "oic.if.a"]
},
{ "href": "/door",
"rt": ["oic.r.door"],
"if": ["oic.if.baseline", "oic.if.a"]
}
"permission": 15
"signature": {
  "sigtype": "oic.sec.sigtype.pk7",
  "sigvalue": "ENCODED-SIGNATURE-VALUE"
}

"responses": {
  "400": {
    "description": "The request is invalid."
  },
  "201": {
    "description": "The ACL entry is created."
  },
  "204": {
    "description": "The ACL entry is updated."
  }
}

"put": {
  "description": "Sets the acl Resource data\n",
  "parameters": {
    "/parameters/interface",
    { "name": "body",
      "in": "body",
      "required": true,
      "schema": { "$ref": "/definitions/Sacl" },
      "x-example":{
        "aclist2":[
          {
            "aceid": 1,
            "subject": { "uuid": "e61c3e6b-9c54-4b81-8ce5-f9039c1d04d9" },
            "resources": {
              "href": "/temp",
              "rt": ["oic.r.temperature"],
              "if": ["oic.if.baseline", "oic.if.a"]
            },
          },
          {
            "href": "/temp",
            "rt": ["oic.r.temperature"],
            "if": ["oic.if.baseline", "oic.if.s"]
          }
        ],
        "permission": 31,
        "validity": {
          "period": "20160101T180000Z/20170102T070000Z",
          "recurrence": [ "DSTART:XXXXX",
                          "RRULE:FREQ=DAILY;UNTIL=20180131T140000Z;BYMONTH=1" ]
        }
      }},
      { 
        "aceid": 2,
        "subject": { 
          "authority": "685b94f5-cb23-45a0-a5f1-b4aebef50ebe",
          "role": "SOME_STRING"
        }
      }
    }
  }
}
"resources": [
  {
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.baseline", "oic.if.a"],
  },
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.baseline", "oic.if.a"],
  }
],
"permission": 15
"signature": {
  "sigtype": "oic.sec.sigtype.pk7",
  "sigvalue": "ENCODED-SIGNATURE-VALUE"
}
],
"responses": {
  "400": {
    "description": "The request is invalid."
  },
  "201": {
    "description": "The signed ACL entry is created."
  }
},
"delete": {
  "description": "Deletes the signed ACL data. When DELETE is used without query parameters, the entire collection is deleted. When DELETE is used with the query parameter where "acl" is specified, only the matched entry is deleted."
  "parameters": {
    "$ref": "/parameters/interface",
    "in": "query",
    "description": "Delete the signed ACL identified by the string containing subject UUID."
  },
  "responses": {
    "200": {
      "description": "The signed ACL instance or the the entire signed ACL Resource has been successfully deleted."
    },
    "400": {
      "description": "The request is invalid."
    }
  }
},
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "Sacl": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource."
      },
      "items": {
      
    }}}}
"maxLength": 64,
"type": "string",
"enum": ["oic.r.sacl"]
},
"minItems": 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": {
        "properties": {
          "href": {
            "allOf": [
              {
                "description": "When present, the ACE only applies when the href matches."
              },
              {
                "description": "This is the target URI, it can be specified as a Relative
Reference or fully-qualified URI."
              }
            ]
          }
        },
        "if": {
        "description": "When present, the ACE only applies when the if (interface)
matches\nThe interface set supported by this Resource."
      }
    }
  }
}
"rt": {
    "description": "When present, the ACE only applies when the rt (resource type) matches
Resource Type of the Resource.",
    "items": {
        "maxLength": 64,
        "type": "string"
    },
    "minItems": 1,
    "type": "array"
},
"wc": {
    "description": "A wildcard matching policy.",
    "pattern": "^\[+-*\]$",
    "type": "string"
}
},
"subject": {
    "anyOf": [
        {
            "description": "Device identifier.",
            "properties": {
                "uuid": {
                    "description": "A UUID Device ID
Format pattern according to IETF RFC 4122.",
                    "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$",
                    "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": "object"
        }
    ]
},
"type": "object"
"type": "object",
"required": [
  "aceid",
  "resources",
  "permission",
  "subject"
],
"type": "object",
"items": {
  "type": "string"
},
"type": "array"
],
"required": [
  "period"
],
"type": "string"
},
"type": "array"
],
"required": ["aceid",
  "resources",
  "permission",
  "subject"
],
"type": "object",
"signature": {
  "description": "The signature over the ACL Resource:\nEncoded signature data.\n",
  "properties": {
    "sigtype": {
      "description": "The string specifies the predefined signature format.\n",
      "x-detail-desc": ["RFC7515 JSON web signature (JWS) object.\n",
        "RFC2315 base64 encoded object.\n",
        "CBOR encoded JWS object."
      ],
      "enum": ["oic.sec.sigtype.jws",
        "oic.sec.sigtype.pk7"
      ]
    }
  }
}
C.12.5 Property definition

Table C.22 defines the Properties that are part of the "oic.r.sacl" Resource Type.

Table C.22 – The Property definitions of the Resource with type "rt" = "oic.r.sacl".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>signature</td>
<td>object: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>The signature over the ACL Resource Encoded signature data.</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>aclist2</td>
<td>array: see schema</td>
<td>Yes</td>
<td>Read Write</td>
<td>Access Control Entries in the ACL Resource.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
</tbody>
</table>

C.12.6 CRUDN behaviour

Table C.23 defines the CRUDN operations that are supported on the "oic.r.sacl" Resource Type.
Table C.23 – The CRUDN operations of the Resource with type "rt" = "oic.r.sacl".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>put</td>
<td>get</td>
<td>post</td>
<td>delete</td>
<td>observe</td>
</tr>
</tbody>
</table>

C.13 Session

C.13.1 Introduction

Resource that manages the persistent session between a Device and OCF Cloud.

C.13.2 Well-known URI

/oic/sec/session

C.13.3 Resource type

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

C.13.4 OpenAPI 2.0 definition

```json
{
   "swagger": "2.0",
   "info": {
      "title": "Session",
      "version": "v1.0-20181001",
      "license": {
         "name": "OCF Data Model License",
         "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbc8dbd4ba/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/session" : {
         "post": {
            "description": "Resource that manages the persistent session between a Device and OCF Cloud.",
            "parameters": [
               {"$ref": "/#/parameters/interface"},
               {
                  "name": "body",
                  "in": "body",
                  "required": true,
                  "schema": { "$ref": "/#/definitions/Account-Session-Request" },
                  "x-example": {
                     "uid" : "123e4567-e89b-12d3-a456-d6e39e4b6e55",
                     "di" : "9cfbe8e-5a1e-4d1c-9d01-00c04fd430c8",
                     "accesstoken" : "0f3d9f7fe5491d54077d",
                     "login" : true
                  }
               }
            ],
            "responses": {
               "204": {
                  "description": "",
                  "x-example": {
                     "rt" : ["oic.r.session"],
                     "expiresin" : 3600
                  }
               },
               "schema": { "$ref": "/#/definitions/Account-Session-Response" }
            }
         }
      }
   }
}
```
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "Account-Session-Request": {
    "properties": {
      "uid": {
        "description": "Format pattern according to IETF RFC 4122.",
        "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}\$",
        "type": "string"
      },
      "di": {
        "description": "The Device ID
Format pattern according to IETF RFC 4122.",
        "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}\$",
        "type": "string"
      },
      "accesstoken": {
        "description": "Access-Token used to grant access right for the Device to sign-in.",
        "pattern": "^[?!$|\s+]$.+",
        "type": "string"
      },
      "login": {
        "description": "Action for the request: true = login, false = logout.",
        "type": "boolean"
      }
    },
    "type": "object",
    "required": ["uid", "di", "accesstoken", "login"]
  },
  "Account-Session-Response": {
    "properties": {
      "expiresin": {
        "description": "Access-Token remaining life time in seconds (-1 if permanent)",
        "readOnly": true,
        "type": "integer"
      },
      "rt": {
        "description": "Resource Type of the Resource.",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.session"]
        },
        "minItems": 1,
        "readOnly": true,
        "type": "array"
      },
      "n": {
        "$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"
        }
      }
    }
  }
}
C.13.5 Property definition

Table C.24 defines the Properties that are part of the "oic.r.session" Resource Type.

**Table C.24 – The Property definitions of the Resource with type "rt" = "oic.r.session".**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>expiresin</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td>Access-Token remaining life time in seconds (-1 if permanent).</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>di</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>The Device ID Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>accesstoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Access-Token used to grant access right for the Device to sign-in.</td>
</tr>
<tr>
<td>uid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>login</td>
<td>boolean</td>
<td>Yes</td>
<td>Read Write</td>
<td>Action for the request: true = login, false = logout.</td>
</tr>
</tbody>
</table>

C.13.6 CRUDN behaviour

Table C.25 defines the CRUDN operations that are supported on the "oic.r.session" Resource Type.

**Table C.25 – The CRUDN operations of the Resource with type "rt" = "oic.r.session".**

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>post</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
C.14 Security Profile

C.14.1 Introduction

Resource specifying supported and active security profile(s).

C.14.2 Well-known URI

/oic/sec/sp

C.14.3 Resource type

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

C.14.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Security Profile",
    "version": "v1.0-20190208",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4cfbce8bdc4ba/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/sp": {
      "get": {
        "description": "Resource specifying supported and active security profile(s).\n",
        "parameters": [
          {
            "$ref": "#/parameters/interface"
          }
        ],
        "responses": {
          "200": {
            "description": "",
            "x-example":
            {
              "rt": ["oic.r.sp"],
              "supportedprofiles": ["1.3.6.1.4.1.51414.0.0.1.0", "1.3.6.1.4.1.51414.0.0.2.0"],
              "currentprofile": "1.3.6.1.4.1.51414.0.0.1.0"
            }
          },
          "400": {
            "description": "The request is invalid."
          }
        }
      },
      "post": {
        "description": "Sets or updates Device provisioning status data.\n",
        "parameters": [
          {
            "$ref": "#/parameters/interface"
          },
          {
            "name": "body",
            "in": "body",
            "required": true,
            "schema": {
              "$ref": "#/definitions/SP-Update"
            }
          }
        ],
        "responses": {
          "200": {
            "description": "",
            "x-example":
            {
              "supportedprofiles": ["1.3.6.1.4.1.51414.0.0.1.0", "1.3.6.1.4.1.51414.0.0.2.0"],
              "currentprofile": "1.3.6.1.4.1.51414.0.0.1.0"
            }
          }
        }
      }
    }
  }
}
```
"responses": {
  "200": {
    "description": "",
    "x-example": {
      "rt": ["oic.r.sp"],
      "supportedprofiles": ["1.3.6.1.4.1.151414.0.0.1.0", "1.3.6.1.4.1.151414.0.0.2.0"],
      "currentprofile": "1.3.6.1.4.1.151414.0.0.1.0"
    },
    "schema": { "$ref": "#/definitions/SP" }
  },
  "400": {
    "description": "The request is invalid."
  }
}

"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
}

"definitions": {
  "SP": {
    "properties": {
      "rt": {
        "description": "Resource Type of the Resource.",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.sp"]
        },
        "minItems": 1,
        "readOnly": true,
        "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"
      },
      "currentprofile": {
        "description": "Security Profile currently active.",
        "type": "string"
      },
      "supportedprofiles": {
        "description": "Array of supported Security Profiles.",
        "items": {
          "type": "string"
        },
        "type": "array"
      },
      "if": {
        "description": "The interface set supported by this Resource.",
        "items": {
          "enum": ["oic.if.baseline"
        },
        "type": "string"


C.14.5 Property definition

Table C.26 defines the Properties that are part of the "oic.r.sp" Resource Type.

Table C.26 – The Property definitions of the Resource with type "rt" = "oic.r.sp".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>supportedprofiles</td>
<td>array: see schema</td>
<td></td>
<td>Read Write</td>
<td>Array of supported Security Profiles.</td>
</tr>
<tr>
<td>currentprofile</td>
<td>string</td>
<td></td>
<td>Read Write</td>
<td>Security Profile currently active.</td>
</tr>
<tr>
<td>id</td>
<td>multiple types:</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td></td>
<td>see schema</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>multiple types:</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td></td>
<td>see schema</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>currentprofile</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Security Profile currently active.</td>
</tr>
<tr>
<td>supportedprofiles</td>
<td>array: see schema</td>
<td></td>
<td>Read Write</td>
<td>Array of supported Security Profiles.</td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
</tbody>
</table>

C.14.6 CRUDN behaviour

Table C.27 defines the CRUDN operations that are supported on the "oic.r.sp" Resource Type.

Table C.27 – The CRUDN operations of the Resource with type "rt" = "oic.r.sp".

<table>
<thead>
<tr>
<th>Create</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>post</td>
<td></td>
<td></td>
<td>observe</td>
</tr>
</tbody>
</table>
C.15 Token Refresh

C.15.1 Introduction
Obtain fresh access-token using the refresh token, client should refresh access-token before it expires.

C.15.2 Well-known URI
/oic/sec/tokenrefresh

C.15.3 Resource type
The Resource Type is defined as: "oic.r.tokenrefresh".

C.15.4 OpenAPI 2.0 definition

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Token Refresh",
    "version": "v1.0-20181001",
    "license": {
      "name": "OCF Data Model License",
      "url": "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbc8bdc4ba/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/tokenrefresh": {
      "post": {
        "description": "Obtain fresh access-token using the refresh token, client should refresh access-token before it expires."
      },
      "parameters": [
        { "$ref": "/parameters/interface" },
        {
          "name": "body",
          "in": "body",
          "required": true,
          "schema": { "$ref": "/definitions/TokenRefresh-Request" },
          "x-example": {
            "uid": "123e4567-e89b-12d3-a456-d6e313b71d8f",
            "di": "9cfb2b8e-3e5e-4d1c-9d01-00c4d434c8",
            "refresh_token": "00f40464afbe532464c"
          }
        }
      ],
      "responses": {
        "204": {
          "description": "2.04 Changed respond with new access-token."
        }
      }
    }
  }
}
```

Copyright Open Connectivity Foundation, Inc. © 2016-2019. All rights Reserved
"parameters": {
  "interface": {
    "in": "query",
    "name": "if",
    "type": "string",
    "enum": ["oic.if.baseline"]
  }
},
"definitions": {
  "TokenRefresh-Request": {
    "properties": {
      "refreshToken": {
        "description": "Refresh token received by account management or during token refresh procedure.",
        "pattern": "(?![\s]+$).*",
        "type": "string"
      },
      "uid": {
        "description": "Format pattern according to IETF RFC 4122.",
        "pattern": "^[a-zA-F0-9]{8}-[a-zA-F0-9]{4}-[a-zA-F0-9]{4}-[a-zA-F0-9]{4}-[a-zA-F0-9]{12}$/",
        "type": "string"
      },
      "di": {
        "description": "Format pattern according to IETF RFC 4122.",
        "pattern": "^[a-zA-F0-9]{8}-[a-zA-F0-9]{4}-[a-zA-F0-9]{4}-[a-zA-F0-9]{4}-[a-zA-F0-9]{12}$/",
        "type": "string"
      }
    },
    "type": "object",
    "required": ["uid", "di", "refreshToken"]
  },
  "TokenRefresh-Response": {
    "properties": {
      "expiresIn": {
        "description": "Access-Token life time in seconds (-1 if permanent).",
        "readOnly": true,
        "type": "integer"
      },
      "rt": {
        "description": "Resource Type of the Resource.",
        "items": {
          "maxLength": 64,
          "type": "string",
          "enum": ["oic.r.tokenrefresh"]
        },
        "minItems": 1,
        "readOnly": true,
        "type": "array"
      },
      "refreshToken": {
        "description": "Refresh token received by account management or during token refresh procedure.",
        "pattern": "(?![\s]+$).*",
        "type": "string"
      },
      "accesstoken": {
        "description": "Granted Access-Token.",
        "pattern": "(?![\s]+$).*",
        "readOnly": true,
        "type": "string"
      },
      "n": {
        "$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"
      }
    }
  }
}
C.15.5 Property definition

Table C.28 defines the Properties that are part of the "oic.r.tokenrefresh" Resource Type.

Table C.28 – The Property definitions of the Resource with type "rt" = "oic.r.tokenrefresh".

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value type</th>
<th>Mandatory</th>
<th>Access mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>refreshtoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Refresh token received by account management or during token refresh procedure.</td>
</tr>
<tr>
<td>uid</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>di</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Format pattern according to IETF RFC 4122.</td>
</tr>
<tr>
<td>if</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>The interface set supported by this Resource.</td>
</tr>
<tr>
<td>expiresin</td>
<td>integer</td>
<td>Yes</td>
<td>Read Only</td>
<td>Access-Token life time in seconds (-1 if permanent).</td>
</tr>
<tr>
<td>accesstoken</td>
<td>string</td>
<td>Yes</td>
<td>Read Only</td>
<td>Granted Access-Token.</td>
</tr>
<tr>
<td>refresh</td>
<td>string</td>
<td>Yes</td>
<td>Read Write</td>
<td>Refresh token received by account management or during token refresh procedure.</td>
</tr>
<tr>
<td>n</td>
<td>multiple types: see schema</td>
<td>No</td>
<td>Read Write</td>
<td></td>
</tr>
<tr>
<td>rt</td>
<td>array: see schema</td>
<td>No</td>
<td>Read Only</td>
<td>Resource Type of the Resource.</td>
</tr>
</tbody>
</table>
### C.15.6 CRUDN behaviour

Table C.29 defines the CRUDN operations that are supported on the "oic.r.tokenrefresh" Resource Type.

**Table C.29 – The CRUDN operations of the Resource with type "rt" = "oic.r.tokenrefresh".**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Read</th>
<th>Update</th>
<th>Delete</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>post</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>id</th>
<th>multiple types:</th>
<th>No</th>
<th>Read Write</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>see schema</td>
<td>No</td>
<td>Read Write</td>
</tr>
</tbody>
</table>
Annex D
(informative)

OID definitions

This annex captures the OIDs defined throughout the document. The OIDs listed are intended to be used within the context of an X.509 v3 certificate. MAX is an upper bound for SEQUENCES of UTF8Strings and OBJECT IDENTIFIERS and should not exceed 255.

```
id-OCF OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1)
                      private(4) enterprise(1) OCF(51414) }

-- OCF Security specific OIDs

id-ocfSecurity OBJECT IDENTIFIER ::= { id-OCF 0 }
id-ocfX509Extensions OBJECT IDENTIFIER ::= { id-OCF 1 }

-- OCF Security Categories

id-ocfSecurityProfile ::= { id-ocfSecurity 0 }
id-ocfCertificatePolicy ::= { id-ocfSecurity 1 }

-- OCF Security Profiles

sp-unspecified ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 0 }
sp-baseline ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 1 }
sp-black ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 2 }
sp-blue ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 3 }
sp-purple ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 4 }
sp-unspecified-v0 ::= ocfSecurityProfileOID {id-sp-unspecified 0}
sp-baseline-v0 ::= ocfSecurityProfileOID {id-sp-baseline 0}
sp-black-v0 ::= ocfSecurityProfileOID {id-sp-black 0}
sp-blue-v0 ::= ocfSecurityProfileOID {id-sp-blue 0}
sp-purple-v0 ::= ocfSecurityProfileOID {id-sp-purple 0}

ocfSecurityProfileOID ::= UTF8String

-- OCF Security Certificate Policies

ocfCertificatePolicy-v1 ::= { id-ocfCertificatePolicy 2}

-- OCF X.509v3 Extensions

ocfVersion ::= SEQUENCE { major INTEGER, minor INTEGER, build INTEGER }

ocfCompliance ::= SEQUENCE { version ocfVersion, securityProfileSEQUENCE SIZE (1..MAX) OF ocfSecurityProfileOID, 
deviceName UTF8String, deviceManufacturer UTF8String }

claim-secure-boot ::= ocfSecurityClaimsOID { id-ocfSecurityClaims 0 }
```
claim-hw-backed-cred-storage ::= ocfSecurityClaimsOID { id-ocfSecurityClaims 1 }

ocfSecurityClaimsOID ::= OBJECT IDENTIFIER

ocfSecurityClaims ::= SEQUENCE SIZE (1..MAX) of ocfSecurityClaimsOID

cpl-at-IANAPen ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 0 }
cpl-at-model ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 1 }
cpl-at-version ::= OBJECT IDENTIFIER { id-ocfCPLAttributes 2 }

ocfCPLAttributes ::= SEQUENCE {
cpl-at-IANAPen UTF8String,
cpl-at-model UTF8String,
cpl-at-version UTF8String}
Annex E
(informative)

Security considerations specific to Bridged Protocols

The text in this Annex is provided for information only. This Annex has no normative impact. This information is applicable at the time of initial publication and may become out of date.

E.1 Security Considerations specific to the AllJoyn Protocol

This clause intentionally left empty.

E.2 Security Considerations specific to the Bluetooth LE Protocol

BLE GAP supports two security modes, security mode 1 and security mode 2. Each security mode has several security levels (see Table E.1)

Security mode 1 and Security level 2 or higher would typically be considered secure from an OCF perspective. The appropriate selection of security mode and level is left to the vendor.

Table E.1 GAP security mode

<table>
<thead>
<tr>
<th>GAP security mode</th>
<th>security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security mode 1</td>
<td>1 (no security)</td>
</tr>
<tr>
<td></td>
<td>2 (Unauthenticated pairing with encryption)</td>
</tr>
<tr>
<td></td>
<td>3 (Authenticated pairing with encryption)</td>
</tr>
<tr>
<td></td>
<td>4 (Authenticated LE Secure Connections pairing with encryption)</td>
</tr>
<tr>
<td>Security mode 2</td>
<td>1 (Unauthenticated pairing with data signing)</td>
</tr>
<tr>
<td></td>
<td>2 (Authenticated pairing with data signing)</td>
</tr>
</tbody>
</table>

Figure E-1 shows how communications in both ecosystems of OCF-BLE Bridge Platform are secured by their own security.

Figure E-1 Security Considerations for BLE Bridge

E.3 Security Considerations specific to the oneM2M Protocol

This clause intentionally left empty.
E.4 Security Considerations specific to the U+ Protocol

A U+ server supports one of the TLS 1.2 cipher suites as in Table E.2 defined in IETF RFC 5246.

**Table E.2 TLS 1.2 Cipher Suites used by U+**

<table>
<thead>
<tr>
<th>Cipher Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CCM</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CCM_8</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CCM</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
</tbody>
</table>

The security of the Haier U+ Protocol is proprietary, and further details are presently unavailable.

E.5 Security Considerations specific to the Z-Wave Protocol

Z-Wave currently supports two kinds of security class which are S0 Security Class and S2 Security Class, as shown in Table E.3. Bridged Z-wave Servers using S2 Security Class for communication with a Virtual Bridged Client would typically be considered secure from an OCF perspective. The appropriate selection for S2 Security Class and Class Name is left to the vendor.

Figure E-2 presents how OCF Client and Bridged Z-Wave Server communicate based upon their own security.
Figure E-2 Security Considerations for Z-Wave Bridge

All 3 types of S2 Security Class such as S2 Access Control, S2 Authenticated and S2 Unauthenticated provides the following advantages from the security perspective;

- The unique device specific key for every secure device enables validation of device identity and prevents man-in-the-middle compromises to security
- The Secure cryptographic key exchange methods during inclusion achieves high level of security between the Virtual Z-Wave Client and the Bridged Z-Wave Server.
- Out of band key exchange for product authentication which is combined with device specific key prevents eavesdropping and man-in-the-middle attack vectors.

See Table E.3 for a summary of Z-Wave Security Classes.

Table E.3 Z-Wave Security Class

<table>
<thead>
<tr>
<th>Security Class</th>
<th>Class Name</th>
<th>Validation of device identity</th>
<th>Key Exchange</th>
<th>Message Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2</td>
<td>S2 Access Control</td>
<td>Device Specific key</td>
<td>Out-of-band inclusion</td>
<td>Encrypted command transmission</td>
</tr>
<tr>
<td>S2</td>
<td>S2 Authenticated</td>
<td>Device Specific key</td>
<td>Out-of-band inclusion</td>
<td>Encrypted command transmission</td>
</tr>
<tr>
<td>S2</td>
<td>S2 Unauthenticated</td>
<td>Device Specific key</td>
<td>Z-wave RF band used for inclusion</td>
<td>Encrypted command transmission</td>
</tr>
<tr>
<td>S0</td>
<td>S0 Authenticated</td>
<td>N/A</td>
<td>Z-wave RF band used for inclusion</td>
<td>Encrypted command transmission</td>
</tr>
</tbody>
</table>

On the other hand, S0 Security Class has the vulnerability of security during inclusion by exchanging of temporary ‘well-known key’ (e.g. 1234). As a result of that, it could lead the disclosure of the network key if the log of key exchange methods is captured, so Z-Wave devices might be no longer secure in that case.

E.6 Security Considerations specific to the Zigbee Protocol

The Zigbee 3.0 stack supports multiple security levels. A security level is supported by both the network (NWK) layer and application support (APS) layer. A security attribute in the Zigbee 3.0 stack, "nwkSecurityLevel", represents the security level of a device.
The security level `nwkSecurityLevel > 0x04` provides message integrity code (MIC) and/or AES128-CCM encryption (ENC). Zigbee Servers using `nwkSecurityLevel > 0x04` would typically be considered secure from an OCF perspective. The appropriate selection for `nwkSecurityLevel` is left to the vendor.

See Table E.4 for a summary of the Zigbee Security Levels.

**Table E.4 Zigbee 3.0 Security Levels to the Network, and Application Support layers**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Security Level Sub-Field</th>
<th>Security Attributes</th>
<th>Data Encryption</th>
<th>Frame Integrity (Length of M of MIC, in Number of Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>'000'</td>
<td>None</td>
<td>OFF</td>
<td>NO (M=0)</td>
</tr>
<tr>
<td>0x01</td>
<td>'001'</td>
<td>MIC-32</td>
<td>OFF</td>
<td>YES (M=4)</td>
</tr>
<tr>
<td>0x02</td>
<td>'010'</td>
<td>MIC-64</td>
<td>OFF</td>
<td>YES (M=8)</td>
</tr>
<tr>
<td>0x03</td>
<td>'011'</td>
<td>MIC-128</td>
<td>OFF</td>
<td>YES (M=16)</td>
</tr>
<tr>
<td>0x04</td>
<td>'100'</td>
<td>ENC</td>
<td>ON</td>
<td>NO (M=0)</td>
</tr>
<tr>
<td>0x05</td>
<td>'101'</td>
<td>ENC-MIC-32</td>
<td>ON</td>
<td>YES (M=4)</td>
</tr>
<tr>
<td>0x06</td>
<td>'110'</td>
<td>ENC-MIC-64</td>
<td>ON</td>
<td>YES (M=8)</td>
</tr>
<tr>
<td>0x07</td>
<td>'111'</td>
<td>ENC-MIC-128</td>
<td>ON</td>
<td>YES (M=16)</td>
</tr>
</tbody>
</table>

Figure E-3 shows how communications in both ecosystems of OCF-Zigbee Bridge Platform are secured by their own security.

**Figure E-3 Security Considerations for Zigbee Bridge**