

OCF Cloud Security Specification

VERSION 2.2.3 | February 2021



OPEN CONNECTIVITY
FOUNDATION™

CONTACT admin@openconnectivity.org
Copyright Open Connectivity Foundation, Inc. © 2021.
All Rights Reserved.

LEGAL DISCLAIMER

1
2 NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND
3 OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY
4 INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY ANY OF THE AUTHORS OR
5 DEVELOPERS OF THIS DOCUMENT. THE INFORMATION CONTAINED HEREIN IS PROVIDED
6 ON AN "AS IS" BASIS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW,
7 THE AUTHORS AND DEVELOPERS OF THIS DOCUMENT HEREBY DISCLAIM ALL OTHER
8 WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT
9 COMMON LAW, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF
10 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OPEN INTERCONNECT
11 CONSORTIUM, INC. FURTHER DISCLAIMS ANY AND ALL WARRANTIES OF NON-
12 INFRINGEMENT, ACCURACY OR LACK OF VIRUSES.

13 The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other
14 countries. *Other names and brands may be claimed as the property of others.

15 Copyright © 2019-2021 Open Connectivity Foundation, Inc. All rights reserved.

16 Copying or other form of reproduction and/or distribution of these works are strictly prohibited

CONTENTS

17		
18		
19	Introduction	vi
20	Scope.....	1
21	Normative References	1
22	Terms, definitions, and abbreviated terms	1
23	3.1 Terms and definitions	1
24	3.2 Abbreviated terms	2
25	Document Conventions and Organization	2
26	4.1 Conventions.....	2
27	4.2 Notation.....	2
28	4.3 Data types	3
29	Security overview	4
30	5.1 Preamble	4
31	5.2 Device Provisioning for OCF Cloud and Device Registration Overview	4
32	5.3 Credential overview.....	4
33	Device provisioning for OCF Cloud.....	4
34	6.1 Cloud Provisioning General	4
35	6.2 Device Provisioning by Mediator	5
36	Device authentication with OCF Cloud.....	7
37	7.1 Device Authentication with OCF Cloud General.....	7
38	7.2 Device Connection with the OCF Cloud	7
39	7.3 Security Considerations	9
40	Message integrity and confidentiality	9
41	8.1 Cloud Session Semantics	9
42	8.2 Cipher suites for OCF Cloud Credentials	9
43	Security Resources.....	9
44	9.1 Account Resource	9
45	9.2 Account Session Resource	11
46	9.3 Account Token Refresh Resource.....	12
47	Security hardening guidelines	13
48	10.1 Security hardening guidelines general	13
49	Annex A (normative) Resource Type definitions.....	14
50	A.1 List of Resource Type definitions	14
51	A.2 Account Token	14
52	A.2.1 Introduction.....	14
53	A.2.2 Well-known URI	14
54	A.2.3 Resource type.....	14
55	A.2.4 OpenAPI 2.0 definition	14
56	A.2.5 Property definition.....	17
57	A.2.6 CRUDN behaviour.....	18
58	A.3 Session.....	18
59	A.3.1 Introduction.....	18
60	A.3.2 Well-known URI	18

61	A.3.3	Resource type.....	18
62	A.3.4	OpenAPI 2.0 definition	18
63	A.3.5	Property definition.....	20
64	A.3.6	CRUDN behaviour.....	21
65	A.4	Token Refresh	21
66	A.4.1	Introduction.....	21
67	A.4.2	Well-known URI	21
68	A.4.3	Resource type.....	22
69	A.4.4	OpenAPI 2.0 definition	22
70	A.4.5	Property definition.....	24
71	A.4.6	CRUDN behaviour.....	25
72			

FIGURES

73	
74	Figure 1 – User authorization and provisioning using Authorization Code Grant Flow5
75	Figure 2 – Device Provisioning using Authorization Code Grant Flow6
76	Figure 3 – Device connection with OCF Cloud8
77	

Tables

78	
79	Table 1 – Mapping of Properties of "oic.r.account" and "oic.r.coapcloudconf" Resources7
80	Table 2 – Device connection with the OCF Cloud flow8
81	Table 3 – Definition of the "oic.r.account" Resource.....10
82	Table 4 – Properties of the "oic.r.account" Resource11
83	Table 5 – Definition of the "oic.r.session" Resource12
84	Table 6 – Properties of the "oic.r.session" Resource.....12
85	Table 7 – Definition of the "oic.r.tokenrefresh" Resource13
86	Table 8 – Properties of the "oic.r.tokenrefresh" Resource13
87	Table 9 – Sensitive Data related to OCF Cloud.....13
88	Table A.1 – Alphabetized list of security Resources14
89	Table A.2 – The Property definitions of the Resource with type "rt" = "oic.r.account".17
90	Table A.3 – The CRUDN operations of the Resource with type "rt" = "oic.r.account".18
91	Table A.4 – The Property definitions of the Resource with type "rt" = "oic.r.session".....20
92	Table A.5 – The CRUDN operations of the Resource with type "rt" = "oic.r.session".21
93	Table A.6 – The Property definitions of the Resource with type "rt" = "oic.r.tokenrefresh".24
94	Table A.7 – The CRUDN operations of the Resource with type "rt" = "oic.r.tokenrefresh".....25
95	
96	
97	

Introduction

99 This document, and all the other parts associated with this document, were developed in response
100 to worldwide demand for smart home focused Internet of Things (IoT) devices, such as appliances,
101 door locks, security cameras, sensors, and actuators; these to be modelled and securely controlled,
102 locally and remotely, over an IP network.

103 While some inter-device communication existed, no universal language had been developed for
104 the IoT. Device makers instead had to choose between disparate frameworks, limiting their market
105 share, or developing across multiple ecosystems, increasing their costs. The burden then falls on
106 end users to determine whether the products they want are compatible with the ecosystem they
107 bought into, or find ways to integrate their devices into their network, and try to solve interoperability
108 issues on their own.

109 In addition to the smart home, IoT deployments in commercial environments are hampered by a
110 lack of security. This issue can be avoided by having a secure IoT communication framework, which
111 this standard solves.

112 The goal of these documents is then to connect the next 25 billion devices for the IoT, providing
113 secure and reliable device discovery and connectivity across multiple OSs and platforms. There
114 are multiple proposals and forums driving different approaches, but no single solution addresses
115 the majority of key requirements. This document and the associated parts enable industry
116 consolidation around a common, secure, interoperable approach.

117 **Scope**

118 This document defines security objectives, philosophy, Resources and mechanisms that impacts
119 OCF base layers of ISO/IEC 30118-1. ISO/IEC 30118-1 contains informative security content. The
120 OCF Security Document contains security normative content and may contain informative content
121 related to the OCF base or other OCF documents.

122 **Normative References**

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

126 ISO/IEC 30118-1 *Information technology – Open Connectivity Foundation (OCF) Document – Part*
127 *1: Core specification*
128 <https://www.iso.org/standard/53238.html>
129 Latest version available at:
130 https://openconnectivity.org/specs/OCF_Core_Specification.pdf

131 ISO/IEC 30118-2, *Information technology – Open Connectivity Foundation (OCF) Document –*
132 *Part 2: Security specification*
133 <https://www.iso.org/standard/74239.html>
134 Latest version available at: https://openconnectivity.org/specs/OCF_Security_Specification.pdf

135 ISO/IEC 30118-8, *Information technology – Open Connectivity Foundation (OCF) Document –*
136 *Part 8: Device to Cloud Services,*
137 <https://www.iso.org/standard/79360.html>
138 Latest version available at:
139 https://openconnectivity.org/specs/OCF_OCF_Device_To_Cloud_Services_Specification.pdf

140 IETF RFC 6749, *The OAuth 2.0 Authorization Framework*, October 2012,
141 <https://tools.ietf.org/html/rfc6749>

142 IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*, October 2012,
143 <https://tools.ietf.org/html/rfc6750>
144

145 IETF RFC 8323, *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets*,
146 February 2018, <https://tools.ietf.org/html/rfc8323>

147 oneM2M Release 3 Documents, <http://www.onem2m.org/technical/published-drafts>

148 OpenAPI document, aka *Swagger RESTful API Documentation Specification*, Version 2.0
149 <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md>

150 **Terms, definitions, and abbreviated terms**

151 **3.1 Terms and definitions**

152 For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1, ISO/IEC
153 30118-2, ISO/IEC 30118-8 and the following apply.

154 ISO and IEC maintain terminological databases for use in standardization at the following
155 addresses:

- 156 – ISO Online browsing platform: available at <https://www.iso.org/obp>
- 157 – IEC Electropedia: available at <http://www.electropedia.org/>

158 **3.1.1**
159 **Access Token**
160 credential used to authorize the connection with the OCF Cloud and access protected Resources

161 Note 1 to entry: An Access Token is a string while the OCF Device has no internal logic based on its contents and
162 only forwards the token as-is

163 **3.1.2**
164 **Authorization Provider**
165 server issuing Access Tokens (3.1.1) via a Mediator to the Client after successfully authenticating
166 the *OCF Cloud User* (3.1.4) and obtaining authorization

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

168 **3.1.3**
169 **Device Registration**
170 process by which Device is enrolled/registered to the OCF Cloud infrastructure (using Device
171 certificate and unique credential) and becomes ready for further remote operation through the cloud
172 interface (e.g. connection to remote Resources or publishing of its own Resources for access)

173 **3.1.4**
174 **OCF Cloud User**
175 person or organization authorizing a set of Devices to interact with each other via an OCF Cloud

176 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
177 organization that onboarded that Device. The OCF Cloud User delegates, to the OCF Cloud authority, authority to route
178 between Devices registered by the OCF Cloud User. The OCF Cloud delegates, to the OCF Cloud User, authority to
179 select the set of Devices which can register and use the services of the OCF Cloud.

180 **3.2 Abbreviated terms**

181 For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 30118-1,
182 ISO/IEC 30118-2 and ISO/IEC 30118-8 apply.

183 **Document Conventions and Organization**

184 **4.1 Conventions**

185 In this document a number of terms, conditions, mechanisms, sequences, parameters, events,
186 states, or similar terms are printed with the first letter of each word in uppercase and the rest
187 lowercase (e.g., Network Architecture). Any lowercase uses of these words have the normal
188 technical English meaning.

189 In this document, to be consistent with the IETF usages for RESTful operations, the RESTful
190 operation words CRUDN, CREATE, RETRIVE, UPDATE, DELETE, and NOTIFY will have all letters
191 capitalized. Any lowercase uses of these words have the normal technical English meaning.

192 **4.2 Notation**

193 In this document, features are described as required, recommended, allowed or DEPRECATED as
194 follows:

195 Required (or shall or mandatory)(M).

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

199 Recommended (or should)(S).

200 – These features add functionality supported by Core Architecture and should be implemented.
201 Recommended features take advantage of the capabilities Core Architecture, usually without
202 imposing major increase of complexity. Notice that for compliance testing, if a recommended
203 feature is implemented, it shall meet the specified requirements to be in compliance with these

204 guidelines. Some recommended features could become requirements in the future. The phrase
205 "should not" indicates behaviour that is permitted but not recommended.

206 Allowed (may or allowed)(O).

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

210 DEPRECATED.

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

217 Conditionally allowed (CA).

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

220 Conditionally required (CR).

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

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

225 Words that are emphasized are printed in italic.

226 In all of the Property and Resource definition tables that are included throughout this document the
227 "Mandatory" column indicates that the item detailed is mandatory to implement; the mandating of
228 inclusion of the item in a Resource Payload associated with a CRUDN action is dependent on the
229 applicable schema for that action.

230 **4.3 Data types**

231 Resources are defined using data types derived from JSON values as defined in clause 4.3 in
232 ISO/IEC 30118-1

233 **Security overview**

234 **5.1 Preamble**

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

- 237 – Device and Mediator connect over DTLS using "/oic/sec/cred"
- 238 – Device is provisioned by Mediator with following information:
 - 239 – the URL of OCF Cloud
 - 240 – Authorization Provider Name to identify the origin of the Access Token
 - 241 – Access Token / Authorization Code that is validated / exchanged by the OCF Cloud
 - 242 – UUID of the OCF Cloud

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

246 **5.2 Device Provisioning for OCF Cloud and Device Registration Overview**

247 As mentioned in the start of Clause 0, communication between a Device and OCF Cloud is subject
248 to different criteria in comparison to Devices which are within a single local network. The Device is
249 configured in order to connect to the OCF Cloud by a Mediator as specified in the CoAPCloudConf
250 Resource clauses in ISO/IEC 30118-8. Provisioning includes the remote connectivity and local
251 details such as URL where the OCF Cloud hosting environment can be found, the OCF Cloud
252 verifiable Access Token and optionally the name of the Authorization Provider which issued the
253 Access Token.

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

255 **5.3 Credential overview**

256 Devices may use credentials to prove the identity and role(s) of the parties in bidirectional
257 communication

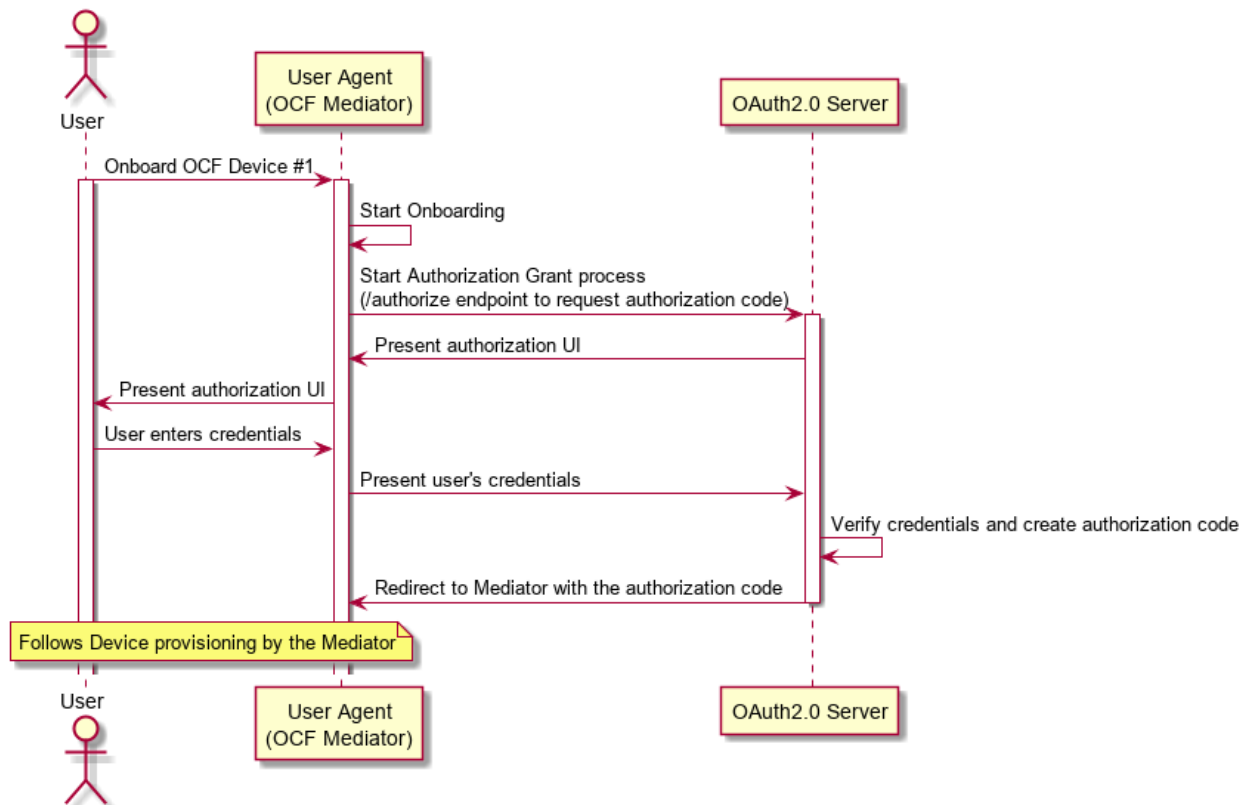
258 Access Tokens are provided to an OCF Cloud once an authenticated session with an OCF Cloud
259 is established, to verify the User ID with which the Device is to be associated.

260 **Device provisioning for OCF Cloud**

261 **6.1 Cloud Provisioning General**

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

265 The OCF Cloud is expected to use a secure mechanism for associating a Mediator with an OCF
266 Cloud User. The choice of mechanism is up to the OCF Cloud. Recommended solution is based on
267 the OAuth2.0 Authorization Grant Type flow specified in IETF RFC 6749, where the Mediator act
268 as a User-Agent and presents authorization UI to the user - see Figure 1. OCF Cloud is expected
269 to ensure that the suitable authentication mechanism is used to authenticate the OCF Cloud User.



270

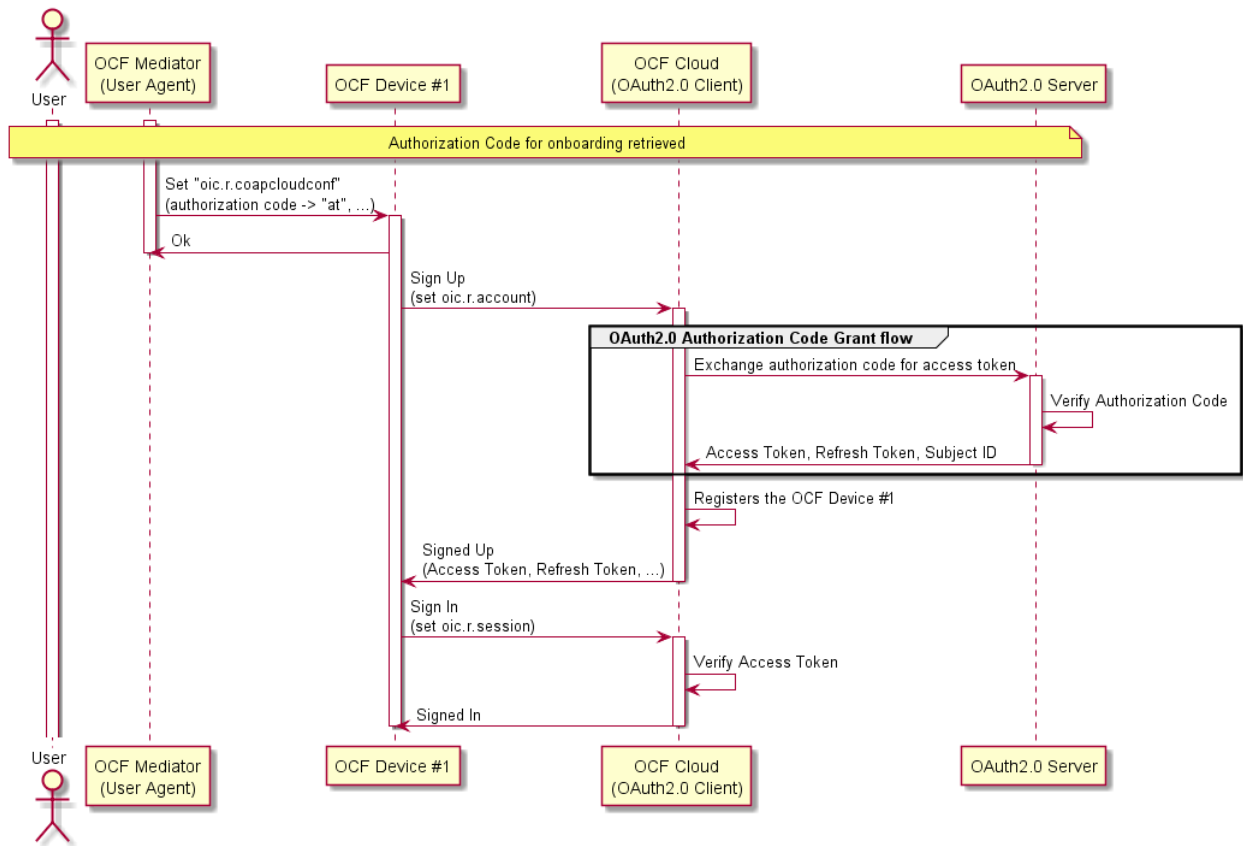
271 **Figure 1 – User authorization and provisioning using Authorization Code Grant Flow**

272 **6.2 Device Provisioning by Mediator**

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

275 The Mediator obtains an Authorization Code or directly an Access Token from the Authorization
 276 Server as described in ISO/IEC 30118-8. This value is then used by the Device for registering with
 277 the OCF Cloud as described in clause 0. At the time of Device Registration OCF Cloud exchanges
 278 the Authorization Code for the Access Token, returns it back to the OCF Device and associates
 279 the TLS session with corresponding Device UUID. The OCF Cloud maintains a map where Access
 280 Token and Mediator provided Device UUID are stored.

281 The Mediator provisions the Device, as described in ISO/IEC 30118-8. The Mediator provisions
 282 OCF Cloud URI to the "cis" Property of "oic.r.coapcloudconf" Resource, OCF Cloud UUID to the
 283 "sid" Property of "oic.r.coapcloudconf" Resource and per-Device Access Token or Authorization
 284 Code to the "at" Property of "oic.r.coapcloudconf" Resource on Device. Exchanged and returned
 285 provisioned Access Token is to be treated by Device as an Access Token with "Bearer" token type
 286 as defined in IETF RFC 6750. The provisioned "at" value follows a proprietary data format, and
 287 may include multiple values marshalled/concatenated together into a single string (e.g.
 288 "{\"token\": \"abc\", \"client_id\": \"1234\", \"idp\": \"identityProvider1\"}" is a valid "at" Property value).
 289 See Figure 2 for the detailed overview of the recommended flow, which includes optional OAuth
 290 2.0 Authorization Code Grant



291

292

Figure 2 – Device Provisioning using Authorization Code Grant Flow

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

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

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

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

307 The Mediator should provision the "oic.r.coapcloudconf" Resource with the Properties in Table 1.
 308 These details once provisioned are used by the Device to perform Device Registration to the OCF
 309 Cloud. OCF Device is not expected to have any internal logic based on the values of "at" and "apn"
 310 Properties. The values of these Properties are forwarded as-is to the OCF Cloud. After the initial
 311 registration, the Device should use updated values received from the OCF Cloud instead. If OCF
 312 Cloud User wants the Device to re-register with the OCF Cloud, they can use the Mediator to re-
 313 provision the "oic.r.coapcloudconf" Resource with the new values.

314 **Table 1 – Mapping of Properties of "oic.r.account" and "oic.r.coapcloudconf" Resources**

Property Title	oic.r.coapcloudconf	oic.r.account	Description
Authorization Provider Name	apn	authprovider	The name of Authorization Provider through which Access Token was obtained.
OCF Cloud URL	cis	-	This is the URL connection is established between Device and OCF Cloud.
Access Token	at	accesstoken	Access Token used to authorize the TLS connection for communication with the OCF Cloud, or the Authorization Code which is then verified and exchanged for the Access Token during Device Registration.
OCF Cloud UUID	sid	-	This is the identity of the OCF Cloud that the Device is configured to use.

315 **Device authentication with OCF Cloud**

316 **7.1 Device Authentication with OCF Cloud General**

317 The mechanisms for Device Authentication in clauses 10.2, 10.3 and 10.4 of ISO/IEC 30118-2
 318 imply that a Device is authorized to communicate with any other Device meeting the criteria
 319 provisioned in "/oic/sec/cred"; the "/oic/sec/acl2" Resource (or "/oic/sec/acl1" Resource of OIC1.1
 320 Servers) are additionally used to restrict access to specific Resources. The present clause
 321 describes Device authentication for OCF Cloud, which uses slightly different criteria as described
 322 in ISO/IEC 30118-2. A Device accessing an OCF Cloud shall establish a TLS session. The mutual
 323 authenticated TLS session is established using Server certificate and Client certificate.

324 Each Device is identified by the Access Token obtained from the Device Registration response.
 325 The OCF Cloud holds an OCF Cloud association table that maps Access Token, User ID and Device
 326 UUID. The Device Registration shall happen while the Device is in RFNOP state. After Device
 327 Registration, the updated Access Token, Device UUID and User ID are used by the Device for the
 328 subsequent connection with the OCF Cloud.

329 **7.2 Device Connection with the OCF Cloud**

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

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

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

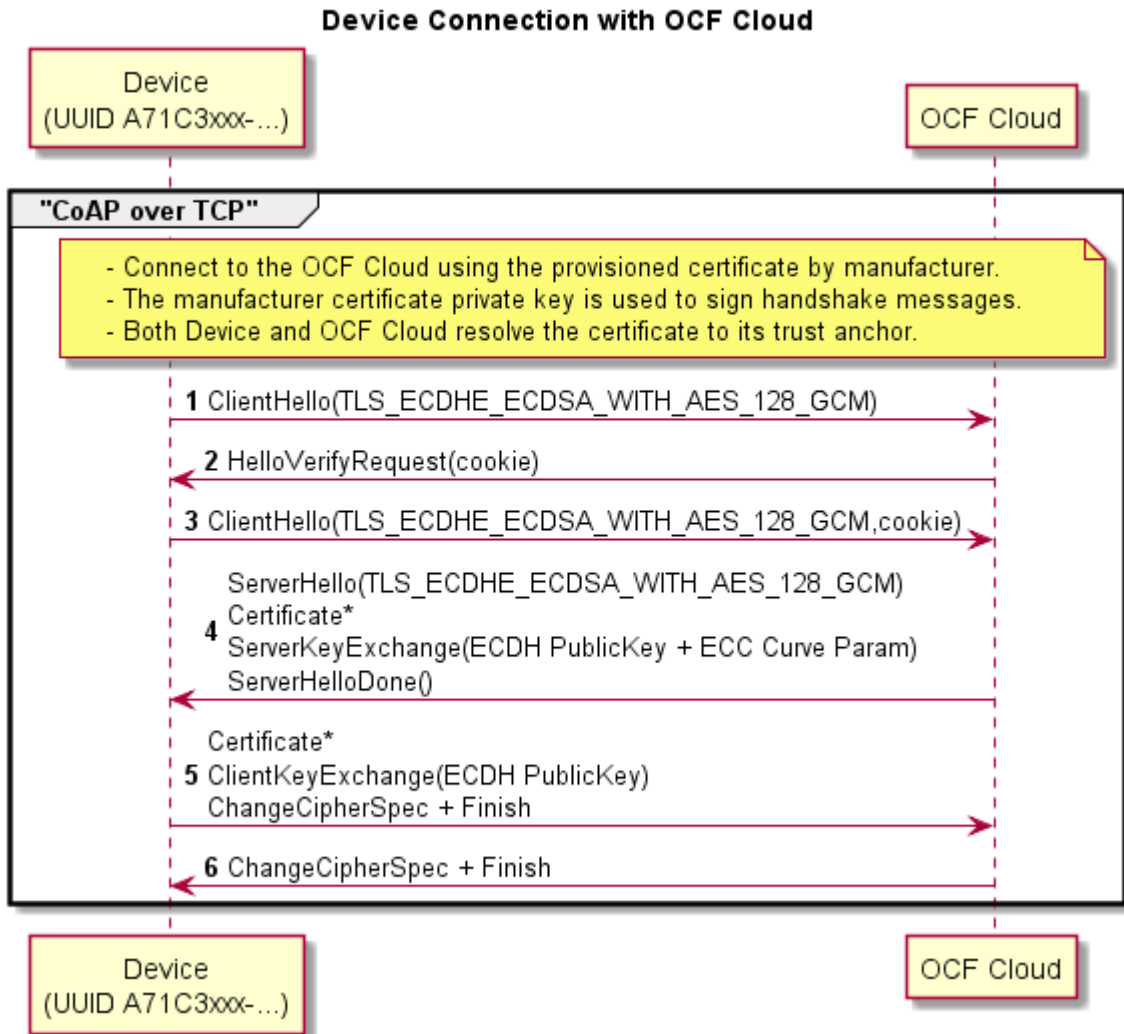
337 The OCF Cloud is expected to validate the manufacturer certificate provided by the Device.

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

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

346 Figure 3 depicts sequence for Device connection with OCF Cloud and steps described in Table 2.

347 .



348

349

Figure 3 – Device connection with OCF Cloud

350

351

Table 2 – Device connection with the OCF Cloud flow

Steps	Description
1 - 6	TLS connection between the OCF Cloud and Device. The Device's manufacturer certificate may contain data attesting to the Device hardening and security properties

352 **7.3 Security Considerations**

353 When an OCF Server receives a request sent via the OCF Cloud, then the OCF Server permits
354 that request using the identity of the OCF Cloud rather than the identity of the OCF Client. If there
355 is no mechanism through which the OCF Cloud permits only those interactions which the user
356 intends between OCF Clients and OCF Server via the OCF Cloud, and denies all other interactions,
357 then OCF Clients might get elevated privileges by submitting a request via the OCF Cloud. This is
358 highly undesirable from the security perspective. Consequently, OCF Cloud implementations are
359 expected to provide some mechanism through which the OCF Cloud prevents OCF Clients getting
360 elevated privileges when submitting a request via the OCF Cloud. In the present document release,
361 the details of the mechanism are left to the implementation.

362 The security considerations about the manufacturer certificate as described in clause 7.3.6.5 of
363 ISO/IEC 30118-2 are also applicable in the Device authentication with the OCF Cloud.

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

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

369 **Message integrity and confidentiality**

370 **8.1 Cloud Session Semantics**

371 The messages between the OCF Cloud and Device shall be exchanged only if the Device and OCF
372 Cloud authenticate each other as described in 0. The asymmetric cipher suites as described in 8.2
373 shall be employed for establishing a secured session and for encrypting/decrypting between the
374 OCF Cloud and the Device. The OCF Endpoint sending the message shall encrypt and authenticate
375 the message using the cipher suite as described in 8.2 and the OCF Endpoint shall verify and
376 decrypt the message before processing it.

377 **8.2 Cipher suites for OCF Cloud Credentials**

378 All Devices supporting OCF Cloud Certificate Credentials shall implement:

379 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

380 All Devices supporting OCF Cloud Certificate Credentials should implement:

381 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

382 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,

383 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,

385 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

386

387 **Security Resources**

388 **9.1 Account Resource**

389 The Account Resource specifies the Properties based on IETF RFC 6749 Access Token based
390 account creation. The mechanism to obtain credentials is described in Clause 0. The Account
391 Resource is used for Device Registration. The Account Resource is instantiated on the OCF Cloud
392 as "oic/sec/account" SVR and is used by cloud-enabled Devices to register with the OCF Cloud. It
393 should be only accessible on a secure channel; non-secure channel should not be able access this
394 Resource.

395 During the Device Registration process, an OCF Cloud can provide a distinct URI of another OCF
 396 Cloud ("redirected-to" OCF Cloud). Both initial and redirected-to OCF Clouds are expected to
 397 belong to the same Vendor; they are assumed to have the same UUID and are assumed to have
 398 an Out-of-Band Communication Channel established. Device does not have to perform the Device
 399 Registration on the redirected-to OCF Cloud and the OCF Cloud may ignore such attempts.
 400 Redirected-to OCF Cloud is expected to accept the Access Token, provided to the Device by the
 401 initial OCF Cloud.

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

404 The UPDATE operation on the OCF Cloud's "/oic/sec/account" Resource behaves as follows:

- 405 – A Device intending to register with the OCF Cloud shall send UPDATE with following Properties
 406 "di" ("di" Property Value of "/oic/d" Resource), and "accesstoken" as configured by the Mediator
 407 ("at" Property Value of "oic.r.coapcloudconf" Resource). The OCF Cloud verifies it is the same
 408 "accesstoken" which was assigned to the Mediator for the corresponding "di" Property Value.
 409 The "accesstoken" is the permission for the Device to access the OCF Cloud. If the "apn" was
 410 included when the Mediator UPDATED the "oic.r.coapcloudconf" Resource, the Device shall
 411 also include "authprovider" Property when registering with the OCF Cloud. If no "apn" is
 412 specified, then the "authprovider" Property shall not be included in the UPDATE request.
- 413 – OCF Cloud returns "accesstoken", "uid", "refreshtoken", and "expiresin" It may also return
 414 "redirecturi". Received "accesstoken" is to be treated by Device as an Access Token with
 415 "Bearer" token type as defined in IETF RFC 6750. This "accesstoken" shall be used for the
 416 following Account Session start using "oic/sec/session" SVR. Received "refreshtoken" is to be
 417 treated by Device as a Refresh Token as defined in IETF RFC 6749. The Device stores the
 418 OCF Cloud's Response values. If "redirecturi" is received, Device shall use received value as
 419 a new OCF Cloud URI instead of "cis" Property Value of "oic.r.coapcloudconf" Resource for
 420 further connections.

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

- 422 – To deregister with the OCF Cloud, a DELETE operation shall be sent with the "accesstoken"
 423 and either the "uid" or "di" Properties to be deregistered with the OCF Cloud. In case the "di"
 424 Property is omitted in a DELETE operation, the OCF Cloud is expected to deregister the Device
 425 with a matching "accesstoken" Property value. On DELETE with the OCF Cloud, the Device
 426 should also delete values internally stored. Once deregister with an OCF Cloud, Device can
 427 connect to any other OCF Cloud. Device deregistered need to go through the steps in 0 again
 428 to be registered with the OCF Cloud.

429 The "oic.r.account" Resource is defined in Table 3.

430 **Table 3 – Definition of the "oic.r.account" Resource**

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

431 Table 4 defines the Properties of the "oic.r.account " Resource Type.

Table 4 – Properties of the "oic.r.account" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
Device UUID	di	string	uuid	W	Yes	Unique Device identifier. Format pattern according to IETF RFC 4122.
Authorization Provider Name	authprovider	string	N/A	W	No	The name of Authorization Provider through which Access Token was obtained.
Access Token	accesstoken	string	Non-empty string	W	Yes	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID, or the Authorization Code which is then verified and exchanged for the Access Token during Device Registration.
Access Token	accesstoken	string	Non-empty string	R	Yes	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID.
Refresh Token	refreshtoken	string	Non-empty string	R	Yes	Refresh token can be used to refresh the Access Token before getting expired.
Token Expiration	expiresin	integer	-	R	Yes	Access Token life time in seconds (-1 if permanent).
User ID	uid	string	uuid	R	Yes	Unique OCF Cloud User identifier. Format pattern according to IETF RFC 4122.
Redirect URI	redirecturi	string	-	R	No	Using this URI, the Client needs to reconnect to a redirected OCF Cloud. If provided, this value shall be used by the Device instead of Mediator-provided URI during the Device Registration.

433 9.2 Account Session Resource

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

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

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

442 The UPDATE operation is defined as follows for OCF Cloud's "/oic/sec/session" Resource:

- 443 – The Device connecting to the OCF Cloud shall send an UPDATE request message to the OCF
 444 Cloud's "/oic/sec/session" Resource. The message shall include the "di" Property Value of
 445 "/oic/d" Resource and "uid", "login" Value ("true" to establish connection; "false" to disconnect)
 446 and "accesstoken" as returned by OCF Cloud during Device Registration. The OCF Cloud
 447 verifies it is the same Access Token which was returned to the Device during Device
 448 Registration process or during Token Refresh. If Device was attempting to establish the
 449 connection and provided values were verified as correct by the OCF Cloud, OCF Cloud sends
 450 a response with remaining lifetime of the associated Access Token ("expiresin" Property Value).

451 The "oic.r.session" Resource is defined in Table 5.

452

Table 5 – Definition of the "oic.r.session" Resource

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

453 Table 6 defines the Properties of the "oic.r.session" Resource.

454

Table 6 – Properties of the "oic.r.session" Resource

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
User ID	uid	string	uuid	W	Yes	User ID provided by Device Registration process. Format pattern according to IETF RFC 4122.
Device UUID	di	string	uuid	W	Yes	Unique Device UUID registered for a Device. Format pattern according to IETF RFC 4122.
Access Token	accesstoken	string	A string of at least one character	W	Yes	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID
Login Status	login	boolean	N/A	W	Yes	Action for the request: true = login, false = logout
Token Expiration	expiresin	integer	N/A	R	Yes	Remaining Access Token life time in seconds (-1 if permanent) This Property is only provided to Device during connection establishment (when "login" Property Value equals "true"), it's not available otherwise

455 **9.3 Account Token Refresh Resource**

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

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

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

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

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

- 464 – The Device attempting to refresh the Access Token shall send an UPDATE request message
465 to the OCF Cloud's "/oic/sec/tokenrefresh" Resource. The message shall include the "di"
466 Property Value of "/oic/d" Resource, "uid" and "refreshtoken", as returned by OCF Cloud.
- 467 – OCF Cloud response is expected to include a "refreshtoken", new "accesstoken", and
468 "expiresin". Received "accesstoken" is to be treated by Device as an Access Token with
469 "Bearer" token type as defined in IETF RFC 6750. This Access Token is the permission for the
470 Device to access the OCF Cloud. Received "refreshtoken" is to be treated by Device as a
471 Refresh Token as defined in IETF RFC 6749. Received "refreshtoken" may be the new Refresh
472 Token or the same one as provided by the Device in the UPDATE request. In case when new
473 distinct "refreshtoken" is provided by the OCF Cloud, the Device shall discard the old value.

474 The OCF Cloud's response values "refreshtoken", "accesstoken" and "expiresin" are securely
 475 stored on the Device.

476 The "oic.r.tokenrefresh" Resource is defined in Table 7.

477 **Table 7 – Definition of the "oic.r.tokenrefresh" Resource**

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

478 Table 8 defines the Properties of the "oic.r.tokenrefresh" Resource.

479 **Table 8 – Properties of the "oic.r.tokenrefresh" Resource**

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Description
User ID	uid	string	uuid	W	Yes	User ID provided by Sign-up process. Format pattern according to IETF RFC 4122.
Device UUID	di	string	uuid	W	Yes	Unique Device UUID registered for an OCF Cloud User account. Format pattern according to IETF RFC 4122.
Refresh Token	refreshtoken	string	A string of at least one character	RW	Yes	Refresh token can be used to refresh the Access Token before getting expired.
Access Token	accesstoken	string	A string of at least one character	R	Yes	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID.
Token Expiration	expiresin	integer	-	R	Yes	Access Token life time in seconds (-1 if permanent).

480 **Security hardening guidelines**

481 **10.1 Security hardening guidelines general**

482 In addition to the Sensitive Data list outlined in Table 75 of ISO/IEC 30118-2, any Device
 483 implementing OCF Cloud connection capabilities should also provide reasonable protection for the
 484 information in Table 9.

485 **Table 9 – Sensitive Data related to OCF Cloud**

Data	Integrity protection	Confidentiality protection
OCF Cloud URL	Yes	Not required
OCF Cloud Identity	Yes	Not required

486

487 **Annex A**
488 **(normative)**
489 **Resource Type definitions**

490 **A.1 List of Resource Type definitions**

491 All the clauses in Annex A describe the Resource Types with a RESTful API definition language.
492 The Resource Type definitions presented in Annex A are formatted for readability, and so may
493 appear to have extra line breaks.

494 Table A.1 contains the list of defined security Resources in this document.

495 **Table A.1 – Alphabetized list of security Resources**

Friendly Name (informative)	Resource Type (rt)	Clause
Account	oic.r.account	A.2
Account Session	oic.r.session	A.3
Account Token Refresh	oic.r.tokenrefresh	A.4

496 **A.2 Account Token**

497 **A.2.1 Introduction**

498 Sign-up using generic account provider.

499 **A.2.2 Well-known URI**

500 /oic/sec/account

501 **A.2.3 Resource type**

502 The Resource Type is defined as: "oic.r.account".

503 **A.2.4 OpenAPI 2.0 definition**

```
504 {  
505   "swagger": "2.0",  
506   "info": {  
507     "title": "Account Token",  
508     "version": "20190111",  
509     "license": {  
510       "name": "OCF Data Model License",  
511       "url":  
512       "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/LI  
513       CENSE.md",  
514       "x-copyright": "copyright 2016-2017, 2019 Open Connectivity Foundation, Inc. All rights  
515       reserved."  
516     },  
517     "termsOfService": "https://openconnectivityfoundation.github.io/core/DISCLAIMER.md"  
518   },  
519   "schemes": ["http"],  
520   "consumes": ["application/json"],  
521   "produces": ["application/json"],  
522   "paths": {  
523     "/oic/sec/account" : {  
524       "post": {  
525         "description": "Sign-up using generic account provider.\n",  
526         "parameters": [  
527           {"$ref": "#/parameters/interface"},  
528           {  
529             "name": "body",  
530             "in": "body",  
531             "required": true,  
532             "schema": { "$ref": "#/definitions/Account-request" },  
533             "x-example":  
534             {
```

```

535         "di" : "9cfbeb8e-5ale-4dlc-9d01-00c04fd430c8",
536         "authprovider" : "github",
537         "accesstoken" : "8802f2eaf8b5e147a936"
538     }
539 }
540 ],
541 "responses": {
542     "204": {
543         "description" : "2.04 Changed respond with required and optional information\n",
544         "x-example":
545         {
546             "rt": ["oic.r.account"],
547             "accesstoken" : "0f3d9f7fe5491d54077d",
548             "refreshtoken" : "00fe4644a6fbe5324eec",
549             "expiresin" : 3600,
550             "uid" : "123e4567-e89b-12d3-a456-d6e313b71d9f",
551             "redirecturi" : "coaps+tcp://example.com:443"
552         },
553         "schema": { "$ref": "#/definitions/Account-response" }
554     }
555 }
556 },
557 "delete": {
558     "description": "Delete a device. This also removes all resources in the device on cloud
559 side.\nexample: /oic/account?di=9cfbeb8e-5ale-4dlc-9d01-
560 00c04fd430c8&accesstoken=0f3d9f7fe5491d54077d\n",
561     "parameters": [
562         { "$ref": "#/parameters/interface" }
563     ],
564     "responses": {
565         "202": {
566             "description" : "2.02 Deleted response informing the device is successfully
567 deleted.\n"
568         }
569     }
570 }
571 }
572 },
573 "parameters": {
574     "interface" : {
575         "in" : "query",
576         "name" : "if",
577         "type" : "string",
578         "enum" : ["oic.if.baseline"]
579     }
580 },
581 "definitions": {
582     "Account-request" : {
583         "properties": {
584             "authprovider": {
585                 "description": "The name of Authorization Provider through which Access Token was
586 obtained",
587                 "type": "string"
588             },
589             "accesstoken" : {
590                 "description": "Access-Token used for communication with OCF Cloud after account
591 creation",
592                 "pattern": "(?!$|\\s+).*",
593                 "type": "string"
594             },
595             "di": {
596                 "description": "Format pattern according to IETF RFC 4122.",
597                 "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
598 9]{12}$",
599                 "type": "string"
600             }
601         },
602         "type" : "object",
603         "required": ["di", "accesstoken"]
604     },
605     "Account-response": {
606         "properties": {

```

```

607     "expiresin" : {
608         "description": "Access-Token remaining life time in seconds (-1 if permanent)",
609         "readOnly": true,
610         "type": "integer"
611     },
612     "rt": {
613         "description": "Resource Type of the Resource",
614         "items": {
615             "maxLength": 64,
616             "type": "string",
617             "enum" : ["oic.r.account"]
618         },
619         "minItems": 1,
620         "maxItems": 1,
621         "readOnly": true,
622         "type": "array"
623     },
624     "refreshToken" : {
625         "description": "Refresh token can be used to refresh the Access Token before getting
626 expired",
627         "pattern": "(?!$|\\s+).*",
628         "readOnly": true,
629         "type": "string"
630     },
631     "uid" : {
632         "description": "Format pattern according to IETF RFC 4122.",
633         "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
634 9]{12}$",
635         "type": "string"
636     },
637     "accesstoken" : {
638         "description": "Access-Token used for communication with cloud after account creation",
639         "pattern": "(?!$|\\s+).*",
640         "type": "string"
641     },
642     "n": {
643         "$ref":
644         "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
645         schema.json#/definitions/n"
646     },
647     "id": {
648         "$ref":
649         "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
650         schema.json#/definitions/id"
651     },
652     "redirecturi" : {
653         "description": "Using this URI, the Client needs to reconnect to a redirected OCF Cloud.
654 If provided, this value shall be used by the Device instead of Mediator-provided URI during the
655 Device Registration.",
656         "readOnly": true,
657         "type": "string"
658     },
659     "if": {
660         "description": "The interface set supported by this resource",
661         "items": {
662             "enum": [
663                 "oic.if.baseline"
664             ],
665             "type": "string"
666         },
667         "minItems": 1,
668         "maxItems": 1,
669         "uniqueItems": true,
670         "readOnly": true,
671         "type": "array"
672     }
673 },
674 "type" : "object",
675 "required": ["accesstoken", "refreshToken", "expiresin", "uid"]
676 }
677 }

```

678 }
 679

680 **A.2.5 Property definition**

681 Table A.2 defines the Properties that are part of the "oic.r.account" Resource Type.

682 **Table A.2 – The Property definitions of the Resource with type "rt" = "oic.r.account".**

Property name	Value type	Mandatory	Access mode	Description
di	string	Yes	Write Only	Unique Device identifier. Format pattern according to IETF RFC 4122.
authprovider	string	No	Write Only	The name of Authorization Provider through which Access Token was obtained.
accesstoken	string	Yes	Write Only	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID, or the Authorization Code which is then verified and exchanged for the Access Token during Device Registration.
id	multiple types: see schema	No	Read Write	
refresh token	string	Yes	Read Only	Refresh token can be used to refresh the Access Token before getting expired.
rt	array: see schema	No	Read Only	Resource Type of the Resource
accesstoken	string	Yes	Read Only	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID.
uid	string	Yes	Read Only	Unique OCF Cloud User

				identifier. Format pattern according to IETF RFC 4122.
expiresin	integer	Yes	Read Only	Access-Token life time in seconds (-1 if permanent)
if	array: see schema	No	Read Only	The interface set supported by this Resource
redirecturi	string	No	Read Only	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.
n	multiple types: see schema	No	Read Write	

683 **A.2.6 CRUDN behaviour**

684 Table A.3 defines the CRUDN operations that are supported on the "oic.r.account" Resource Type.

685 **Table A.3 – The CRUDN operations of the Resource with type "rt" = "oic.r.account".**

Create	Read	Update	Delete	Notify
		post	delete	

686 **A.3 Session**

687 **A.3.1 Introduction**

688 Resource that manages the persistent session between a Device and OCF Cloud.

689 **A.3.2 Well-known URI**

690 /oic/sec/session

691 **A.3.3 Resource type**

692 The Resource Type is defined as: "oic.r.session".

693 **A.3.4 OpenAPI 2.0 definition**

```

694 {
695   "swagger": "2.0",
696   "info": {
697     "title": "Session",
698     "version": "v1.0-20181001",
699     "license": {
700       "name": "OCF Data Model License",
701       "url":
702 "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/LI
703 CENSE.md",
704     "x-copyright": "copyright 2016-2017, 2019 Open Connectivity Foundation, Inc. All rights
705 reserved."
706   },

```

```

707     "termsOfService": "https://openconnectivityfoundation.github.io/core/DISCLAIMER.md"
708   },
709   "schemes": ["http"],
710   "consumes": ["application/json"],
711   "produces": ["application/json"],
712   "paths": {
713     "/oic/sec/session" : {
714       "post": {
715         "description": "Resource that manages the persistent session between a Device and OCF
716 Cloud.",
717         "parameters": [
718           { "$ref": "#/parameters/interface" },
719           {
720             "name": "body",
721             "in": "body",
722             "required": true,
723             "schema": { "$ref": "#/definitions/Account-Session-Request" },
724             "x-example":
725               {
726                 "uid" : "123e4567-e89b-12d3-a456-d6e313b71d9f",
727                 "di" : "9cfbeb8e-5ale-4dlc-9d01-00c04fd430c8",
728                 "accesstoken" : "0f3d9f7fe5491d54077d",
729                 "login" : true
730               }
731           }
732         ],
733         "responses": {
734           "204": {
735             "description": "",
736             "x-example":
737               {
738                 "rt": ["oic.r.session"],
739                 "expiresin" : 3600
740               },
741             "schema": { "$ref": "#/definitions/Account-Session-Response" }
742           }
743         }
744       }
745     }
746   },
747   "parameters": {
748     "interface" : {
749       "in" : "query",
750       "name" : "if",
751       "type" : "string",
752       "enum" : ["oic.if.baseline"]
753     }
754   },
755   "definitions": {
756     "Account-Session-Request" : {
757       "properties": {
758         "uid": {
759           "description": "Format pattern according to IETF RFC 4122.",
760           "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
761 9]{12}$",
762           "type": "string"
763         },
764         "di": {
765           "description": "The Device UUID\nFormat pattern according to IETF RFC 4122.",
766           "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
767 9]{12}$",
768           "type": "string"
769         },
770         "accesstoken": {
771           "description": "Access-Token used to grant access right for the Device to sign-in.",
772           "pattern": "(?!$|\\s+).*",
773           "type": "string"
774         },
775         "login": {
776           "description": "Action for the request: true = login, false = logout.",
777           "type": "boolean"
778         }
779       }
780     }
781   }

```

```

779     },
780     "type" : "object",
781     "required": ["uid", "di", "accesstoken", "login"]
782 },
783 "Account-Session-Response" : {
784   "properties": {
785     "expiresin": {
786       "description": "Access-Token remaining life time in seconds (-1 if permanent).",
787       "readOnly": true,
788       "type": "integer"
789     },
790     "rt": {
791       "description": "Resource Type of the Resource.",
792       "items": {
793         "maxLength": 64,
794         "type": "string",
795         "enum": ["oic.r.session"]
796       },
797       "minItems": 1,
798       "readOnly": true,
799       "type": "array"
800     },
801     "n": {
802       "$ref":
803 "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
804 schema.json#/definitions/n"
805     },
806     "id": {
807       "$ref":
808 "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
809 schema.json#/definitions/id"
810     },
811     "if": {
812       "description": "The interface set supported by this Resource.",
813       "items": {
814         "enum": [
815           "oic.if.baseline"
816         ],
817         "type": "string"
818       },
819       "minItems": 1,
820       "readOnly": true,
821       "type": "array"
822     }
823   },
824   "type" : "object",
825   "required" : ["expiresin"]
826 }
827 }
828 }
829

```

830 A.3.5 Property definition

831 Table A.4 defines the Properties that are part of the "oic.r.session" Resource Type.

832 **Table A.4 – The Property definitions of the Resource with type "rt" = "oic.r.session".**

Property name	Value type	Mandatory	Access mode	Description
if	array: see schema	No	Read Only	The interface set supported by this Resource.
expiresin	integer	Yes	Read Only	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.
rt	array: see schema	No	Read Only	Resource Type of the Resource.
id	multiple types: see schema	No	Read Write	
n	multiple types: see schema	No	Read Write	
di	string	Yes	Write Only	Unique Device UUID registered for a Device. Format pattern according to IETF RFC 4122.
accesstoken	string	Yes	Write Only	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID.
uid	string	Yes	Write Only	User ID provided by Device Registration process. Format pattern according to IETF RFC 4122.
login	boolean	Yes	Write Only	Action for the request: true = login, false = logout.

833 **A.3.6 CRUDN behaviour**

834 Table A.5 defines the CRUDN operations that are supported on the "oic.r.session" Resource Type.

835 **Table A.5 – The CRUDN operations of the Resource with type "rt" = "oic.r.session".**

Create	Read	Update	Delete	Notify
		post		

836 **A.4 Token Refresh**

837 **A.4.1 Introduction**

838 Obtain fresh Access Token using the refresh token, client should refresh Access Token before it
839 expires.

840 **A.4.2 Well-known URI**

841 /oic/sec/tokenrefresh

842 A.4.3 Resource type

843 The Resource Type is defined as: "oic.r.tokenrefresh".

844 A.4.4 OpenAPI 2.0 definition

```
845 {
846   "swagger": "2.0",
847   "info": {
848     "title": "Token Refresh",
849     "version": "v1.0-20181001",
850     "license": {
851       "name": "OCF Data Model License",
852       "url":
853       "https://github.com/openconnectivityfoundation/core/blob/e28a9e0a92e17042ba3e83661e4c0fbce8bdc4ba/LI
854       CENSE.md",
855       "x-copyright": "copyright 2016-2017, 2019 Open Connectivity Foundation, Inc. All rights
856       reserved."
857     },
858     "termsOfService": "https://openconnectivityfoundation.github.io/core/DISCLAIMER.md"
859   },
860   "schemes": ["http"],
861   "consumes": ["application/json"],
862   "produces": ["application/json"],
863   "paths": {
864     "/oic/sec/tokenrefresh" : {
865       "post": {
866         "description": "Obtain fresh access-token using the refresh token, client should refresh
867         access-token before it expires.\n",
868         "parameters": [
869           { "$ref": "#/parameters/interface" },
870           {
871             "name": "body",
872             "in": "body",
873             "required": true,
874             "schema": { "$ref": "#/definitions/TokenRefresh-Request" },
875             "x-example":
876             {
877               "uid" : "123e4567-e89b-12d3-a456-d6e313b71d9f",
878               "di" : "9cfbeb8e-5a1e-4d1c-9d01-00c04fd430c8",
879               "refreshToken" : "00fe4644a6fbe5324eec"
880             }
881           }
882         ],
883         "responses": {
884           "204": {
885             "description": "2.04 Changed respond with new access-token.\n",
886             "x-example":
887             {
888               "rt": ["oic.r.tokenrefresh"],
889               "accessToken" : "8ce598980761869837be",
890               "refreshToken" : "d4922312b6df0518e146",
891               "expiresin" : 3600
892             }
893           },
894           "schema": { "$ref": "#/definitions/TokenRefresh-Response" }
895         }
896       }
897     }
898   },
899   "parameters": {
900     "interface" : {
901       "in" : "query",
902       "name" : "if",
903       "type" : "string",
904       "enum" : ["oic.if.baseline"]
905     }
906   },
907   "definitions": {
908     "TokenRefresh-Request" : {
909       "properties": {
910         "refreshToken": {
```

```

912         "description": "Refresh token received by account management or during token refresh
913 procedure.",
914         "pattern": "(?!$|\\s+).*",
915         "type": "string"
916     },
917     "uid": {
918         "description": "Format pattern according to IETF RFC 4122.",
919         "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
920 9]{12}$",
921         "type": "string"
922     },
923     "di": {
924         "description": "Format pattern according to IETF RFC 4122.",
925         "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-
926 9]{12}$",
927         "type": "string"
928     }
929 },
930 "type": "object",
931 "required": ["uid", "di", "refreshtoken"]
932 },
933 "TokenRefresh-Response" : {
934     "properties": {
935         "expiresin": {
936             "description": "Access-Token life time in seconds (-1 if permanent).",
937             "readOnly": true,
938             "type": "integer"
939         },
940         "rt": {
941             "description": "Resource Type of the Resource.",
942             "items": {
943                 "maxLength": 64,
944                 "type": "string",
945                 "enum": ["oic.r.tokenrefresh"]
946             },
947             "minItems": 1,
948             "readOnly": true,
949             "type": "array"
950         },
951         "refreshtoken": {
952             "description": "Refresh token received by account management or during token refresh
953 procedure.",
954             "pattern": "(?!$|\\s+).*",
955             "type": "string"
956         },
957         "accesstoken": {
958             "description": "Granted Access-Token.",
959             "pattern": "(?!$|\\s+).*",
960             "readOnly": true,
961             "type": "string"
962         },
963         "n": {
964             "$ref":
965 "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
966 schema.json#/definitions/n"
967         },
968         "id": {
969             "$ref":
970 "https://openconnectivityfoundation.github.io/core/schemas/oic.common.properties.core-
971 schema.json#/definitions/id"
972         },
973         "if" :
974         {
975             "description": "The interface set supported by this Resource.",
976             "items": {
977                 "enum": [
978                     "oic.if.baseline"
979                 ],
980                 "type": "string"
981             },
982             "minItems": 1,
983             "readOnly": true,

```

```

984     "type": "array"
985   },
986 },
987 "type" : "object",
988 "required": ["accesstoken", "refreshtoken", "expiresin"]
989 }
990 }
991 }
992

```

993 A.4.5 Property definition

994 Table A.6 defines the Properties that are part of the "oic.r.tokenrefresh" Resource Type.

995 **Table A.6 – The Property definitions of the Resource with type "rt" = "oic.r.tokenrefresh".**

Property name	Value type	Mandatory	Access mode	Description
refreshtoken	string	Yes	Write Only	Refresh token can be used to refresh the Access Token before getting expired.
uid	string	Yes	Write Only	User ID provided by Sign-up process. Format pattern according to IETF RFC 4122.
di	string	Yes	Write Only	Unique Device UUID registered for an OCF Cloud User account. Format pattern according to IETF RFC 4122.
if	array: see schema	No	Read Only	The interface set supported by this Resource.
expiresin	integer	Yes	Read Only	Access Token life time in seconds (-1 if permanent).
accesstoken	string	Yes	Read Only	Access Token used to authorize and associate the TLS connection for communication with the OCF Cloud with the Device UUID.
refreshtoken	string	Yes	Read Only	Refresh token can be used to refresh the Access Token before getting expired.
n	multiple types: see schema	No	Read Write	

rt	array: see schema	No	Read Only	Resource Type of the Resource.
id	multiple types: see schema	No	Read Write	

996 **A.4.6 CRUDN behaviour**

997 Table A.7 defines the CRUDN operations that are supported on the "oic.r.tokenrefresh" Resource
 998 Type.

999 **Table A.7 – The CRUDN operations of the Resource with type "rt" = "oic.r.tokenrefresh".**

Create	Read	Update	Delete	Notify
		post		

1000

1001