

OCF Onboarding Tool Specification

VERSION 2.2.0 | July 2020



OPEN CONNECTIVITY
FOUNDATION™

CONTACT admin@openconnectivityfoundation.org
Copyright OCF © 2020. All Rights Reserved.



2 **LEGAL DISCLAIMER**

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

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

16 Copyright © 2017-2020 Open Connectivity Foundation, Inc. All rights reserved.

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

18 **CONTENTS**

19 1 Scope 1

20 2 Normative References 1

21 3 Terms, definitions, and abbreviated terms 2

22 3.1 Terms and definitions..... 2

23 3.2 Abbreviated terms 3

24 4 Document Conventions and Organization 4

25 5 Services and Availability in the OBT 5

26 5.1 Purpose of the OBT 5

27 5.2 General OBT requirements 6

28 5.3 DOTS 7

29 5.3.1 Assuming ownership of a Device 7

30 5.3.2 DOTS and Bridging..... 8

31 5.3.3 Security considerations regarding selecting an Ownership Transfer Method 9

32 5.4 CMS 9

33 5.5 AMS..... 10

34 6 Certificate management requirements 10

35 6.1 Issuing identity certificates and role certificates 10

36 6.2 Provisioning Trust Anchor certificates 11

37 7 Ownership Transfer Methods 11

38 7.1 Preamble 11

39 7.2 Just Works Owner Transfer Method 11

40 7.3 Random PIN / Shared Credential based Owner Transfer Method 11

41 7.4 Manufacturer Certificate Based Owner Transfer Method 12

42 7.5 Vendor-Specific Owner Transfer Methods 12

43

44 **FIGURES**

45 **No table of figures entries found.**

46

47 **Tables**

48 Table 1 –Overview of OBT access in Device Onboarding States6

49 Table 2 – ACL entries to provision for role usage uniformity..... 10

50

51

52 **1 Scope**

53 This document defines mechanisms supported by an OCF Onboarding Tool (OBT). This document
54 contains security normative content for the OBT and may contain informative content related to the
55 OCF base or OCF Security Specification other OCF documents.

56 **2 Normative References**

57 The following documents are referred to in the text in such a way that some or all of their content
58 constitutes requirements of this document. For dated references, only the edition cited applies. For
59 undated references, the latest edition of the referenced document (including any amendments)
60 applies.

61 ISO/IEC 30118-1:2018 Information technology -- Open Connectivity Foundation (OCF)
62 Specification -- Part 1: Core specification
63 <https://www.iso.org/standard/53238.html>
64 Latest version available at:
65 https://openconnectivity.org/specs/OCF_Core_Specification.pdf

66 ISO/IEC 30118-2:2018 Information technology – Open Connectivity Foundation (OCF)
67 Specification – Part 2: Security specification
68 <https://www.iso.org/standard/74239.html>
69 Latest version available at: https://openconnectivity.org/specs/OCF_Security_Specification.pdf

70 ISO/IEC 30118-3:2018 Information technology -- Open Connectivity Foundation (OCF)
71 Specification -- Part 3: Bridging specification
72 <https://www.iso.org/standard/74240.html>
73 Latest version available at:
74 https://openconnectivity.org/specs/OCF_Bridging_Specification.pdf

75 ISO/IEC 30118-7:2018, Information technology – Open Connectivity Foundation (OCF)
76 Specification – Part 7: Wi-Fi Easy Setup specification
77 Latest version available at:
78 https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf

79 NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation
80 Using Deterministic Random Bit Generators
81 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>

82 Open Connectivity Foundation (OCF) Specification – Cloud Security Specification
83 Latest version available at:
84 https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf

85

86 **3 Terms, definitions, and abbreviated terms**

87 **3.1 Terms and definitions**

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

90 ISO and IEC maintain terminological databases for use in standardization at the following
91 addresses:

92 – ISO Online browsing platform: available at <https://www.iso.org/obp>

93 – IEC Electropedia: available at <http://www.electropedia.org/>

94 **3.1.1**

95 **Access Control Entry**

96 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

97 **3.1.2**

98 **Access Control List**

99 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

100 **3.1.3**

101 **Access Management Service (AMS)**

102 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

103 **3.1.4**

104 **Bridge**

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

106 **3.1.5**

107 **Client**

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

109 **3.1.6**

110 **Credential Management Service (CMS)**

111 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

112 **3.1.7**

113 **Device**

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

115 **3.1.8**

116 **Device Ownership Transfer Service (DOTS)**

117 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

118 **3.1.9**

119 **End User**

120 The person using the [particular] product

121 **3.1.10**

122 **(OCF) Onboarding**

123 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

124 **3.1.11**

125 **Onboarding Tool (OBT)**

126 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

127 **3.1.12**

128 **Out of Band Communication Channel**

129 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

130 **3.1.13**
131 **Owned (or "in Owned State")**
132 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

133 **3.1.14**
134 **Owner Credential**
135 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

136 **3.1.15**
137 **Property**
138 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

139 **3.1.16**
140 **Resource**
141 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

142 **3.1.17**
143 **OCF Security Domain**
144 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

145 **3.1.18**
146 **Owner Transfer Method**
147 Note 1 to entry: See ISO/IEC 30118-2:2018.

148 **3.1.19**
149 **Security Virtual Resource (SVR)**
150 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

151 **3.1.20**
152 **Server**
153 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

154 **3.1.21**
155 **Trust Anchor**
156 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

157 **3.1.22**
158 **Unowned (or "in Unowned State")**
159 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

160 **3.1.23**
161 **Virtual OCF Device**
162 Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

163 **3.2 Abbreviated terms**

164 **3.2.1**
165 **ACE**
166 Access Control Entry
167 Note 1 to entry: See ISO/IEC 30118-2:2018.

168 **3.2.2**
169 **ACL**
170 Access Control List
171 Note 1 to entry: See ISO/IEC 30118-2:2018.

172 **3.2.3**
173 **AMS**
174 Access Management Service

175 Note 1 to entry: See ISO/IEC 30118-2:2018.

176 **3.2.4**

177 **CMS**

178 Credential Management Service

179 Note 1 to entry: See ISO/IEC 30118-2:2018.

180 **3.2.5**

181 **OBT**

182 Onboarding Tool

183 Note 1 to entry: See ISO/IEC 30118-2:2018.

184 **3.2.6**

185 **OTM**

186 Owner Transfer Method

187 Note 1 to entry: See ISO/IEC 30118-2:2018.

188 **3.2.7**

189 **PIN**

190 Personal Identification Number

191 Note 1 to entry: See ISO/IEC 30118-2:2018.

192 **3.2.8**

193 **PPSK**

194 PIN-authenticated pre-shared key

195 Note 1 to entry: See ISO/IEC 30118-2:2018.

196 **3.2.9**

197 **SVR**

198 Security Virtual Resource

199 Note 1 to entry: See ISO/IEC 30118-2:2018.

200 **3.2.10**

201 **VOD**

202 Virtual OCF Device

203 Note 1 to entry: See ISO/IEC 30118-3:2018.

204 **4 Document Conventions and Organization**

205 See ISO/IEC 30118-1:2018.

206 **5 Services and Availability in the OBT**

207 **5.1 Purpose of the OBT**

208 The purpose of an OBT is to provide the foundation of trust for an OCF Security Domain. An OBT
209 is an OCF Device which can provide a variety of functions. The OBT functions fall into two main
210 categories: establishing ownership of Devices being added to the OCF Security Domain; and
211 provisioning of Devices in the OCF Security Domain. The intent is that a single OBT can provide
212 all these functions, but there is no prohibition against these functions being distributed across
213 multiple OBTs.

214 OCF Security Domain is associated with its UUID, determined by an OBT. The OBT is responsible
215 for maintaining the OCF Security Domain UUID, and provisions the same value to each Device that
216 is part of the same domain.

217 The term (OCF) Onboarding refers to the initial establishment of ownership over a Device, and
218 initial provisioning of the Device for normal operation (see clause 5.3 of ISO/IEC 30118-2:2018). A
219 Device can be reset to enable subsequent Onboarding of the Device, for example following a
220 subsequent sale to another person. A Device can also be further provisioned without repeating
221 the entire Onboarding process.

222 The following OBT functions are specified:

- 223 – A Device Ownership Transfer Service (DOTS) establishes ownership of Devices being added
224 to the OCF Security Domain. This function is described in clause 5.3.
- 225 – A Credential Management Service (CMS) manages the credentials and Roles of Devices in the
226 OCF Security Domain. This function is described in clause 5.4.
- 227 – An Access Management Service (AMS) manages the access of Devices in the OCF Security
228 Domain. This function is described in clause 5.5.
- 229 – Optional: A Mediator facilitates further configuration of Devices in the OCF Security Domain for
230 various purposes including Wi-Fi configuration (see ISO/IEC 30118-7:2018) and OCF Cloud
231 access (see Cloud Security Specification).

232 The OBT demands a higher level of security hardening than regular OCF Devices in order to
233 preserve integrity and confidentiality of sensitive credentials being stored.

234 As mentioned, to accommodate a scalable and modular design, these functions are considered as
235 services that could be deployed on separate Devices. Currently, the deployment assumes that
236 these services are all deployed as part of an OBT. Regardless of physical deployment scenario,
237 the same security-hardening requirement applies to any physical server that hosts the services
238 discussed here.

239 The Device Onboarding States are defined in clause 8 of ISO/IEC 30118-2:2018. Table 1 provides
240 an overview of the access granted to the OBT components according to the Device Onboarding
241 States.

Table 1 –Overview of OBT access in Device Onboarding States

Device Onboarding State	Description		Applicable Resources & Access	Entity Authorized to READ/WRITE	Purpose	"/oic/sec/doxm:owned"
RESET	Full reset of OCF Device to manufacturer default.		No Access	No Access	Remove info in SVRs.	FALSE
RFOTM	Ready for Ownership Transfer Mechanism.	Prior to successful OTM	"/oic/sec/doxm" (R: all, W: oxmsel)	Any	R: Determine supported OTMs W: Select an OTM	FALSE
		After successful OTM	"/oic/sec/doxm" (RW) "/oic/sec/cred" (RW)	DOTS	Claim ownership. Establish credentials for authenticating DOTS, AMS, CMS & optionally other Devices	
			(At discretion of End User of DOTS) "/oic/sec/sp" (RW)	DOTS	R: Determine supported Security Profiles. W: Set current security profile.	
			(At discretion of End User of DOTS) "/oic/sec/acl2" (RW)	DOTS	Configure further ACEs	
			"/oic/sec/pstat" (RW)	DOTS	Transition to RFPRO or RESET	
RFPRO	Ready for Provisioning.	"/oic/sec/cred" (RW)	CMS or matching ACE	Establish credentials for authenticating Devices in normal operation, including Roles	TRUE	
		"/oic/sec/acl2" (RW)	AMS or matching ACE	Establish ACEs for normal operation		
		"/oic/sec/sp" (RW)	DOTS or matching ACE	R: Determine supported Security Profiles. W: Set current security profile		
		"/oic/sec/pstat" (RW)	DOTS, CMS, AMS or matching ACE	Transition to RFNOP		
RFNOP	Ready for Normal Operation.	"/oic/sec/pstat"	DOTS, CMS, AMS or matching ACE	Transition to RFPRO, SRESET or RESET	TRUE	
		Vertical Resources	Matching ACE	Normal Operation		
SRESET	Soft RESET.	"/oic/sec/cred" (RW)	CMS	Corrections as needed	TRUE	
		"/oic/sec/acl2" (RW)	AMS	Corrections as needed		
		"/oic/sec/doxm" (RW)	DOTS	Corrections as needed		
		"/oic/sec/pstat" (RW)	DOTS, CMS or AMS	Transition to RFPRO or RESET		

243

244 5.2 General OBT requirements

245 An OBT shall be hosted on an OCF Device.

246 An OBT shall host at least one of a DOTS, AMS and CMS.

247 All DOTS, AMS and CMS shall be hosted on an OBT.

248 An OBT may change the Device state of a Device by updating "s" field in the "dos" Property object
249 of the "/oic/sec/pstat" Resource to the desired value. The allowed Device state transitions are
250 defined in 13.8 of ISO/IEC 30118-2:2018.

251 After successful OTM, but before placing the newly-onboarded Device in RFNOP, the OBT shall
252 remove all SVR entries in the "resources" array for ACEs where the Subject is "anon-clear" or
253 "auth-crypt".

254 The OBT should support all mandatory and optional ciphersuites in clauses 11.3.3 and 11.3.4 of
255 ISO/IEC 30118-2:2018.

256 **5.3 DOTS**

257 **5.3.1 Assuming ownership of a Device**

258 The DOTS shall support all OTMs in clause 7.

259 An overview is provided in clauses 5.3.3 and 7.2 of ISO/IEC 30118-2:2018.

260 The following steps shall be performed to take ownership of a Device. The Device is presumed to
261 be in RFOTM.

262 1) The DOTS performs a multicast retrieve on the "/oic/sec/doxm" Resource using "owned=false"
263 query parameter as described in ISO/IEC 30118-2:2018.

264 2) Before proceeding, the DOTS shall obtain acknowledgement from the OBT End User that the
265 OBT End User approves the DOTS assuming ownership of the discovered Device(s). See
266 security considerations in clause 5.3.3.

267 3) The DOTS selects a mutually supported OTM from the "oxms" Property of the "/oic/sec/doxm"
268 Resource. See security considerations in clause 5.3.3.

269 4) The DOTS shall UPDATE the "oxmsel" Property of "/oic/sec/doxm" the value corresponding to
270 the OTM being used, before performing other OTM steps.

271 5) The DOTS shall initiate a DTLS Session as specified for the OTM configured to the oxmsel
272 Property of the "/oic/sec/doxm" Resource. Details are provided in clause 7.

273 6) The DOTS shall send an UPDATE request message to "/oic/sec/pstat" to set the value of "om"
274 to 0b 0000 0100 to select Client-directed provisioning.

275 7) The DOTS shall UPDATE the "devowneruuid" Property of the "/oic/sec/doxm" Resource with
276 the UUID of the DOTS.

277 8) The DOTS may RETRIEVE the updated "deviceuuid" Property of the "/oic/sec/doxm" Resource
278 after the DOTS has updated the "devowneruuid" Property value of the "/oic/sec/doxm"
279 Resource to a non-nil-UUID value.

280 9) The DOTS shall UPDATE the "deviceuuid" of the "/oic/sec/doxm" Resource. The updated value
281 shall be a value that the DOTS has generated. The DOTS should use a NIST SP-800-90A-
282 compliant RNG to guarantee sufficient entropy.

283 10) The DOTS shall provision the ownership credential as follows:

284 a) The DOTS shall generate a Shared Key using the SharedKey Credential Calculation method
285 described in clause 7.3.2 of ISO/IEC 30118-2:2018.

286 b) The DOTS shall add an entry to the "creds" array to the new Device's "/oic/sec/cred"
287 Resource, identified as a symmetric pair-wise key, with an empty "privatedata" Properties,
288 and with the value of the "subjectuuid" Property set to the value of "devowneruuid" Property
289 of the "/oic/sec/doxm" Resource. See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of
290 such a request.

291 c) Upon receipt of the DOTS's symmetric Owner Credential, the new Device independently
292 generates the Shared Key using the SharedKey Credential Calculation method described in
293 clause 7.3.2 of ISO/IEC 30118-2:2018 and stores it with the Owner Credential.

294 11) The following steps are applied subsequent to successful establishment of ownership
295 credentials, and prior to transitioning to RFPRO. These steps may occur in any order.

296 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/doxm" Resource with the
297 UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has
298 "oic.d.dots" value in "rt" Property of its "oic/d" Resource. The DOTS shall expose "oic.d.dots"
299 value in "rt" Property of its "/oic/d" Resource.

300 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/pstat" Resource with the
301 UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has
302 "oic.d.dots" value in "rt" Property of its "oic/d" Resource. The DOTS shall expose "oic.d.dots"
303 value in "rt" Property of its "/oic/d" Resource.

304 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the
305 UUID of the CMS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has
306 "oic.d.dots" value in "rt" Property of its "oic/d" Resource. The DOTS shall expose "oic.d.dots"
307 value in "rt" Property of its "/oic/d" Resource.

308 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/acl2" Resource with the
309 UUID of the AMS. The DOTS shall only do so, if the OCF Device, which hosts AMS has
310 "oic.d.ams" value in "rt" Property of its "oic/d" Resource. The AMS shall expose "oic.d.ams"
311 value in "rt" Property of its "/oic/d" Resource.

312 – The DOTS shall update the "owned" Property of the "/oic/sec/doxm" Resource with value
313 "true".

314 – The DOTS shall provision the "/oic/sec/cred" Resource with credentials that enable secure
315 connections between OCF Services (e.g. DOTS, CMS, AMS, Mediator) and the new Device.
316 The DOTS shall provision credentials according to the supported credential types shown in
317 the "sct" Property of the "/oic/sec/doxm" Resource.

318 – The DOTS may UPDATE the "/oic/sec/acl2" Resource with ACEs and may UPDATE the
319 "/oic/sec/cred" Resource with further credentials.

320 – If the provisioned Device exposes "/oic/sec/sdi" Resource then an OBT hosting DOTS shall:
321 – Provision "uuid" Property of "/oic/sec/sdi" Resource with OCF Security Domain UUID.
322 If the OCF Security Domain UUID has not been derived yet, the DOTS shall generate
323 the UUID value randomly. DOTS shall use the same UUID value when onboarding a
324 Device into the same OCF Security Domain.

325 – Provision "name" Property of "/oic/sec/sdi" Resource with a human readable name,
326 received from an OCF Security Domain Owner. The DOTS should implement a user
327 interface to receive this information, when a new OCF Security Domain is being created.
328 If no user interface is implemented the DOTS should provision a copy of the "/oic/d:n"
329 of the DOTS.

330 – Provision "priv" Property of "/oic/sec/sdi" Resource with the value selected by the OCF
331 Security Domain Owner or preconfigured by the manufacturer. The DOTS should
332 implement a user interface to receive this information.

333 NOTE: When the Device is an OCF v1.3 Device, the DOTS is expected to send an UPDATE request to /oic/sec/doxm to
334 change the value of "owned" to true.

335 12) To transition the Device to RFPRO, the DOTS sends an UPDATE request changing the "dos.s"
336 Property of the "/oic/sec/pstat" Resource to RFPRO.

337 5.3.2 DOTS and Bridging

338 Bridge Platforms, their Bridge and VOD components are specified in ISO/IEC 30118-3:2018.
339 Bridges and VODs are individually onboarded to an OCF Security Domain. Unowned VODs on a

340 Bridge Platform are not discoverable while the Bridge on that Bridge Platform is Unowned. In other
341 words, the VODs can only be onboarded while the Bridge is Owned. The implication is that the
342 DOTS onboards the Bridge first, and then onboard the VODs. For details, see ISO/IEC 30118-
343 3:2018.

344 **5.3.3 Security considerations regarding selecting an Ownership Transfer Method**

345 A DOTS and/or DOTS operator might have strict requirements for the list of OTMs that are
346 acceptable when transferring ownership of a new Device. Some of the factors to be considered
347 when determining those requirements are:

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

351 For example, the operator of a DOTS might require that all of the Devices being onboarded support
352 either the Random PIN based OTM or the Manufacturer Certificate based OTM.

353 **5.4 CMS**

354 An introduction to the credential management is provided in clause 5.4.3 of ISO/IEC 30118-2:2018.

355 The credential types are specified in clause 9.3 of ISO/IEC 30118-2:2018.

356 The supported credential types with which the Device can be provisioned are provided in the "sct"
357 Property of the "/oic/sec/doxm" Resource. The CMS shall provision credentials according to the
358 credential types supported.

359 NOTE: The value of "sct" has no correlation to supported OTMs.

360 The CMS shall support adding certificate entries ("credtype" value of "8") to the "creds" Property
361 to the "/oic/sec/cred" Resource as defined in clause 13.3 of ISO/IEC 30118-2:2018. The CMS shall
362 support removing entries from the "creds" Property to the "/oic/sec/cred" Resource as defined in
363 clause 13.3 of ISO/IEC 30118-2:2018. The CMS may support changing existing entries in the
364 "creds" Property to the "/oic/sec/cred" Resource as defined in 13.3 of ISO/IEC 30118-2:2018.

365 Certificate provisioning of local Credentials is described in clause 9.4.5 of ISO/IEC 30118-2:2018.
366 The following points are pertinent to the CMS

- 367 – The CMS has its own CA certificate and key pair. The certificate is either a) self-signed if it acts
368 as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either
369 case, the certificate has the format described in clause 9.4.2 of ISO/IEC 30118-2:2018.
- 370 – The CMS shall support issuing an identity certificate for the Device as described in clause 6.1.
- 371 – The CMS shall support issuing role certificates as described in clause 6.1.
- 372 – When issuing a role certificate or an identity certificate, the CMS shall include a string of format
373 "uuid:X" in the Common Name component of the Subject Name of the issued certificate, where
374 X is provisioned to match the "deviceuuid" Property of the "/oic/sec/doxm" Resource.
- 375 – The CMS shall support provisioning a Trust Anchor as described in clause 6.2.

376 CRL provisioning is specified in clause 9.4.6 of ISO/IEC 30118-2:2018, using the "/oic/sec/crl"
377 Resource specified in clause 13.4 of ISO/IEC 30118-2:2018. The issuing CMS issues the certificate
378 revocation lists for certificates it issues. If a certificate private key is compromised, the CMS
379 revokes the certificate. If CRLs are used by a Device, the CMS is expected to regularly (for example;
380 every 3 months) update the "/oic/sec/crl" resource for the Devices it manages.

381 An introduction to Role Management is provided in clause 5.4.3 of ISO/IEC 30118-2:2018.

382 **5.5 AMS**

383 The AMS shall support adding entries to the "aclist2" Property of the "/oic/sec/acl2" Resource as
384 defined in clause 13.5 of ISO/IEC 30118-2:2018.

385 The AMS shall support removing existing entries in the "aclist2" Property of the "/oic/sec/acl2"
386 Resource as defined in clause 13.5 of ISO/IEC 30118-2:2018.

387 The AMS may support changing existing entries in the "aclist2" Property of the "/oic/sec/acl2"
388 Resource as defined in 13.5 of ISO/IEC 30118-2:2018.

389 The AMS should support other operations as defined in clause 13.5 of ISO/IEC 30118-2:2018.

390 Clause 6.2 of Cloud Security Specification provides normative requirements on the AMS when
391 configuring ACE entries of a Device which supports OCF Cloud.

392 The AMS determines an appropriate ACL configuration for each Server based on the rules for ACL
393 evaluation and enforcement at Servers specified in clause 12 of ISO/IEC 30118-2:2018. The
394 formatting of the ACL Resource specified in clause 13.5 of ISO/IEC 30118-2:2018.

395 To support homogenous behaviour across OCF ecosystem, AMS can provision explicit ACL entries
396 to legacy devices based on the value of "icv" Property of "/oic/d" Resource, so that they recognize
397 default "oic.role.*" Roles added in later releases. Table 2 enumerates the list of Roles and their
398 access policies to provision per each version.

399 **Table 2 – ACL entries to provision for role usage uniformity**

Version	Role	Access Policy: Permission	Access Policy: Resource	Description
"2.4.0" and prior	"oic.role.owner"	-RU--	All SVRs	Grant right to perform all supported operations on all supported SVRs

400

401 **6 Certificate management requirements**

402 **6.1 Issuing identity certificates and role certificates**

403 A CMS shall perform the following steps to issue an identity certificate or role certificate to a Device.

- 404 1) If the Device has the "/oic/sec/csr" Resource, then
- 405 a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to
406 obtain a certificate signing request for which the CMS will create a certificate.
 - 407 b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing
408 request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-
409 2:2018.
- 410 2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise
411 obtain) a certificate chain using the using a public key pair generated by the CMS, and
412 complying with clause 9.4.2 of ISO/IEC 30118-2:2018.
- 413 3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the
414 "/oic/sec/cred" Resource of the Device meeting the following criteria:
- 415 – The "subjectuuid" Property shall have the value of "deviceuuid" Property of the
416 "/oic/sec/doxm" Resource.
 - 417 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key
418 with Certificate.

419 – The "credusage" Property shall have the value of "oic.sec.cred.cert" or
420 "oic.sec.cred.rolecert" corresponding to an identity certificate or role certificate as
421 respectively.

422 – The "publicdata" Property shall contain the newly-created certificate chain.

423 See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of a request adding an entry to the "creds"
424 Property of the "/oic/sec/cred" Resource.

425 **6.2 Provisioning Trust Anchor certificates**

426 To provision a Trust Anchor certificate to a Device, a CMS shall send a request to the Device to
427 add an entry to the "creds" Property of the "/oic/sec/cred" Resource of the Device meeting the
428 following criteria:

429 – The "subjectuid" Property shall have the value of "*" (matching all identities) or a specific UUID
430 (matching a single identity).

431 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with
432 Certificate

433 – The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a
434 certificate Trust Anchor

435 – The "publicdata" Property shall contain the Trust Anchor certificate.

436 See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of a request adding an entry to the "creds"
437 Property of the "/oic/sec/cred" Resource.

438 **7 Ownership Transfer Methods**

439 **7.1 Preamble**

440 OTM Implementation requirements are discussed in clause 7.3.1 of ISO/IEC 30118-2:2018.

441 **7.2 Just Works Owner Transfer Method**

442 This OTM is specified in clause 7.3.4.1 of ISO/IEC 30118-2:2018.

443 All DOTS shall implement the mandatory ciphersuites and should implement the optional
444 ciphersuites for Devices specified for this OTM in clause 11.3.2.1 of ISO/IEC 30118-2:2018.

445 Security considerations for this OTM are provided in clause 7.3.4.2 of ISO/IEC 30118-2:2018.

446 **7.3 Random PIN / Shared Credential based Owner Transfer Method**

447 Details of this OTM are provided in clause 7.3.5 of ISO/IEC 30118-2:2018. The following points are
448 pertinent to the DOTS:

449 – This OTM relies on the Device generating a random number that is communicated to the DOTS
450 over an Out of Band Communication Channel.

451 – The Platform hosting a DOTS which supports this OTM shall provide a user interface for
452 manual input of the random number.

453 – A DOTS may support other vendor-defined Out of Band Communication Channel for
454 receiving the random number from the Device. Security considerations regarding Out of
455 Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.

456 – When the DOTS receives the ServerKeyExchange, then the DOTS can identify the new Device
457 with which it is establishing the DOC by matching the "psk_identity_hint" field of the
458 ServerKeyExchange message in the DTLS handshake with the "deviceuuid" Property of the
459 "/oic/sec/doxm" Resource being sent in responses when the new Device is in RFOTM and when
460 a Device Onboarding Connection is not currently established. The DOTS shall compute the

461 PIN-authenticated pre-shared key (PPSK) using the algorithm specified in clause 7.3.5.2 of
462 ISO/IEC 30118-2:2018.

463 Furthermore, the following requirements apply to the DTLS handshake messages for this OTM:

- 464 – The DOTS shall set the "psk_identity" field of the ClientKeyExchange message to the string
465 "oic.sec.doxm.rdp".

466 NOTE: The string "oic.sec.doxm.rdp" is the URN defined for the Random PIN-based OTM in Table 18 of ISO/IEC 30118-
467 2:2018, and is included to allow future OTMs to re-use the DTLS ciphersuites without confusion about which OTM should
468 be applied.

469 All DOTS shall implement the mandatory ciphersuites and should implement the optional
470 ciphersuites for Devices specified for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2:2018.

471 Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-
472 2:2018.

473 **7.4 Manufacturer Certificate Based Owner Transfer Method**

474 Details of this OTM are provided in clause 7.3.6 of ISO/IEC 30118-2:2018. The following points are
475 pertinent to the DOTS:

- 476 – The DOTS shall validate the certificate presented by the Device in the DTLS handshake against
477 the Trust Anchors contained in its entries of the "/oic/sec/cred" Resource that have a
478 "credusage" Property populated with "oic.sec.cred.mfgtrustca".

- 479 – The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2:2018.

480 All DOTS shall implement the mandatory and optional ciphersuites for Devices specified for this
481 OTM in clause 11.3.2.3 of ISO/IEC 30118-2:2018.

482 Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses
483 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2:2018.

484 **7.5 Vendor-Specific Owner Transfer Methods**

485 Clauses 7.3.1 and 7.3.7 of ISO/IEC 30118-2:2018 provide requirements for Vendor-specific OTMs.