

OCF Onboarding Tool Specification

VERSION 2.1.0 | November 2019



OPEN CONNECTIVITY
FOUNDATION™

CONTACT admin@openconnectivity.org

Copyright Open Connectivity Foundation, Inc. © 2019.
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 © 2017-2019 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 8

32 5.4 CMS 9

33 5.5 AMS..... 9

34 6 Certificate management requirements 10

35 6.1 Issuing identity certificates and role certificates 10

36 6.2 Provisioning Trust Anchor certificates 10

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 OTM 11

41 7.4 Manufacturer Certificate Based Owner Transfer Method 11

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 – Informative overview of OBT access in Device Onboarding States6

49

50

51 **1 Scope**

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

55 **2 Normative References**

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

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

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

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

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

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

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

84

85 **3 Terms, definitions, and abbreviated terms**

86 **3.1 Terms and definitions**

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

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

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

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

93 **3.1.1**

94 **Access Control Entry**

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

96 **3.1.2**

97 **Access Control List**

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

99 **3.1.3**

100 **Access Management Service (AMS)**

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

102 **3.1.4**

103 **Bridge**

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

105 **3.1.5**

106 **Client**

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

108 **3.1.6**

109 **Credential Management Service (CMS)**

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

111 **3.1.7**

112 **Device**

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

114 **3.1.8**

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

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

117 **3.1.9**

118 **End User**

119 The person using the [particular] product

120 **3.1.10**

121 **(OCF) Onboarding**

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

123 **3.1.11**

124 **Onboarding Tool (OBT)**

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

126 **3.1.12**

127 **Out of Band Communication Channel**

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

129 **3.1.13**
130 **Owned (or "in Owned State")**
131 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

132 **3.1.14**
133 **Owner Credential**
134 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

135 **3.1.15**
136 **Property**
137 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

138 **3.1.16**
139 **Resource**
140 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

141 **3.1.17**
142 **OCF Security Domain**
143 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

144 **3.1.18**
145 **Owner Transfer Method**
146 Note 1 to entry: See ISO/IEC 30118-2:2018.

147 **3.1.19**
148 **Security Virtual Resource (SVR)**
149 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

150 **3.1.20**
151 **Server**
152 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

153 **3.1.21**
154 **Trust Anchor**
155 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

156 **3.1.22**
157 **Unowned (or "in Unowned State")**
158 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

159 **3.1.23**
160 **Virtual OCF Device**
161 Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

162 **3.2 Abbreviated terms**

163 **3.2.1**
164 **ACE**
165 Access Control Entry
166 Note 1 to entry: See ISO/IEC 30118-2:2018.

167 **3.2.2**
168 **ACL**
169 Access Control List
170 Note 1 to entry: See ISO/IEC 30118-2:2018.

171 **3.2.3**
172 **AMS**
173 Access Management Service

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

175 **3.2.4**

176 **CMS**

177 Credential Management Service

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

179 **3.2.5**

180 **OBT**

181 Onboarding Tool

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

183 **3.2.6**

184 **OTM**

185 Owner Transfer Method

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

187 **3.2.7**

188 **PIN**

189 Personal Identification Number

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

191 **3.2.8**

192 **PPSK**

193 PIN-authenticated pre-shared key

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

195 **3.2.9**

196 **SVR**

197 Security Virtual Resource

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

199 **3.2.10**

200 **VOD**

201 Virtual OCF Device

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

203 **4 Document Conventions and Organization**

204 See ISO/IEC 30118-1:2018.

205 **5 Services and Availability in the OBT**

206 **5.1 Purpose of the OBT**

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

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

218 The following OBT functions are specified:

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

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

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

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

Table 1 – Informative overview of OBT access in Device Onboarding States

Device Onboarding State	Description		Applicable Resources & Access	Entity Authorized to READ/WRITE	Purpose
RESET	Full reset of OCF Device to manufacturer default. Unowned		No Access	No Access	Remove info in SVRs.
RFOTM	Ready for Ownership Transfer Mechanism. Unowned	Prior to successful OTM	"/oic/sec/doxm" (R: all, W: oxmsel)	Any	R: Determine supported OTMs W: Select an OTM
		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. Owned.		"/oic/sec/cred" (RW)	CMS or matching ACE	Establish credentials for authenticating Devices in normal operation, including Roles
			"/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. Owned.		"/oic/sec/pstat"	DOTS, CMS, AMS or matching ACE	Transition to RFPRO, SRESET or RESET
			Vertical Resources	Matching ACE	Normal Operation
SRESET	Soft RESET. Owned		"/oic/sec/cred" (RW)	CMS	Corrections as needed
			"/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

239

240 5.2 General OBT requirements

241 An OBT shall be hosted on an OCF Device.

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

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

244 The software of an OBT shall be field updatable. (This requirement need not be tested but can be
245 certified via a vendor declaration.)

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

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

252 The OBT is expected to support all mandatory and optional ciphersuites in clauses 11.3.3 and
253 11.3.4 of ISO/IEC 30118-2:2018.

254 **5.3 DOTS**

255 **5.3.1 Assuming ownership of a Device**

256 The DOTS shall support all OTMs in clause 7.

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

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

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

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

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

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

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

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

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

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

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

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

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

284 b) The DOTS shall add an entry to the "creds" array to the new Device's "/oic/sec/cred"
285 Resource, identified as a symmetric pair-wise key, with an empty "privatedata" Properties,
286 and with the value of the "subjectuuid" Property set to the value of "devowneruuid" Property

287 of the "/oic/sec/doxm" Resource. See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of
288 such a request.

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

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

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

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

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

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

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

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

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

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

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

322 5.3.2 DOTS and Bridging

323 Bridge Platforms, their Bridge and VOD components are specified in ISO/IEC 30118-3:2018.
324 Bridges and VODs are individually onboarded to an OCF Security Domain. Unowned VODs on a
325 Bridge Platform are not discoverable while the Bridge on that Bridge Platform is Unowned. In other
326 words, the VODs can only be onboarded while the Bridge is Owned. The implication is that the
327 DOTS onboards the Bridge first, and then onboard the VODs. For details, see ISO/IEC 30118-
328 3:2018.

329 5.3.3 Security considerations regarding selecting an Ownership Transfer Method

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

333 – The security considerations described for each of the OTMs.

334 – The probability that a man-in-the-middle attacker might be present in the environment used to
335 perform the ownership transfer.

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

338 **5.4 CMS**

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

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

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

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

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

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

352 – The CMS has its own CA certificate and key pair. The certificate is either a) self-signed if it acts
353 as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either
354 case, the certificate has the format described in clause 9.4.2 of ISO/IEC 30118-2:2018.

355 – The CMS shall support issuing an identity certificate for the Device as described in clause 6.1.

356 – The CMS shall support issuing role certificates as described in clause 6.1.

357 – The CMS shall support provisioning a Trust Anchor as described in clause 6.2.

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

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

364 **5.5 AMS**

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

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

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

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

372 Clause 6.2 of ISO/IEC 30118-X:2018 provides normative requirements on the AMS when
373 configuring ACE entries of a Device which supports OCF Cloud.

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

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

381 **Table X – 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

382

383 **6 Certificate management requirements**

384 **6.1 Issuing identity certificates and role certificates**

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

- 386 1) If the Device has the "/oic/sec/csr" Resource, then
- 387 a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to
 388 obtain a certificate signing request for which the CMS will create a certificate.
- 389 b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing
 390 request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-
 391 2:2018.
- 392 2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise
 393 obtain) a certificate chain using the using a public key pair generated by the CMS, and
 394 complying with clause 9.4.2 of ISO/IEC 30118-2:2018.
- 395 3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the
 396 "/oic/sec/cred" Resource of the Device meeting the following criteria:
- 397 – The "subjectuuid" Property shall have the value of "deviceuuid" Property of the
 398 "/oic/sec/doxm" Resource
 - 399 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key
 400 with Certificate
 - 401 – The "credusage" Property shall have the value of "oic.sec.cred.cert" or
 402 "oic.sec.cred.rolecert" corresponding to a identity certificate or role certificate as
 403 respectively.
 - 404 – The "publicdata" Property shall contain the newly-created certificate chain.

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

407 **6.2 Provisioning Trust Anchor certificates**

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

- 411 – The "subjectuuid" Property shall have the value of "" (matching all identities) or a specific UUID
 412 (matching a single identity).

- 413 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with
414 Certificate
- 415 – The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a
416 certificate Trust Anchor
- 417 – The "publicdata" Property shall contain the Trust Anchor certificate.
- 418 See clause 13.3.1 of ISO/IEC 30118-2:2018 for details of a request adding an entry to the "creds"
419 Property of the "/oic/sec/cred" Resource.

420 **7 Ownership Transfer Methods**

421 **7.1 Preamble**

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

423 **7.2 Just Works Owner Transfer Method**

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

425 All DOTS are expected to implement the following ciphersuites:

- 426 – The mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.1
427 of ISO/IEC 30118-2:2018, and
- 428 – The OCF-defined vendor-specific ciphersuites (these were used prior to the IETF specifying
429 the ciphersuites listed in clause 11.3.2.1 of ISO/IEC 30118-2:2018):
- 430 – TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256 (with the value 0xFF00).
- 431 – TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256 (with the value 0xFF01).

432

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

434 **7.3 Random PIN / Shared Credential based OTM**

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

- 437 – This OTM relies on the Device generating a random number that is communicated to the DOTS
438 over an Out of Band Communication Channel.
- 439 – The Platform hosting a DOTS which supports this OTM shall provide a user interface for
440 manual input of the random number.
- 441 – A DOTS may support other vendor-defined Out of Band Communication Channel for
442 receiving the random number from the Device. Security considerations regarding Out of
443 Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.
- 444 – The DOTS shall compute the PIN-authenticated pre-shared key (PPSK) using the algorithm
445 specified in clause 7.3.5.2 of ISO/IEC 30118-2:2018.

446 All DOTS are expected to implement the mandatory and optional ciphersuites for Devices specified
447 for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2:2018.

448 Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-
449 2:2018.

450 **7.4 Manufacturer Certificate Based Owner Transfer Method**

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

453 - The DOTS shall validate the certificate presented by the Device in the TLS Handshake against
454 the Trust Anchors contained in its entries of the "/oic/sec/cred" Resource that have a
455 "credusage" Property populated with "oic.sec.cred.mfgtrustca".

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

457 All DOTS are expected to implement the mandatory and optional ciphersuites for Devices specified
458 for this OTM in clause 11.3.2.3 of ISO/IEC 30118-2:2018.

459 Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses
460 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2:2018.

461 **7.5 Vendor-Specific Owner Transfer Methods**

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