

# OCF Onboarding Tool Specification

VERSION 2.0.5 | September 2019



**OPEN** CONNECTIVITY  
FOUNDATION™

CONTACT [admin@openconnectivity.org](mailto: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 ..... 8

33 5.5 AMS..... 9

34 6 Certificate management requirements ..... 9

35 6.1 Issuing identity certificates and role certificates ..... 9

36 6.2 Provisioning Trust Anchor certificates ..... 10

37 7 Ownership Transfer Methods ..... 10

38 7.1 Preamble ..... 10

39 7.2 Just Works Owner Transfer Method ..... 10

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 ..... 11

43

44 **FIGURES**

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

46

47 **Tables**

48 Table 1 – Informative overview of OBT access in Device Onboarding States .....6

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](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](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](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](https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf)

78 Open Connectivity Foundation (OCF) Specification – Cloud Security Specification  
79 Latest version available at:  
80 [https://openconnectivity.org/specs/OCF\\_Cloud\\_Security\\_Specification.pdf](https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf)

81

## 82 **3 Terms, definitions, and abbreviated terms**

### 83 **3.1 Terms and definitions**

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

86 ISO and IEC maintain terminological databases for use in standardization at the following  
87 addresses:

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

#### 90 **3.1.1** 91 **Access Control Entry**

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

#### 93 **3.1.2** 94 **Access Control List**

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

#### 96 **3.1.3** 97 **Access Management Service (AMS)**

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

#### 99 **3.1.4** 100 **Bridge**

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

#### 102 **3.1.5**

#### 103 **3.1.6** 104 **Client**

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

#### 106 **3.1.7** 107 **Credential Management Service (CMS)**

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

#### 109 **3.1.8** 110 **Device**

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

#### 112 **3.1.9** 113 **Device Ownership Transfer Service (DOTS)**

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

#### 115 **3.1.10** 116 **End User**

117 The person using the [particular] product

#### 118 **3.1.11** 119 **(OCF) Onboarding**

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

#### 121 **3.1.12** 122 **Onboarding Tool (OBT)**

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

124 **3.1.13**  
125 **Out of Band Communication Channel**  
126 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

127 **3.1.14**  
128 **Owned (or "in Owned State")**  
129 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

130 **3.1.15**  
131 **Owner Credential**  
132 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

133 **3.1.16**  
134 **Property**  
135 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

136 **3.1.17**  
137 **Resource**  
138 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

139 **3.1.18**  
140 **OCF Security Domain**  
141 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

142 **3.1.19**  
143 **Owner Transfer Method**  
144 Note 1 to entry: See ISO/IEC 30118-2:2018.

145 **3.1.20**  
146 **Security Virtual Resource (SVR)**  
147 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

148 **3.1.21**  
149 **Server**  
150 Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

151 **3.1.22**  
152 **Trust Anchor**  
153 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

154 **3.1.23**  
155 **Unowned (or "in Unowned State")**  
156 Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

157 **3.1.24**  
158 **Virtual OCF Device**  
159 Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

160 **3.2 Abbreviated terms**

161 **3.2.1**  
162 **ACE**  
163 Access Control Entry  
164 Note 1 to entry: See ISO/IEC 30118-2:2018.

165 **3.2.2**  
166 **ACL**  
167 Access Control List  
168 Note 1 to entry: See ISO/IEC 30118-2:2018.

169 **3.2.3**  
170 **AMS**  
171 Access Management Service

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

173 **3.2.4**  
174 **CMS**  
175 Credential Management Service

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

177 **3.2.5**  
178 **OBT**  
179 Onboarding Tool

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

181 **3.2.6**  
182 **OTM**  
183 Owner Transfer Method

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

185 **3.2.7**  
186 **PIN**  
187 Personal Identification Number

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

189 **3.2.8**  
190 **PPSK**  
191 PIN-authenticated pre-shared key

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

193 **3.2.9**  
194 **SVR**  
195 Security Virtual Resource

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

197 **3.2.10**  
198 **VOD**  
199 Virtual OCF Device

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

201 **4 Document Conventions and Organization**

202 See ISO/IEC 30118-1:2018.



## 203 **5 Services and Availability in the OBT**

### 204 **5.1 Purpose of the OBT**

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

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

216 The following OBT functions are specified:

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

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

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

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

237

**238 5.2 General OBT requirements**

239 An OBT shall be hosted on an OCF Device.

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

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

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

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

247 The OBT is expected to support all mandatory and optional ciphersuites in clauses 11.3.3 and  
248 11.3.4 of ISO/IEC 30118-2:2018.

## 249 **5.3 DOTS**

### 250 **5.3.1 Assuming ownership of a Device**

251 The DOTS shall support all OTMs in clause 7.

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

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

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

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

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

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

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

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

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

270 8) The DOTS shall RETRIEVE the updated "deviceuuid" Property of the "/oic/sec/doxm" Resource  
271 after the DOTS has updated the "devowneruuid" Property value of the "/oic/sec/doxm"  
272 Resource to a non-nil-UUID value.

273 9) The DOTS may update the "deviceuuid" of the "/oic/sec/doxm" Resource to a value that the  
274 DOTS has selected.

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

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

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

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

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

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

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

296 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the  
297 UUID of the CMS. 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/acl2" Resource with the  
301 UUID of the AMS. The DOTS shall only do so, if the OCF Device, which hosts AMS has  
302 "oic.d.ams" value in "rt" Property of its "oic/d" Resource. The AMS shall expose "oic.d.ams"  
303 value in "rt" Property of its "/oic/d" Resource.

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

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

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

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

### 314 5.3.2 DOTS and Bridging

315 Bridge Platforms, their Bridge and VOD components are specified in ISO/IEC 30118-3:2018.  
316 Bridges and VODs are individually onboarded to an OCF Security Domain. Unowned VODs on a  
317 Bridge Platform are not discoverable while the Bridge on that Bridge Platform is Unowned. In other  
318 words, the VODs can only be onboarded while the Bridge is Owned. The implication is that the  
319 DOTS onboard the Bridge first, and then onboard the VODs. For details, see ISO/IEC 30118-  
320 3:2018.

### 321 5.3.3 Security considerations regarding selecting an Ownership Transfer Method

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

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

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

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

## 330 5.4 CMS

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

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

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

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

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

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

- 344 – The CMS has its own CA certificate and key pair. The certificate is either a) self-signed if it acts  
345 as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either  
346 case, the certificate has the format described in clause 9.4.2 of ISO/IEC 30118-2:2018.
- 347 – The CMS shall support issuing an identity certificate for the Device as described in clause 6.1.
- 348 – The CMS shall support issuing role certificates as described in clause 6.1.
- 349 – The CMS shall support provisioning a Trust Anchor as described in clause 6.2.

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

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

## 356 **5.5 AMS**

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

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

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

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

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

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

## 369 **6 Certificate management requirements**

### 370 **6.1 Issuing identity certificates and role certificates**

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

372 1) If the Device has the "/oic/sec/csr" Resource, then

- 373 a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to  
374 obtain a certificate signing request for which the CMS will create a certificate.
- 375 b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing  
376 request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-  
377 2:2018.
- 378 2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise  
379 obtain) a certificate chain using the using a public key pair generated by the CMS, and  
380 complying with clause 9.4.2 of ISO/IEC 30118-2:2018.
- 381 3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the  
382 "/oic/sec/cred" Resource of the Device meeting the following criteria:
- 383 – The "subjectuuid" Property shall have the value of "deviceuuid" Property of the  
384 "/oic/sec/doxm" Resource
  - 385 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key  
386 with Certificate
  - 387 – The "credusage" Property shall have the value of "oic.sec.cred.cert" or  
388 "oic.sec.cred.rolecert" corresponding to a identity certificate or role certificate as  
389 respectively.
  - 390 – The "publicdata" Property shall contain the newly-created certificate chain.

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

## 393 **6.2 Provisioning Trust Anchor certificates**

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

- 397 – The "subjectuuid" Property shall have the value of "\*" (matching all identities) or a specific UUID  
398 (matching a single identity).
- 399 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with  
400 Certificate
- 401 – The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a  
402 certificate Trust Anchor
- 403 – The "publicdata" Property shall contain the Trust Anchor certificate.

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

## 406 **7 Ownership Transfer Methods**

### 407 **7.1 Preamble**

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

### 409 **7.2 Just Works Owner Transfer Method**

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

411 All DOTS are expected to implement the following ciphersuites:

- 412 – The mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.1  
413 of ISO/IEC 30118-2:2018, and
- 414 – The OCF-defined vendor-specific ciphersuites (these were used prior to the IETF specifying  
415 the ciphersuites listed in clause 11.3.2.1 of ISO/IEC 30118-2:2018):

- 416 – TLS\_ECDH\_ANON\_WITH\_AES\_128\_CBC\_SHA256 (with the value 0xFF00).
- 417 – TLS\_ECDH\_ANON\_WITH\_AES\_256\_CBC\_SHA256 (with the value 0xFF01).

418

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

### 420 **7.3 Random PIN / Shared Credential based OTM**

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

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

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

434 Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-  
435 2:2018.

### 436 **7.4 Manufacturer Certificate Based Owner Transfer Method**

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

- 439 – The DOTS shall validate the certificate presented by the Device in the TLS Handshake against  
440 the Trust Anchors configured to the DOTS.
- 441 – The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2:2018.

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

444 Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses  
445 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2:2018.

### 446 **7.5 Vendor-Specific Owner Transfer Methods**

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