

OCF Onboarding Tool Specification

VERSION 2.2.7 | November 2023



CONTACT admin@openconnectivity.org
Copyright Open Connectivity Foundation, Inc. © 2023.
All Rights Reserved.

LEGAL DISCLAIMER

2
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 © 2017-2022 Open Connectivity Foundation, Inc. All rights reserved.

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

CONTENTS

18		
19	Introduction.....	iv
20	1 Scope.....	1
21	2 Normative References	1
22	3 Terms, definitions, and abbreviated terms	2
23	3.1 Terms and definitions.....	2
24	3.2 Symbols and abbreviated terms	2
25	4 Document conventions and organization.....	2
26	4.1 Conventions.....	2
27	4.2 Notation.....	2
28	4.3 Data types	3
29	5 Services and availability in the OBT	4
30	5.1 Purpose of the OBT	4
31	5.2 General OBT requirements	5
32	5.3 DOTS	6
33	5.3.1 Assuming ownership of a Device	6
34	5.3.2 DOTS and bridging.....	7
35	5.3.3 Security considerations regarding selecting an Ownership Transfer Method	8
36	5.4 CMS	8
37	5.5 AMS.....	8
38	6 Certificate management requirements	9
39	6.1 Issuing identity certificates and role certificates	9
40	6.2 Provisioning Trust Anchor certificates	10
41	6.3 Provisioning an OSCORE Security Context for End-to-End security of unicast	
42	messages	10
43	6.4 Provisioning Clients and Servers in a Simple Secure Multicast Group.....	11
44	7 Ownership Transfer Methods.....	13
45	7.1 Preamble	13
46	7.2 Just Works Owner Transfer Method	13
47	7.3 Random PIN / Shared Credential based Owner Transfer Method	13
48	7.4 Manufacturer Certificate Based Owner Transfer Method	13
49	7.5 Vendor-Specific Owner Transfer Methods	14
50	Bibliography.....	14
51		

Tables

52	
53	Table 1 – Overview of OBT access in Device Onboarding states5
54	Table 2 – ACL entries to provision for role usage uniformity.....9
55	
56	

57 **Introduction**

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

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

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

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

76 The OCF specification suite is made up of nineteen discrete documents, the documents fall into
77 logical groupings as described herein:

- 78 – Core framework
 - 79 – Core Specification
 - 80 – Security Specification
 - 81 – Onboarding Tool Specification
- 82 – Bridging framework and bridges
 - 83 – Bridging Specification
 - 84 – Resource to Alljoyn Interface Mapping Specification
 - 85 – OCF Resource to oneM2M Resource Mapping Specification
 - 86 – OCF Resource to BLE Mapping Specification
 - 87 – OCF Resource to EnOcean Mapping Specification
 - 88 – OCF Resource to LWM2M Mapping Specification
 - 89 – OCF Resource to UPlus Mapping Specification
 - 90 – OCF Resource to Zigbee Cluster Mapping Specification
 - 91 – OCF Resource to Z-Wave Mapping Specification
- 92 – Resource and Device models
 - 93 – Resource Type Specification
 - 94 – Device Specification
- 95 – Core framework extensions
 - 96 – Easy Setup Specification
 - 97 – Core Optional Specification
- 98 – OCF Cloud
 - 99 – Cloud API for Cloud Services Specification

- 100 – Device to Cloud Services Specification
- 101 – Cloud Security Specification

OCF Onboarding Tool Specification

102

103 **1 Scope**

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

107 **2 Normative References**

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

112 ISO/IEC 30118-1, *Information technology – Open Connectivity Foundation (OCF) Specification –*
113 *Part 1: Core specification*

114 <https://www.iso.org/standard/53238.html>

115 Latest version available at:

116 https://openconnectivity.org/specs/OCF_Core_Specification.pdf

117 ISO/IEC 30118-2, *Information technology – Open Connectivity Foundation (OCF) Specification –*
118 *Part 2: Security specification*

119 <https://www.iso.org/standard/74239.html>

120 Latest version available at: https://openconnectivity.org/specs/OCF_Security_Specification.pdf

121 NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation
122 Using Deterministic Random Bit Generators

123 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>

124

125 **3 Terms, definitions, and abbreviated terms**

126 **3.1 Terms and definitions**

127 For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1,
128 ISO/IEC 30118-2 and [1] apply.

129 ISO and IEC maintain terminological databases for use in standardization at the following
130 addresses:

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

133 **3.2 Symbols and abbreviated terms**

134 For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 30118-1,
135 ISO/IEC 30118-2 and [1] apply.

136 **4 Document conventions and organization**

137 **4.1 Conventions**

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

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

145 **4.2 Notation**

146 In this document, features are described as required, recommended, allowed or DEPRECATED as
147 follows:

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

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

152 Recommended (or should)(S).

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

159 Allowed (may or allowed)(O).

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

163 DEPRECATED.

- 164 – Although these features are still described in this document, they should not be implemented
165 except for backward compatibility. The occurrence of a deprecated feature during operation of
166 an implementation compliant with the current document has no effect on the implementation's

167 operation and does not produce any error conditions. Backward compatibility may require that
168 a feature is implemented and functions as specified but it shall never be used by
169 implementations compliant with this document.

170 Conditionally allowed (CA).

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

173 Conditionally required (CR).

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

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

178 Words that are emphasized are printed in italic.

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

183 **4.3 Data types**

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

186 **5 Services and availability in the OBT**

187 **5.1 Purpose of the OBT**

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

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

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

202 The following OBT functions are specified:

- 203 – A Device Ownership Transfer Service (DOTS) establishes ownership of Devices being added
204 to the OCF Security Domain. This function is described in clause 5.3.
- 205 – A Credential Management Service (CMS) manages the credentials and Roles of Devices in the
206 OCF Security Domain. This function is described in clause 5.4.
- 207 – An Access Management Service (AMS) manages the access of Devices in the OCF Security
208 Domain. This function is described in clause 5.5.
- 209 – Optional: A Mediator facilitates further configuration of Devices in the OCF Security Domain for
210 various purposes including Wi-Fi configuration (see [2]) and OCF Cloud access (see [3]).

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

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

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

221

222 5.2 General OBT requirements

223 An OBT shall be hosted on an OCF Device.

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

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

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

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

232 The OBT should support all mandatory and optional cipher suites in clauses 11.3.3 and 11.3.4 of
233 ISO/IEC 30118-2.

234 **5.3 DOTS**

235 **5.3.1 Assuming ownership of a Device**

236 The DOTS shall support all OTMs in clause 7.

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

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

240 1) The DOTS performs a multicast RETRIEVE on the "/oic/sec/doxm" Resource using
241 "owned=false" query parameter as described in ISO/IEC 30118-2.

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

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

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

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

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

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

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

258 9) The DOTS shall UPDATE the "deviceuuid" of the "/oic/sec/doxm" Resource. The updated value
259 shall be a value that the DOTS has generated. The DOTS should use a NIST Special
260 Publication 800-90A Revision 1-compliant RNG to guarantee sufficient entropy.

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

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

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

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

272 11) The following steps are applied subsequent to successful establishment of Owner Credential,
273 and prior to transitioning to RFPRO. These steps may occur in any order.

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

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

282 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the
283 UUID of the CMS. The DOTS shall only do so, if the OCF Device, which hosts CMS has
284 "oic.d.cms" value in "rt" Property of its "/oic/d" Resource. The CMS shall expose "oic.d.cms"
285 value in "rt" Property of its "/oic/d" Resource.

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

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

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

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

298 – If the provisioned Device exposes "/oic/sec/sdi" Resource, then an OBT hosting DOTS shall:

299 – Provision "uuid" Property of "/oic/sec/sdi" Resource with OCF Security Domain UUID.
300 If the OCF Security Domain UUID has not been derived yet, the DOTS shall generate
301 the UUID value randomly. DOTS shall use the same UUID value when Onboarding a
302 Device into the same OCF Security Domain.

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

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

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

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

315 5.3.2 DOTS and bridging

316 Bridge Platforms, their Bridge and VOD components are specified in [1]. Bridges and VODs are
317 individually onboarded to an OCF Security Domain. Unowned VODs on a Bridge Platform are not
318 discoverable while the Bridge on that Bridge Platform is Unowned. In other words, the VODs can
319 only be onboarded while the Bridge is Owned. The implication is that the DOTS onboard the
320 Bridge first, and then onboard the VODs. For details, see [1].

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.

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

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. 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. The CMS may support changing existing entries in the "creds"
341 Property to the "/oic/sec/cred" Resource as defined in 13.3 of ISO/IEC 30118-2.

342 Certificate provisioning of local Credentials is described in clause 9.4.5 of ISO/IEC 30118-2. The
343 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.
- 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 – When issuing a role certificate or an identity certificate, the CMS shall include a string of format
350 "uuid:X" in the Common Name component of the Subject Name of the issued certificate, where
351 X is provisioned to match the "deviceuuid" Property of the "/oic/sec/doxm" Resource.
- 352 – The CMS shall support provisioning a Trust Anchor as described in clause 6.2.

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

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

359 **5.5 AMS**

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

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

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

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

367 Clause 6.2 of [3] provides normative requirements on the AMS when configuring ACE entries of a
368 Device which supports OCF Cloud.

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

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

376 **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

377

378 **6 Certificate management requirements**

379 **6.1 Issuing identity certificates and role certificates**

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

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

382 a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to
383 obtain a certificate signing request for which the CMS will create a certificate.

384 b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing
385 request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-2.

386 2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise
387 obtain) a certificate chain using the using a public key pair generated by the CMS, and
388 complying with clause 9.4.2 of ISO/IEC 30118-2.

389 3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the
390 "/oic/sec/cred" Resource of the Device meeting the following criteria:

391 – The "subjectuud" Property shall have the value of "deviceuud" Property of the
392 "/oic/sec/doxm" Resource.

393 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key
394 with Certificate.

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

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

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

401 **6.2 Provisioning Trust Anchor certificates**

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

- 405 – The "subjectuid" Property shall have the value of "*" (matching all identities) or a specific UUID
406 (matching a single identity).
- 407 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with
408 Certificate
- 409 – The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a
410 certificate Trust Anchor
- 411 – The "publicdata" Property shall contain the Trust Anchor certificate.

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

414 **6.3 Provisioning an OSCORE Security Context for End-to-End security of unicast** 415 **messages**

416 ISO/IEC 30118-2 describes how Object Security for Constrained RESTful Environments (OSCORE)
417 protocol [4] is used for End-to-End Security of Unicast Messages.

418 OSCORE communication between two Devices is enabled by provisioning an OSCORE Security
419 Context in a credential entry of the "/oic/sec/cred" Resource in each of the two Devices. The present
420 clause provides the requirements on the CMS for this provisioning. For the purposes of this
421 description, let Device A and Device B denote the two Devices.

422 Prior to provisioning, the CMS generates three values: idA; idB; and an OSCORE Master Secret.

- 423 – The CMS selects a value for idA (identifying the OSCORE Security Context for messages sent
424 from Device A to Device B) conforming to the following criteria:
 - 425 – The total length of idA in bits shall be a multiple of 8 between 16 and 56 inclusive, which
426 corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14
427 characters inclusive.
 - 428 – The first byte of idA shall be 0x01.

429 NOTE 1: The value 0x01 is the OSCORE Identifier Namespace Prefix value assigned for "Directly Provisioned OSCORE
430 Security Context" in ISO/IEC 30118-2.

- 431 – The value of idA should be distinct from all values of "recipientid" in credential entries on
432 Device B at the time of provisioning.
- 433 – The CMS selects a value for idB (identifying the OSCORE Security Context for messages sent
434 from Device B to Device A) conforming to the following criteria:
 - 435 – The total length of idB in bits shall be a multiple of 8 between 16 and 56 inclusive, which
436 corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14
437 characters inclusive.
 - 438 – The first byte of idB shall be 0x01. See Note 1.
 - 439 – The value of idB should be distinct from all values of "recipientid" in credential entries on
440 Device A at the time of provisioning.
- 441 – The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should
442 use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient
443 entropy.

444 The CMS then independently provisions credential entries to Device A and Device B.

445 The CMS provisions the following credential entry to Device A:

- 446 – The "subjectuid" shall be the Device UUID of Device B (that is, the value of
447 "/oic/sec/doxm:deviceuid" on Device B).

448 – The "credtype" shall have the value 64.

449 NOTE 2: The value 64 is the "credtype" value specified for a directly provisioned OSCORE Security Context in
450 ISO/IEC 30118-2.

451 – The "privatedata" Property of the credential entry shall be the OSCORE Master Secret
452 generated by the CMS.

453 – The "oscore" Property shall be present, and shall include the following Properties:

454 – The "senderid" Property shall be set to the lowercase hexadecimal representation of idA
455 with the "0x" encoding prefix omitted.

456 – The "recipientid" Property shall be set to the lowercase hexadecimal representation of idB
457 with the "0x" encoding prefix omitted.

458 The CMS separately provisions the following credential entry to Device B:

459 – The "subjectuid" shall be the Device UUID of Device A (that is, the value of
460 "/oic/sec/doxm:deviceuid" on Device A).

461 – The "credtype" shall have the value 64. See Note 2.

462 – The "privatedata" Property of the credential entry shall be the OSCORE Master Secret
463 generated by the CMS.

464 – The "oscore" Property shall be present, and shall include the following Properties:

465 – The "senderid" Property shall be set to the lowercase hexadecimal representation of idB
466 with the "0x" encoding prefix omitted.

467 – The "recipientid" Property shall be set to the lowercase hexadecimal representation of idA
468 with the "0x" encoding prefix omitted.

469 **6.4 Provisioning Clients and Servers in a Simple Secure Multicast Group**

470 ISO/IEC 30118-2 specifies how Simple Secure Multicast (SSM) secures messages are sent from a
471 Client to multiple Servers in a SSM Group by applying an application layer of in-transit protection
472 below the resource-access authorization layer, using Object Security for Constrained RESTful
473 Environments (OSCORE) [4]. Within the scope of this clause, "Client" refers to the Client of the
474 SSM Group and "Server(s)" refers to a Server(s) in the SSM Group.

475 SSM is enabled by provisioning an SSM Client Context in a credential entry of the "/oic/sec/cred"
476 Resource of the Client, and provisioning (identical) copies of the SSM Server Context in a
477 credential entry of the "/oic/sec/cred" Resource of the Servers. The present clause provides the
478 requirements on the CMS for this provisioning.

479 The OBT recognizes during onboarding, by examining the "/oic/sec/doxm:sct" Property, that one
480 or more Devices in the Security Domain support SSM Client Context credentials and/or SSM Server
481 Context credentials. The OBT may prompt the End User to create one or more SSM Groups, or the
482 OBT may create groups without any End User interaction.

483 On creation of an SSM Group, a corresponding SSM Client Context and SSM Server Context shall
484 be generated by the CMS. The CMS generates four values: idGroup; an associated Device UUID,
485 an OSCORE Master Secret, and SSM Group description.

486 – The CMS selects a value for idGroup (identifying the OSCORE Security Context for messages
487 sent from the Client to the Servers) conforming to the following criteria:

488 – The total length of idGroup in bits shall be a multiple of 8 between 16 and 56 inclusive, which
489 corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14
490 characters inclusive.

491 – The first byte of idGroup shall be 0x02.

492 NOTE 1: The value 0x02 is the OSCORE Identifier Namespace Prefix value assigned for "Simple Secure Multicast" in
493 ISO/IEC 30118-2.

494 – The value of idGroup should be distinct from all values of "recipientid" in credential entries
495 of all Devices in the Security Domain.

496 - The CMS shall select an SSM-Group-subjectuud which will be configured in the "subjectuud"
497 of the credential entry containing the SSM Server Context; the Servers use this "subjectuud"
498 for access control processing applied to verified SSM Requests as specified in ISO/IEC 30118-
499 2. The SSM-Group-subjectuud would typically be the Device UUID (that is, the value in
500 "/oic/sec/doxm:deviceuud") of the Client; this will result in SSM requests from the Client have
501 the same permissions as unicast requests from the Client (e.g. received via DTLS or OSCORE).
502 However, a CMS can select a value for the SSM-Group-subjectuud, which provides the
503 flexibility for the AMS to configure the Servers with

504 - One set of permissions, using ACEs with "subject" matching Client's Device UUID, for
505 unicast requests received from the Client (e.g. received via DTLS or OSCORE), and

506 - Another set of permissions, using ACEs with "subject" matching SSM-Group-subjectuud
507 (and different from the Client's Device UUID), for SSM requests received from the Client.

508 - The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should
509 use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient
510 entropy.

511 - The CMS or End User should select a human-readable string for identifying the SSM Group. If
512 a value is not selected, then this value defaults to the empty string.

513 The CMS then independently provisions credential entries to the Client and Servers of the SSM
514 Group.

515 The CMS provisions the following credential entry, containing the SSM Client Context, to the Client
516 of the SSM Group:

517 - The "subjectuud" may be any schema compliant value. This Property serves no purpose when
518 used in an SSM Client Context.

519 - The "credtype" shall have the value 128.

520 NOTE 2: The value 128 is the "credtype" value specified for a SSM Client Context in ISO/IEC 30118-2.

521 - The "privatedata" Property of the credential entry shall be the OSCORE Master Secret
522 generated by the CMS.

523 - The "oscore" Property shall be present, and shall include the following Properties:

524 - The "senderid" Property shall be set to the lowercase hexadecimal representation of
525 idGroup with the "0x" encoding prefix omitted.

526 - The "desc" Property shall be set to the human-readable description for identifying the SSM
527 Group.

528 The CMS separately provisions the following credential entry, containing the SSM Server Context,
529 to Servers of the SSM Group:

530 - The "subjectuud" shall be set to the SSM-Group-subjectuud selected by the CMS.

531 - The "credtype" shall have the value 256.

532 NOTE 3: The value 256 is the "credtype" value specified for a SSM Server Context in ISO/IEC 30118-2.

533 - The "privatedata" Property of the credential entry shall be the OSCORE Master Secret
534 generated by the CMS.

535 - The "oscore" Property shall be present, and shall include the following Properties:

536 - The "recipientid" Property shall be set to the lowercase hexadecimal representation of
537 idGroup with the "0x" encoding prefix omitted.

538 - The "desc" Property shall be set to the human-readable description for identifying the SSM
539 Group.

540 These provisioning steps may occur implicitly, that is, without End User interaction.

541 **7 Ownership Transfer Methods**

542 **7.1 Preamble**

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

544 **7.2 Just Works Owner Transfer Method**

545 This OTM is specified in clause 7.3.4.1 of ISO/IEC 30118-2.

546 All DOTS shall implement the mandatory cipher suites and should implement the optional cipher
547 suites for Devices specified for this OTM in clause 11.3.2.1 of ISO/IEC 30118-2.

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

549 **7.3 Random PIN / Shared Credential based Owner Transfer Method**

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

- 552 – This OTM relies on the Device generating a random number that is communicated to the DOTS
553 over an Out of Band Communication Channel.
- 554 – The Platform hosting a DOTS which supports this OTM shall provide a user interface for
555 manual input of the random number.
- 556 – A DOTS may support other vendor-defined Out of Band Communication Channel for
557 receiving the random number from the Device. Security considerations regarding Out of
558 Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2.
- 559 – A DOTS shall support receiving a ServerKeyExchange message in the DTLS handshake either
560 with "psk_identity_hint" field formatted as specified in clause 7.3.5.2 of ISO/IEC 30118-2, or
561 with "psk_identity_hint" field comprising only a Device UUID (to ensure backwards compatibility
562 with Devices conforming to older releases). When the DOTS receives the ServerKeyExchange,
563 then
 - 564 – The DOTS can identify the new Device with which it is establishing the DOC by matching
565 the "deviceuuid" part of the "psk_identity_hint" field with the "deviceuuid" Property of the
566 "/oic/sec/doxm" Resource being sent in responses when the new Device is in RFOTM and
567 when a Device Onboarding Connection is not currently established. The DOTS shall
568 compute the PIN-authenticated pre-shared key (PPSK) using the algorithm specified in
569 clause 7.3.5.2 of ISO/IEC 30118-2.

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

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

573 NOTE: The string "oic.sec.doxm.rdp" is the URN defined for the Random PIN-based OTM in Table 18 of ISO/IEC 30118-
574 2, and is included to allow future OTMs to re-use the DTLS cipher suites without confusion about which OTM should be
575 applied.

576 All DOTS shall implement the mandatory cipher suites and should implement the optional cipher
577 suites for Devices specified for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2.

578 Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-2.

579 **7.4 Manufacturer Certificate Based Owner Transfer Method**

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

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

585 – The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2.
586 All DOTS shall implement the mandatory and optional cipher suites for Devices specified for this
587 OTM in clause 11.3.2.3 of ISO/IEC 30118-2.

588 Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses
589 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2.

590 **7.5 Vendor-Specific Owner Transfer Methods**

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

592 Bibliography

- 593 [1] ISO/IEC 30118-3 *Information technology – Open Connectivity Foundation (OCF) Specification*
594 – *Part 3: Bridging specification*
595 <https://www.iso.org/standard/74240.html>
596 Latest version available at:
597 https://openconnectivity.org/specs/OCF_Bridging_Specification.pdf
- 598 [2] ISO/IEC 30118-7, *Information technology – Open Connectivity Foundation (OCF)*
599 *Specification – Part 7: Wi-Fi Easy Setup specification*
600 <https://www.iso.org/standard/79175.html>
601 Latest version available at:
602 https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf
- 603 [3] *Open Connectivity Foundation (OCF) Specification – Cloud Security Specification*
604 Latest version available at:
605 https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf
- 606 [4] IETF RFC 8613, *Object Security for Constrained RESTful Environments (OSCORE)*, July 2019
607 <https://www.rfc-editor.org/info/rfc8613>

608
609