

OCF Onboarding Tool Specification

VERSION 2.2.3 | April 2021



CONTACT admin@openconnectivityfoundation.org
Copyright OCF © 2021. All Rights Reserved.

Copyright Open Connectivity Foundation, Inc. © 2016-2021. All rights Reserved.

LEGAL DISCLAIMER

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

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

Copyright © 2017-2021 Open Connectivity Foundation, Inc. All rights reserved.

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	

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 **Scope**

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

80 **Normative References**

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

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

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

88 Latest version available at:

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

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

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

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

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

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

97

98 **Terms, definitions, and abbreviated terms**

99 **3.1 Terms and definitions**

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

102 ISO and IEC maintain terminological databases for use in standardization at the following
103 addresses:

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

106 **3.2 Symbols and abbreviated terms**

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

109 **Document Conventions and Organization**

110 **4.1 Conventions**

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

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

118 **4.2 Notation**

119 In this document, features are described as required, recommended, allowed or DEPRECATED as
120 follows:

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

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

125 Recommended (or should)(S).

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

132 Allowed (may or allowed)(O).

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

136 DEPRECATED.

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

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

143 Conditionally allowed (CA).

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

146 Conditionally required (CR).

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

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

151 Words that are emphasized are printed in italic.

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

156 **4.3 Data types**

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

159 **Services and Availability in the OBT**

160 **5.1 Purpose of the OBT**

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

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

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

175 The following OBT functions are specified:

- 176 – A Device Ownership Transfer Service (DOTS) establishes ownership of Devices being added
177 to the OCF Security Domain. This function is described in clause 5.3.
- 178 – A Credential Management Service (CMS) manages the credentials and Roles of Devices in the
179 OCF Security Domain. This function is described in clause 5.4.
- 180 – An Access Management Service (AMS) manages the access of Devices in the OCF Security
181 Domain. This function is described in clause 5.5.
- 182 – Optional: A Mediator facilitates further configuration of Devices in the OCF Security Domain for
183 various purposes including Wi-Fi configuration (see [2]) and OCF Cloud access (see [3]).

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

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

191 The Device Onboarding States are defined in clause 8 of ISO/IEC 30118-2. Table 1 provides an
192 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		

194

5.2 General OBT requirements

195 An OBT shall be hosted on an OCF Device.

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

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

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

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

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

207 **5.3 DOTS**

208 **5.3.1 Assuming ownership of a Device**

209 The DOTS shall support all OTMs in clause 7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 245 11) The following steps are applied subsequent to successful establishment of Owner Credential,
246 and prior to transitioning to RFPRO. These steps may occur in any order.
- 247 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/doxm" Resource with the
248 UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has
249 "oic.d.dots" value in "rt" Property of its "/oic/d" Resource. The DOTS shall expose
250 "oic.d.dots" value in "rt" Property of its "/oic/d" Resource.
 - 251 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/pstat" Resource with the
252 UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has
253 "oic.d.dots" value in "rt" Property of its "/oic/d" Resource. The DOTS shall expose
254 "oic.d.dots" value in "rt" Property of its "/oic/d" Resource.
 - 255 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the
256 UUID of the CMS. The DOTS shall only do so, if the OCF Device, which hosts CMS has
257 "oic.d.cms" value in "rt" Property of its "/oic/d" Resource. The CMS shall expose "oic.d.cms"
258 value in "rt" Property of its "/oic/d" Resource.
 - 259 – The DOTS shall update the "rowneruuid" Property of the "/oic/sec/acl2" Resource with the
260 UUID of the AMS. The DOTS shall only do so, if the OCF Device, which hosts AMS has
261 "oic.d.ams" value in "rt" Property of its "/oic/d" Resource. The AMS shall expose "oic.d.ams"
262 value in "rt" Property of its "/oic/d/" Resource.
 - 263 – The DOTS shall update the "owned" Property of the "/oic/sec/doxm" Resource with value
264 "true".
 - 265 – The DOTS shall provision the "/oic/sec/cred" Resource with credentials that enable secure
266 connections between OCF Services (e.g. DOTS, CMS, AMS, Mediator) and the new Device.
267 The DOTS shall provision credentials according to the supported credential types shown in
268 the "sct" Property of the "/oic/sec/doxm" Resource.
 - 269 – The DOTS may UPDATE the "/oic/sec/acl2" Resource with ACEs and may UPDATE the
270 "/oic/sec/cred" Resource with further credentials.
 - 271 – If the provisioned Device exposes "/oic/sec/sdi" Resource, then an OBT hosting DOTS shall:
 - 272 – Provision "uuid" Property of "/oic/sec/sdi" Resource with OCF Security Domain UUID.
273 If the OCF Security Domain UUID has not been derived yet, the DOTS shall generate
274 the UUID value randomly. DOTS shall use the same UUID value when Onboarding a
275 Device into the same OCF Security Domain.
 - 276 – Provision "name" Property of "/oic/sec/sdi" Resource with a human readable name,
277 received from an OCF Security Domain Owner. The DOTS should implement a user
278 interface to receive this information, when a new OCF Security Domain is being created.
279 If no user interface is implemented the DOTS should provision a copy of the "/oic/d:n"
280 of the DOTS.
 - 281 – Provision "priv" Property of "/oic/sec/sdi" Resource with the value selected by the OCF
282 Security Domain Owner or preconfigured by the manufacturer. The DOTS should
283 implement a user interface to receive this information.

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

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

288 5.3.2 DOTS and Bridging

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

294 **5.3.3 Security considerations regarding selecting an Ownership Transfer Method**

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

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

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

303 **5.4 CMS**

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

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

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

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

310 The CMS shall support adding certificate entries ("credtype" value of "8") to the "creds" Property
311 to the "/oic/sec/cred" Resource as defined in clause 13.3 of ISO/IEC 30118-2. The CMS shall
312 support removing entries from the "creds" Property to the "/oic/sec/cred" Resource as defined in
313 clause 13.3 of ISO/IEC 30118-2. The CMS may support changing existing entries in the "creds"
314 Property to the "/oic/sec/cred" Resource as defined in 13.3 of ISO/IEC 30118-2.

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

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

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

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

332 **5.5 AMS**

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

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

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

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

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

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

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

349 **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

350

351 **Certificate management requirements**

352 **6.1 Issuing identity certificates and role certificates**

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

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

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

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

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

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

364 – The "subjectuid" Property shall have the value of "deviceuuid" Property of the
365 "/oic/sec/doxm" Resource.

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

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

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

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

374 **6.2 Provisioning Trust Anchor certificates**

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

- 378 – The "subjectuid" Property shall have the value of "*" (matching all identities) or a specific UUID
379 (matching a single identity).
- 380 – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with
381 Certificate
- 382 – The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a
383 certificate Trust Anchor
- 384 – The "publicdata" Property shall contain the Trust Anchor certificate.

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

387 **6.3 Provisioning an OSCORE Security Context for End-to-End Security of Unicast** 388 **Messages**

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

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

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

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

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

- 404 – The value of idA should be distinct from all values of "recipientid" in credential entries on
405 Device B at the time of provisioning.
- 406 – The CMS selects a value for idB (identifying the OSCORE Security Context for messages sent
407 from Device B to Device A) conforming to the following criteria:
 - 408 – The total length of idB in bits shall be a multiple of 8 between 16 and 56 inclusive, which
409 corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14
410 characters inclusive.
 - 411 – The first byte of idB shall be 0x01. See Note 1.
 - 412 – The value of idB should be distinct from all values of "recipientid" in credential entries on
413 Device A at the time of provisioning.
- 414 – The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should
415 use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient
416 entropy.

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

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

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

421 - The "credtype" shall have the value 64.

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

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

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

427 - The "senderid" Property shall be set to the lowercase hexadecimal representation of idA
428 with the "0x" encoding prefix omitted.

429 - The "recipientid" Property shall be set to the lowercase hexadecimal representation of idB
430 with the "0x" encoding prefix omitted.

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

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

434 - The "credtype" shall have the value 64. See Note 2.

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

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

438 - The "senderid" Property shall be set to the lowercase hexadecimal representation of idB
439 with the "0x" encoding prefix omitted.

440 - The "recipientid" Property shall be set to the lowercase hexadecimal representation of idA
441 with the "0x" encoding prefix omitted.

442 **6.4 Provisioning Clients and Servers in a Simple Secure Multicast Group**

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

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

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

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

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

461 - The total length of idGroup in bits shall be a multiple of 8 between 16 and 56 inclusive, which
462 corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14
463 characters inclusive.

464 - The first byte of idGroup shall be 0x02.

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

467 - The value of idGroup should be distinct from all values of "recipientid" in credential entries
468 of all Devices in the Security Domain.

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

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

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

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

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

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

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

490 – The "subjectuud" may be any schema compliant value. This Property serves no purpose when
491 used in an SSM Client Context.

492 – The "credtype" shall have the value 128.

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

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

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

497 – The "senderid" Property shall be set to the lowercase hexadecimal representation of
498 idGroup with the "0x" encoding prefix omitted.

499 – The "desc" Property shall be set to the human-readable description for identifying the SSM
500 Group.

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

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

504 – The "credtype" shall have the value 256.

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

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

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

509 – The "recipientid" Property shall be set to the lowercase hexadecimal representation of
510 idGroup with the "0x" encoding prefix omitted.

511 – The "desc" Property shall be set to the human-readable description for identifying the SSM
512 Group.

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

514 **Ownership Transfer Methods**

515 **7.1 Preamble**

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

517 **7.2 Just Works Owner Transfer Method**

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

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

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

522 **7.3 Random PIN / Shared Credential based Owner Transfer Method**

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

- 525 – This OTM relies on the Device generating a random number that is communicated to the DOTS
526 over an Out of Band Communication Channel.
- 527 – The Platform hosting a DOTS which supports this OTM shall provide a user interface for
528 manual input of the random number.
- 529 – A DOTS may support other vendor-defined Out of Band Communication Channel for
530 receiving the random number from the Device. Security considerations regarding Out of
531 Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2.
- 532 – A DOTS shall support receiving a ServerKeyExchange message in the DTLS handshake either
533 with "psk_identity_hint" field formatted as specified in clause 7.3.5.2 of ISO/IEC 30118-2, or
534 with "psk_identity_hint" field comprising only a Device UUID (to ensure backwards compatibility
535 with Devices conforming to older releases). When the DOTS receives the ServerKeyExchange,
536 then
- 537 – The DOTS can identify the new Device with which it is establishing the DOC by matching
538 the "deviceuuid" part of the "psk_identity_hint" field with the "deviceuuid" Property of the
539 "/oic/sec/doxm" Resource being sent in responses when the new Device is in RFOTM and
540 when a Device Onboarding Connection is not currently established. The DOTS shall
541 compute the PIN-authenticated pre-shared key (PPSK) using the algorithm specified in
542 clause 7.3.5.2 of ISO/IEC 30118-2.

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

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

546 NOTE: The string "oic.sec.doxm.rdp" is the URN defined for the Random PIN-based OTM in Table 18 of ISO/IEC 30118-
547 2, and is included to allow future OTMs to re-use the DTLS cipher suites without confusion about which OTM should be
548 applied.

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

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

552 **7.4 Manufacturer Certificate Based Owner Transfer Method**

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

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

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

561 Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses
562 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2.

563 **7.5 Vendor-Specific Owner Transfer Methods**

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

565 Bibliography

- 566 [1] ISO/IEC 30118-3 *Information technology – Open Connectivity Foundation (OCF) Specification*
567 – *Part 3: Bridging specification*
568 <https://www.iso.org/standard/74240.html>
569 Latest version available at:
570 https://openconnectivity.org/specs/OCF_Bridging_Specification.pdf
- 571 [2] ISO/IEC 30118-7, *Information technology – Open Connectivity Foundation (OCF)*
572 *Specification – Part 7: Wi-Fi Easy Setup specification*
573 <https://www.iso.org/standard/79175.html>
574 Latest version available at:
575 https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf
- 576 [3] *Open Connectivity Foundation (OCF) Specification – Cloud Security Specification*
577 Latest version available at:
578 https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf
- 579 [4] IETF RFC 8613, *Object Security for Constrained RESTful Environments (OSCORE)*, July 2019
580 <https://www.rfc-editor.org/info/rfc8613>

581
582