

ISO/IEC 30118-2:2018-11 (E)

Information technology - Open Connectivity Foundation (OCF) Specification - Part 2: Security specification

Contents	Page
1 Scope	13
2 Normative References.....	13
3 Terms, Definitions, Symbols and Abbreviations	14
3.1 Terms and definitions	14
3.2 Symbols and Abbreviations	16
3.3 Conventions	17
4 Document Conventions and Organization	18
4.1 Notation.....	18
4.2 Data types	18
4.3 Document structure	19
5 Security Overview	20
5.1 Access Control	22
5.1.1 ACL Architecture	23
5.1.2 Access Control Scoping Levels	26
5.2 Onboarding Overview	27
5.2.1 OnBoarding Steps	29
5.2.2 Establishing a Device Owner	30
5.2.3 Provisioning for Normal Operation.....	31
5.3 Provisioning.....	32
5.3.1 Provisioning a bootstrap service.....	32
5.3.2 Provisioning other services	32
5.3.3 Credential provisioning.....	33
5.3.4 Role assignment and provisioning	33
5.3.5 ACL provisioning.....	33
5.4 Secure Resource Manager-(SRM)	34
5.5 Credential Overview	34
6 Security for the Discovery Process	36
6.1 Security Considerations for Discovery	36
7 Security Provisioning.....	39
7.1 Device Identity.....	39
7.1.1 Device Identity for Devices with UAID	39
7.2 Device Ownership	41
7.3 Device Ownership Transfer Methods	41
7.3.1 OTM implementation requirements.....	41
7.3.2 SharedKey Credential Calculation	42
7.3.3 Certificate Credential Generation	43
7.3.4 Just-Works Owner Transfer Method	43
7.3.5 Random PIN Based Owner Transfer Method	45
7.3.6 Manufacturer Certificate Based Owner Transfer Method.....	47
7.3.7 Vendor Specific Owner Transfer Methods.....	51
7.3.8 Establishing Owner Credentials.....	52

7.3.9	Security considerations regarding selecting an Ownership Transfer Method..	63
7.4	Provisioning.....	63
7.4.1	Provisioning Flows	63
7.5	Bootstrap Example	69
8	Device Onboarding State Definitions	70
8.1	Device Onboarding-Reset State Definition	71
8.2	Device Ready-for-OTM State Definition	72
8.3	Device Ready-for-Provisioning State Definition.....	72
8.4	Device Ready-for-Normal-Operation State Definition	73
8.5	Device Soft Reset State Definition	73
9	Security Credential Management.....	76
9.1	Credential Lifecycle	76
9.1.1	Creation	76
9.1.2	Deletion	76
9.1.3	Refresh	76
9.1.4	Revocation	77
9.2	Credential Types	77
9.2.1	Pair-wise Symmetric Key Credentials	77
9.2.2	Group Symmetric Key Credentials.....	77
9.2.3	Asymmetric Authentication Key Credentials.....	78
9.2.4	Asymmetric Key Encryption Key Credentials	78
9.2.5	Certificate Credentials.....	79
9.2.6	Password Credentials.....	79
9.3	Certificate Based Key Management	79
9.3.1	Overview.....	79
9.3.2	Certificate Format	80
9.3.3	CRL Format.....	85
9.3.4	Resource Model	86
9.3.5	Certificate Provisioning	86
9.3.6	CRL Provisioning	87
10	Device Authentication	90
10.1	Device Authentication with Symmetric Key Credentials.....	90
10.2	Device Authentication with Raw Asymmetric Key Credentials	90
10.3	Device Authentication with Certificates	90
10.3.1	Role Assertion with Certificates.....	91
11	Message Integrity and Confidentiality	93
11.1	Session Protection with DTLS.....	93
11.1.1	Unicast Session Semantics	93
11.2	Cipher Suites.....	93
11.2.1	Cipher Suites for Device Ownership Transfer	93
11.2.2	Cipher Suites for Symmetric Keys	94
11.2.3	Cipher Suites for Asymmetric Credentials.....	94
12	Access Control.....	95
12.1	ACL Generation and Management	95

12.2	ACL Evaluation and Enforcement	95
12.2.1	Host Reference Matching	95
12.2.2	Resource Type Matching	95
12.2.3	Interface Matching.....	95
12.2.4	Multiple Criteria Matching.....	95
12.2.5	Resource Wildcard Matching	96
12.2.6	Subject Matching using Wildcards	97
12.2.7	Subject Matching using Roles	97
12.2.8	ACL Evaluation	97
13	Security Resources	98
13.1	Device Owner Transfer Resource	99
13.2	Credential Resource	104
13.2.1	Properties of the Credential Resource	110
13.2.2	Key Formatting.....	113
13.2.3	Credential Refresh Method Details	113
13.3	Certificate Revocation List.....	115
13.3.1	CRL Resource Definition	115
13.4	ACL Resources	115
13.4.1	OCF Access Control List (ACL) BNF defines ACL structures.	115
13.4.2	ACL Resource.....	116
13.5	Access Manager ACL Resource	126
13.6	Signed ACL Resource	126
13.7	Provisioning Status Resource	126
13.8	Certificate Signing Request Resource	135
13.9	Roles resource	136
13.10	Security Virtual Resources (SVRs) and Access Policy	137
13.11	SVRs, Discoverability and Endpoints	137
13.12	Privacy Consideration for Core and SVRs.....	138
14	Core Interaction Patterns Security.....	140
14.1	Observer	140
14.2	Subscription/Notification	140
14.3	Groups	140
14.4	Publish-subscribe Patterns and Notification.....	140
15	Security Hardening Guidelines/ Execution Environment Security.....	141
15.1	Execution environment elements	141
15.1.1	Secure Storage	141
15.1.2	Secure execution engine	143
15.1.3	Trusted input/output paths.....	143
15.1.4	Secure clock	144
15.1.5	Approved algorithms	144
15.1.6	Hardware tamper protection	144
15.2	Secure Boot	145
15.2.1	Concept of software module authentication	145
15.2.2	Secure Boot process	146

15.2.3	Robustness requirements	146
15.3	Attestation	147
15.4	Software Update	147
15.4.1	Overview:	147
15.4.2	Recognition of Current Differences	147
15.4.3	Software Version Validation	147
15.4.4	Software Update	147
15.4.5	Recommended Usage	148
15.5	Non-OCF Endpoint interoperability	148
15.7	Security Levels	148
16	Appendix A: Access Control Examples	149
16.1	Example OCF ACL Resource	149
16.2	Example Access Manager Service	149
17	Appendix B: Execution Environment Security Profiles	150
18	Appendix C: RAML Definition	151
A.1	OICSecurityAclResource	151
A.1.1	Introduction	151
A.1.2	Example URI	151
A.1.3	Resource Type	151
A.1.4	RAML Definition	151
A.1.5	Property Definition	155
A.1.6	CRUDN behavior	155
A.2	OICSecurityAcl2Resource	155
A.2.1	Introduction	155
A.2.2	Example URI	155
A.2.3	Resource Type	156
A.2.4	RAML Definition	156
A.2.5	Property Definition	160
A.2.6	CRUDN behavior	160
A.2.7	Referenced JSON schemas	160
A.2.8	oic.sec.didtype.json	160
A.2.9	Property Definition	160
A.2.10	Schema Definition	160
A.2.11	oic.sec.ace2.json	160
A.2.12	Property Definition	160
A.2.13	Schema Definition	161
A.2.14	oic.sec.roletype.json	163
A.2.15	Property Definition	163
A.2.16	Schema Definition	163
A.2.17	oic.sec.time-pattern.json	163
A.2.18	Property Definition	163
A.2.19	Schema Definition	163
A.2.20	oic.sec.crudntype.json	164
A.2.21	Property Definition	164

A.2.22	Schema Definition	164
A.3	OICSecurityAmaclResource.....	165
A.3.1	Introduction	165
A.3.2	Example URI	165
A.3.3	Resource Type	165
A.3.4	RAML Definition	165
A.3.5	Property Definition	168
A.3.6	CRUDN behavior.....	168
A.4	OICSecuritySignedAclResource.....	168
A.4.1	Introduction	168
A.4.2	Example URI	168
A.4.3	Resource Type	168
A.4.4	RAML Definition	168
A.4.5	Property Definition	174
A.4.6	CRUDN behavior.....	174
A.4.7	Referenced JSON schemas.....	174
A.4.8	oic.sec.sigtype.json	174
A.4.9	Property Definition	174
A.4.10	Schema Definition	174
A.5	OICSecurityDoxmResource	175
A.5.1	Introduction	175
A.5.2	Example URI	175
A.5.3	Resource Type	175
A.5.4	RAML Definition	175
A.5.5	Property Definition	179
A.5.6	CRUDN behavior.....	180
A.5.7	Referenced JSON schemas.....	180
A.5.8	oic.sec.doxmtype.json	180
A.5.9	Property Definition	180
A.5.10	Schema Definition	180
A.5.11	oic.sec.credtype.json.....	180
A.5.12	Property Definition	180
A.5.13	Schema Definition	180
A.6	OICSecurityPstatResource	181
A.6.1	Introduction	181
A.6.2	Example URI	181
A.6.3	Resource Type	181
A.6.4	RAML Definition	181
A.6.5	Property Definition	185
A.6.6	CRUDN behavior.....	186
A.6.7	Referenced JSON schemas.....	186
A.6.8	oic.sec.dostype.json.....	186
A.6.9	Property Definition	186
A.6.10	Schema Definition	186

A.6.11	oic.sec.dpmtypes.json	187
A.6.12	Property Definition	187
A.6.13	Schema Definition	187
A.6.14	oic.sec.pomtypes.json	187
A.6.15	Property Definition	187
A.6.16	Schema Definition	188
A.6.17	188	
A.7	OICSecurityCredentialResource	188
A.7.1	Introduction	188
A.7.2	Example URI	188
A.7.3	Resource Type	188
A.7.4	RAML Definition	188
A.7.5	Property Definition	192
A.7.6	CRUDN behavior	192
A.7.7	Referenced JSON schemas	192
A.7.8	oic.sec.roletypes.json	192
A.7.9	Property Definition	192
A.7.10	Schema Definition	193
A.7.11	oic.sec.credtypes.json	193
A.7.12	Property Definition	193
A.7.13	Schema Definition	193
A.7.14	oic.sec.pubdatatypes.json	194
A.7.15	Property Definition	194
A.7.16	Schema Definition	194
A.7.17	oic.sec.privdatatypes.json	194
A.7.18	Property Definition	194
A.7.19	Schema Definition	195
A.7.20	oic.sec.optdatatypes.json	195
A.7.21	Property Definition	195
A.7.22	Schema Definition	196
A.7.23	oic.sec.crmtypes.json	196
A.7.24	Property Definition	196
A.7.25	Schema Definition	196
A.8	OICSecurityCsrResource	197
A.8.1	Introduction	197
A.8.2	Example URI	197
A.8.3	Resource Type	197
A.8.4	RAML Definition	197
A.8.5	Property Definition	198
A.8.6	CRUDN behavior	198
A.9	OICSecurityRolesResource	198
A.9.1	Introduction	198
A.9.2	Example URI	199
A.9.3	Resource Type	199

A.9.4	RAML Definition	199
A.9.5	Property Definition	202
A.9.6	CRUDN behavior.....	202
A.10	OICSecurityCrlResource.....	202
A.10.1	Introduction	202
A.10.2	Example URI	202
A.10.3	Resource Type	202
A.10.4	RAML Definition	202
A.10.5	Property Definition	205
A.10.6	CRUDN behavior.....	206

Figures

Figure 1 – OCF Interaction	17
Figure 2 – OCF Layers	20
Figure 3 – OCF Security Enforcement Points.....	22
Figure 4 – Use case-1 showing simple ACL enforcement.....	24
Figure 5 – Use case 2: A policy for the requested Resource is missing.....	24
Figure 6 – Use case-3 showing Access Manager Service supported ACL	25
Figure 7 – Use case-4 showing dynamically obtained ACL from an AMS	26
Figure 8 – Example Resource definition with opaque Properties	27
Figure 9 – Property Level Access Control	27
Figure 10 - Onboarding Overview	28
Figure 11 – OCF Onboarding Process	30
Figure 12 – OCF's SRM Architecture	34
Figure 13 - Discover New Device Sequence	42
Figure 14 – A Just Works Owner Transfer Method.....	44
Figure 15 – Random PIN-based Owner Transfer Method	45
Figure 16 – Manufacturer Certificate Hierarchy.....	48
Figure 17 – Manufacturer Certificate Based Owner Transfer Method Sequence.....	50
Figure 18 – Vendor-specific Owner Transfer Sequence	52
Figure 19 - Establish Device Identity Flow	55
Figure 20 – Owner Credential Selection Provisioning Sequence	57
Figure 21 - Symmetric Owner Credential Provisioning Sequence.....	58
Figure 22 - Asymmetric Ownership Credential Provisioning Sequence.....	59
Figure 23 - Configure Device Services.....	61
Figure 24 - Provision New Device for Peer to Peer Interaction Sequence	62
Figure 25 – Example of Client-directed provisioning	64
Figure 26 – Example of Server-directed provisioning using a single provisioning service	66
Figure 27 – Example of Server-directed provisioning involving multiple support services	68
Figure 28 – Device state model	70
Figure 29 – OBT Sanity Check Sequence in SRESET.....	74
Figure 30 – Certificate Management Architecture	80
Figure 31 – Client-directed Certificate Transfer	87
Figure 32 – Client-directed CRL Transfer	88
Figure 33 – Server-directed CRL Transfer	89
Figure 34 – Asserting a role with a certificate role credential.	92
Figure 35 – OCF Security Resources.....	98
Figure 36 – oic.r.cred Resource and Properties	99
Figure 37 – oic.r.acl2 Resource and Properties	99
Figure 38 – oic.r.amacl Resource and Properties	99

Figure 39 – oic.secr.sacl Resource and Properties	99
Figure 40 – Software Module Authentication.....	145
Figure 41 – Verification Software Module	146
Figure 42 – Software Module Authenticity.....	146

Tables

Table 1 – Symbols and abbreviations	17
Table 2 - Discover New Device Details	42
Table 3 – A Just Works Owner Transfer Method Details	44
Table 4 – Random PIN-based Owner Transfer Method Details	46
Table 5 – Manufacturer Certificate Based Owner Transfer Method Details.....	51
Table 6 – Vendor-specific Owner Transfer Details	52
Table 7 - Establish Device Identity Details	56
Table 8 - Owner Credential Selection Details.....	58
Table 9 - Symmetric Owner Credential Assignment Details.....	58
Table 10 – Asymmetric Owner Credential Assignment Details	59
Table 11 - Configure Device Services Detail.....	62
Table 12 - Provision New Device for Peer to Peer Details.....	63
Table 13 – Steps describing Client -directed provisioning	65
Table 14 – Steps for Server-directed provisioning using a single provisioning service	67
Table 15 – Steps for Server-directed provisioning involving multiple support services	69
Table 16 – Comparison between OCF and X.509 certificate fields	82
Table 17 – Comparison between OCF and X.509 CRL fields	86
Table 18 – ACE2 Wildcard Matching Strings Description	96
Table 19 – Definition of the oic.r.doxm Resource	100
Table 20 – Properties of the oic.r.doxm Resource	102
Table 21 - Properties of the oic.sec.didtype Property.....	102
Table 22 – Properties of the oic.sec.doxmtype Property	104
Table 23 – Definition of the oic.r.cred Resource	106
Table 24 – Properties of the oic.r.cred Resource	106
Table 25 – Properties of the oic.sec.cred Property	109
Table 26 – Properties of the oic.sec.pubdatatype Property	109
Table 27 – Properties of the oic.sec.privdatatype Property	110
Table 28 – Properties of the oic.sec.optdatatype Property	110
Table 29 – Definition of the oic.sec.roletype Property.	110
Table 30 – Value Definition of the oic.sec.crmtype Property	112
Table 31 – 128-bit symmetric key	113
Table 32 – 256-bit symmetric key	113
Table 33 – Definition of the oic.r.crl Resource	115
Table 34 – Properties of the oic.r.crl Resource	115
Table 35 – BNF Definition of OCF ACL.....	116
Table 36 – Definition of the oic.r.acl Resource.....	118
Table 37 – Properties of the oic.r.acl Resource	119
Table 38 – Properties of the oic.r.ace Property	120

Table 39 – Value Definition of the oic.sec.crudtype Property	120
Table 40 – Definition of the oic.sec.acl2 Resource	120
Table 41 – Properties of the oic.sec.acl2 Resource	121
Table 42 – oic.sec.ace2 data type definition.	122
Table 43 – oic.sec.ace2.resource-ref data type definition.	122
Table 44 – Value definition oic.sec.conntype Property	122
Table 45 – Definition of the oic.r.amacl Resource	126
Table 46 – Properties of the oic.r.amacl Resource	126
Table 47 – Definition of the oic.r.sacl Resource	126
Table 48 – Properties of the oic.r.sacl Resource	126
Table 49 – Properties of the oic.sec.sigtype Property	126
Table 50 – Definition of the oic.r.pstat Resource	128
Table 51 – Properties of the oic.r.pstat Resource	130
Table 52 – Properties of the oic.sec.dostype Property	131
Table 53 – Definition of the oic.sec.dpmttype Property	134
Table 54 – Value Definition of the oic.sec.dpmttype Property (Low-Byte)	134
Table 55 – Value Definition of the oic.sec.dpmttype Property (High-Byte)	134
Table 56 – Definition of the oic.sec.pomtype Property	135
Table 57 – Value Definition of the oic.sec.pomtype Property	135
Table 58 – Definition of the oic.r.csr Resource	136
Table 59 – Properties of the oic.r.csr Resource	136
Table 60 – Definition of the oic.r.roles Resource	137
Table 61 – Properties of the oic.r.roles Resource	137
Table 62 – Core Resource Properties state	139
Table 63 – Examples of Sensitive Data	142
Table 64 – OCF Security Profile	150
Table 65 – OCF SVR RAML	151