BS ISO/IEC 30118-2:2018

BSI Standards Publication

Information technology — Open Connectivity Foundation (OCF) Specification

Part 2: Security specification

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

National foreword

This British Standard is the UK implementation of ISO/IEC 30118-2:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/-/99, Participating IST members.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 99445 6

ICS 35.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

INTERNATIONAL STANDARD

ISO/IEC 30118-2

First edition
2018-11

Information technology — Open Connectivity Foundation (OCF) Specification —

Part 2: Security specification

Technologies de l'information — Spécification de la Fondation pour la connectivité ouverte (Fondation OCF) —

Partie 2: Spécification de sécurité

Reference number
ISO/IEC 30118-2:2018(E)

Documents
Document Sharing Hub
© ISO/IEC 2018

Full document details: BS ISO/IEC 30118-2:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by the Open Connectivity Foundation (OCF) (as the OCF Security Specification, Version 1.0.0) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

A list of all parts in the ISO/IEC 30118 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30118-2:2018

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

CONTENTS

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

A.6.11 oic.sec.dpmtype.json ... 187
A.6.12 Property Definition ... 187
A.6.13 Schema Definition ... 187
A.6.14 oic.sec.pomtype.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.roletype.json ... 192
A.7.9 Property Definition ... 192
A.7.10 Schema Definition ... 193
A.7.11 oic.sec.credtype.json ... 193
A.7.12 Property Definition ... 193
A.7.13 Schema Definition ... 193
A.7.14 oic.sec.pubdatatype.json ... 194
A.7.15 Property Definition ... 194
A.7.16 Schema Definition ... 194
A.7.17 oic.sec.privdatatype.json ... 194
A.7.18 Property Definition ... 194
A.7.19 Schema Definition ... 195
A.7.20 oic.sec.optdatatype.json ... 195
A.7.21 Property Definition ... 195
A.7.22 Schema Definition ... 196
A.7.23 oic.sec.crmtype.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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

Table 39 – Value Definition of the oic.sec.crudntype 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.dpmtype Property 134
Table 54 – Value Definition of the oic.sec.dpmtype Property (Low-Byte) 134
Table 55 – Value Definition of the oic.sec.dpmtype 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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

1 Scope

This specification defines security objectives, philosophy, resources and mechanism that impacts OCF base layers of the OCF Core Specification. The OCF Core Specification contains informative security content. The OCF Security specification contains security normative content and may contain informative content related to the OCF base or other OCF specifications.

2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

OCF Core Specification, version 1.1, Open Connectivity Foundation, October 11, 2016. Latest version available at: https://openconnectivity.org/specs/OCF_Core_Specification.pdf.

OCF Device Specification, version 1.1, Open Connectivity Foundation, October 11, 2016. Latest version available at: https://openconnectivity.org/specs/OCF_Device_Specification.pdf.

OCF Resource Type Specification, version 1.1, Open Connectivity Foundation, October 11, 2016. Latest version available at:
https://openconnectivity.org/specs/OCF_Resource_Type_Specification.pdf.

JSON SCHEMA, draft version 4, JSON Schema defines the media type "application/schema+json", a JSON based format for defining the structure of JSON data. JSON Schema provides a contract for what JSON data is required for a given application and how to interact with it. JSON Schema is intended to define validation, documentation, hyperlink navigation, and interaction control of JSON Available at: http://json-schema.org/latest/json-schema-core.html.

RAML, Restful API modelling language version 0.8. Available at: http://raml.org/spec.html.

OCF Security Resource Definitions, *API Definition Language for OCF Security Components,* Release OCF-v1.0.0
https://github.com/openconnectivityfoundation/security

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

3 Terms, Definitions, Symbols and Abbreviations

Terms, definitions, symbols and abbreviations used in this specification are defined by the OCF Core Specification. Terms specific to normative security mechanism are defined in this document in context.

This section restates terminology that is defined elsewhere, in this document or in other OCF specifications as a convenience for the reader. It is considered non-normative.

3.1 Terms and definitions

3.1.1
Access Manager Service

The Access Manager Service dynamically constructs ACL Resources in response to a Device Resource request. An Access Manager Service can evaluate access policies remotely and supply the result to a Server which allows or denies a pending access request.

3.1.2
ACL Provisioning Service

A name and Resource Type (oic.sec.aps) given to a Device that is authorized to provision ACL Resources.

3.1.3
Bootstrap Service

A Device that implements a service of type oic.sec.bss

3.1.4
Client

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.5
Credential Management Service

A name and Resource Type (oic.sec.cms) given to a Device that is authorized to provision credential Resources.

3.1.6
Device

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.7
Device Class

As defined in RFC 7228. RFC 7228 defines classes of constrained devices that distinguish when the OCF small footprint stack is used vs. a large footprint stack. Class 2 and below is for small footprint stacks.

3.1.8
Device ID

A stack instance identifier.

3.1.9
Entity

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.10
Interface

Note 1 to entry: The details are defined in OCF Core Specification.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

3.1.11
Intermediary

A Device that implements both Client and Server roles and may perform protocol translation, virtual device to physical device mapping or Resource translation

3.1.12
OCF Cipher Suite

A set of algorithms and parameters that define the cryptographic functionality of a Device. The OCF Cipher Suite includes the definition of the public key group operations, signatures, and specific hashing and encoding used to support the public key.

3.1.13
Onboarding Tool

A logical entity within a specific IoT network that establishes ownership for a specific device and helps bring the device into operational state within that network

3.1.14
Out of Band Method

Any mechanism for delivery of a secret from one party to another, not specified by OCF

3.1.15
Owner Credential

Credential, provisioned by an Onboarding Tool to a Device during onboarding, for the purposes of mutual authentication of the Device and Onboarding Tool during subsequent interactions

3.1.16
Platform ID

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.17
Property

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.18
Resource

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.19
Role (network context)

Stereotyped behavior of a Device; one of [Client, Server or Intermediary]

3.1.20
Role (Security context)

A Property of an OCF credentials Resource that names a role that a Device may assert when attempting access to Device Resources. Access policies may differ for Client if access is attempted through a role vs. the device UUID. This document assumes the security context unless otherwise stated.

3.1.21
Secure Resource Manager

A module in the OCF Core that implements security functionality that includes management of security Resources such as ACLs, credentials and Device owner transfer state.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

3.1.22
Security Virtual Resource

An SVR is a resource supporting security features.

3.1.23
Server

Note 1 to entry: The details are defined in OCF Core Specification.

3.1.24
Trust Anchor

A well-defined, shared authority, within a trust hierarchy, by which two cryptographic entities (e.g. a Device and an onboarding tool) can assume trust

3.1.25
Unique Authenticable Identifier

A unique identifier created from the hash of a public key and associated OCF Cipher Suite that is used to create the DeviceID. The ownership of a UAID may be authenticated by peer Devices.

3.2 Symbols and Abbreviations

Symbol	Description
ACE	Access Control Entry
ACL	Access Control List
AMS	Access Manager Service
APS	ACL Provisioning Service
BSS	Bootstrap Service
CMS	Credential Management Service
CRUDN	CREATE, RETREIVE, UPDATE, DELETE, NOTIFY
CSR	Certificate Signing Request
ECDSA	Elliptic Curve Digital Signature Algorithm
EPC	Embedded Platform Credential
DPKP	Dynamic Public Key Pair
OC	Owner Credential
OCSP	Online Certificate Status Protocol
OBT	Onboarding Tool
PIN	Personal Identification Number
PSI	Persistent Storage Interface
RNG	Random Number Generator
SACL	Signed Access Control List
SE	Secure Element
SRM	Secure Resource Manager
SVR	Security Virtual Resource
TEE	Trusted Execution Environment
UAID	Unique Authenticable Identifier

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

Table 1 – Symbols and abbreviations

3.3 Conventions

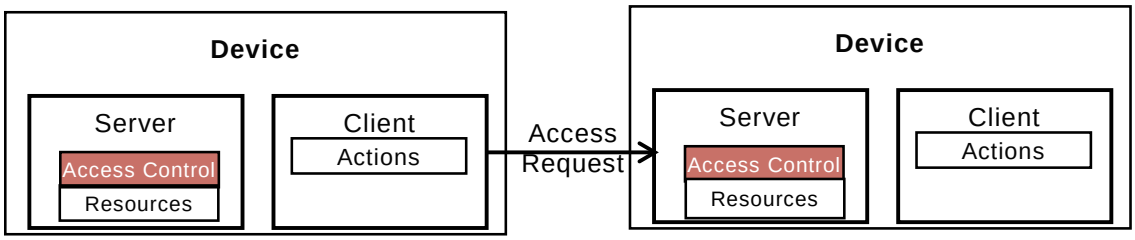

Figure 1 – OCF Interaction

Devices may implement a Client role that performs Actions on Servers. Actions access Resources managed by Servers. The OCF stack enforces access policies on Resources. End-to-end Device interaction can be protected using session protection protocol (e.g. DTLS) or with data encryption methods.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

4 Document Conventions and Organization

This document defines Resources, protocols and conventions used to implement security for OCF core framework and applications.

For the purposes of this document, the terms and definitions given in OCF Core Specification apply.

4.1 Notation

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

Required (or **shall** or **mandatory**).

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

Recommended (or **should**).

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

Allowed (or allowed).

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

Conditionally allowed (CA)

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

Conditionally required (CR)

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

DEPRECATED

Although these features are still described in this specification, they should not be implemented except for backward compatibility. The occurrence of a deprecated feature during operation of an implementation compliant with the current specification has no effect on the implementation's operation and does not produce any error conditions. Backward compatibility may require that a feature is implemented and functions as specified but it shall never be used by implementations compliant with this specification.

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

Words that are emphasized are printed in *italic*.

4.2 Data types

See OCF Core Specification.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

4.3 Document structure

Informative sections may be found in the Overview sections, while normative sections fall outside of those sections.

The Security specification may use RAML as a specification language and JSON Schemas as payload definitions for all CRUDN actions. The mapping of the CRUDN actions is specified in the OCF Core Specification.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

5 Security Overview

This is an informative section. The goal for the OCF security architecture is to protect the Resources and all aspects of HW and SW that are used to support the protection of Resource. From OCF perspective, a Device is a logical entity that conforms to the OCF specifications. In an interaction between the Devices, the Device acting as the Server holds and controls the Resources and provides the Device acting as a Client with access to those Resources, subject to a set of security mechanisms. The Platform, hosting the Device may provide security hardening that will be required for ensuring robustness of the variety of operations described in this specification.

The security theory of operation is described in the following steps.

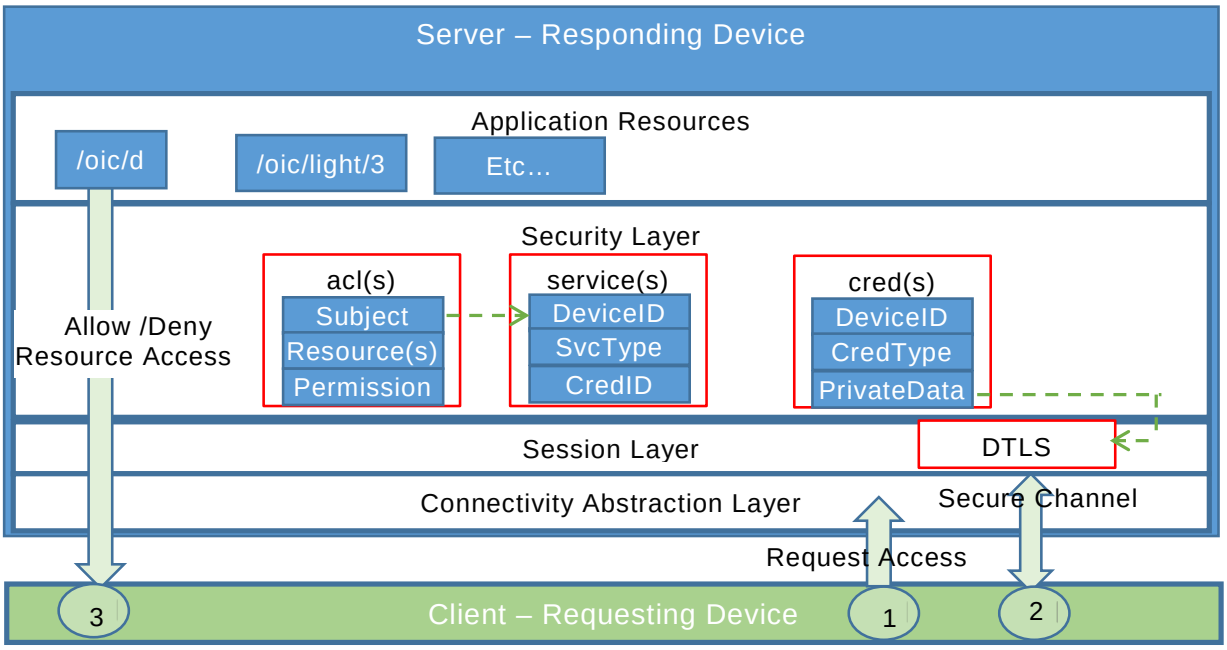

Figure 2 – OCF Layers

1. The Client establishes a network connection to the Server (Device holding the Resources). The connectivity abstraction layer ensures the Devices are able to connect despite differences in connectivity options.
2. The Devices (e.g. Server and Client) exchange messages either with or without a mutually-authenticated secure channel between the two Devices.
   - The oic.sec.cred Resource on each Devices holds the credentials used for mutual authentication and (when applicable) certificate validation.
   - Messages received over a secured channel are associated with a deviceUUID. In the case of a certificate credential, the deviceUUID is in the certificate received from the other Device. In the case of a symmetric key credential, the deviceUUID is configured with the credential in the oic.sec.cred Resource. There should be a binding between the device context and the Platform implementing the Device.
   - The Server can associate the Client with any number of allowed roleid. In the case of mutual authentication using a certificate, the allowed roleid (if any) are provided in role certificates; these are configured by the Client to the Server. In the case of a symmetric key, the allowed roleid (if any) are configured with the credential in the oic.sec.cred.
   - Requests received by a Server over an unsecured channel are treated as anonymous and not associated with any deviceUUID or roleid.
3. The Client submits a request to the Server.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

- If the request is to be sent over the secure channel, then the Client can either explicitly assert specific roleid by including 'role' options in the request, or implicitly assert all roleid associated with the Client by including no 'role' options.

4. The Server receives the request.
   a. If the request is received over an unsecured channel, the Server treats the request as anonymous and no deviceUUID or roleid are associated with the request.
   b. If the request is received over a secure channel, then the Server associates the deviceUUID, and the Server either validates any explicitly asserted roleids by matching to an allowed roleid of the Client, or implicitly asserts all valid roleid of the Client.
   c. The Server then consults the Access Control List (ACL), and looks for an ACL entry matching the following criteria:
      - The requested Resource matches a Resource reference in the ACE
      - The requested operation is allowed by the "permissions" of the ACE, and
      - The "subjectUUID" contains either a special wildcard value matching all Devices or, if the Device is not anonymous, the subject matches the Client Deviceid or a valid asserted roleID. In certain cases, the requester may assert a role, if privileged access is required.

      If there is a matching ACE, then access to the Resource is allowed; otherwise access is denied. Access is enforced by the Server's Secure Resource manager (SRM).

Resource protection includes protection of data both while at rest and during transit. It should be noted that, aside from access control mechanisms, OCF security specification does not include specification of secure storage of Resources, while stored at Servers. However, at rest protection for security Resources is expected to be provided through a combination of secure storage and access control. Secure storage can be accomplished through use of hardware security or encryption of data at rest. The exact implementation of secure storage is subject to a set of hardening requirements that are specified in Section 15 and may be subject to certification guidelines.

Data in transit protection, on the other hand, will be specified fully as a normative part of this specification. In transit protection may be afforded at

1. Resource layer through mechanisms such as JSON Web Encryption (JWE) and JSON Web Signatures (JWS) that allow payload protection independent of underlying transport security. This may be a necessary for transport mechanisms that cannot take advantage of DTLS for payload protection.

2. At transport layer through use of mechanisms such as DTLS. It should be noted that DTLS will provide packet by packet protection, rather than protection for the payload as whole. For instance, if the integrity of the entire payload as a whole is required, separate signature mechanisms must have already been in place before passing the packet down to the transport layer.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

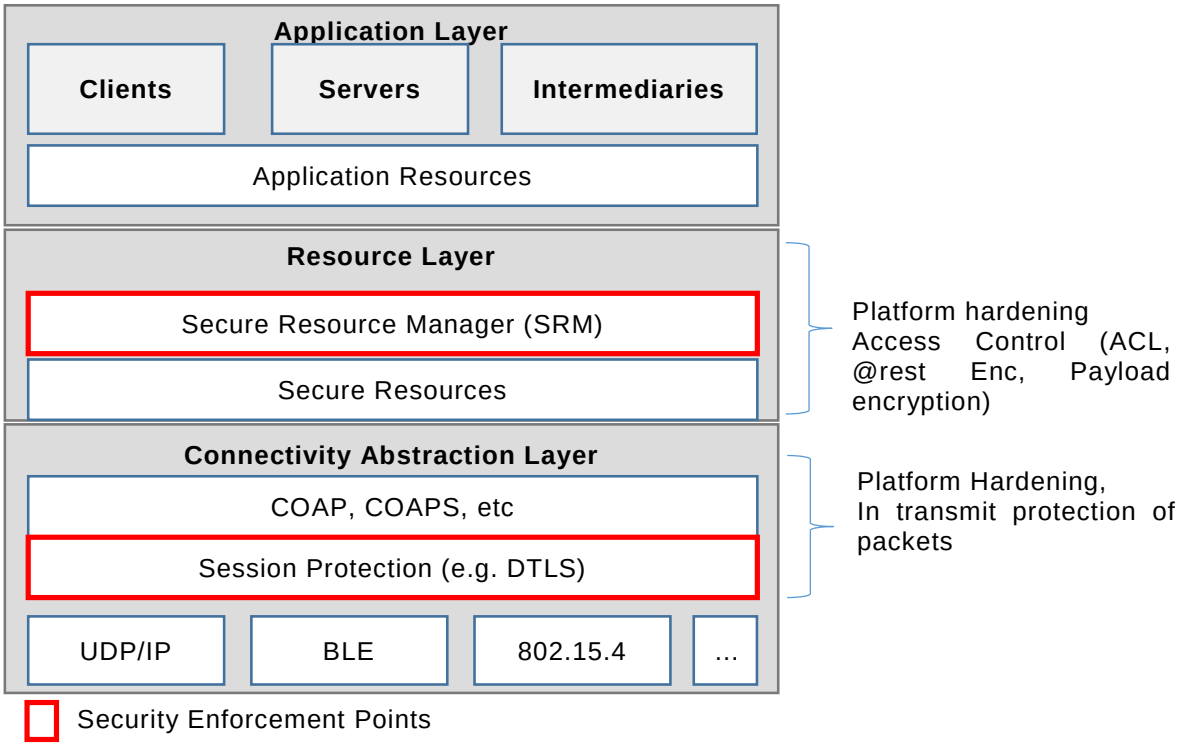

Figure 3 – OCF Security Enforcement Points

5.1 Access Control

The OCF framework assumes that Resources are hosted by a Server and are made available to Clients subject to access control and authorization mechanisms. The Resources at the end point are protected through implementation of access control, authentication and confidentiality protection. This section provide an overview of Access Control (AC) through the use of ACLs However, AC in the OCF stack is expected to be transport and connectivity abstraction layer agnostic.

Implementation of access control relies on a-priori definition of a set of access policies for the Resource. The policies may be stored by a local ACL or an Access Manager Service (AMS) in form of Access Control Entries (ACE), where each ACE defines permissions required to access a specific Resource along with an optional validity period for the granted permission. Two types of access control mechanisms can be applied:

- Subject-based access control (SBAC), where each ACE will match a subject (e.g. identity of requestor) of the requesting entity against the subject included in the policy defined for Resource. Asserting the identity of the requestor requires an authentication process.
- Role-based Access Control (RBAC), where each ACE will match a role required by policy for the Resource to a role taken by the entity requesting access. Asserting the role of the requestor requires proper authorization.

In the OCF access control model, each Resource instance is required to have an associated access control policy. This means, each Device acting as Server, needs to have an ACL for each Resource it is protecting. Lack of an ACE that matches, it results in the Resource being inaccessible.

The ACE must match both the subject (i.e. OCF Client) and the Resource requested for the ACE to apply. There are multiple ways a subject could be matched, (1) device id, (2) role or (3) wildcard. The way in which the client connects to the server may be relevant context for making access

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30118-2:2018

control decisions. Wildcard matching on authenticated vs. unauthenticated and encrypted vs. unencrypted connection allows an access policy to be broadly applied to subject classes.

Example Wildcard Matching Policy:

```
"aclist2": [
  {
      "subject": {"conntype" : "anon-clear" },
      "resources":[
          { "wc":"*" }
        ],
      "permission": 31
  },
  {
      "subject": {"conntype" : "auth-crypt" },
      "resources":[
          { "wc":"*" }
        ],
      "permission": 31
  },
]
```

Details of the format for ACL are defined in Section 12. The ACL is composed of one or more ACEs. The ACL defines the access control policy for the Devices.

It should be noted that the ACL Resource requires the same security protection as other sensitive Resources, when it comes to both storage and handling by SRM and PSI. Thus hardening of an underlying Platform (HW and SW) must be considered for protection of ACLs and as explained below ACLs may have different scoping levels and thus hardening needs to be specially considered for each scoping level. For instance a physical device may host multiple Device implementations and thus secure storage, usage and isolation of ACLs for different Servers on the same Device needs to be considered.

5.1.1 ACL Architecture

The Server examines the Resource(s) requested by the client before processing the request. The access control resources (e.g. /oic/sec/acl, /oic/sec/acl2, etc…) are searched to find one or more ACE entries that match the requestor and the requested Resources. If a match is found then permission and period constraints are applied. If more than one match is found then the logical UNION of permissions is applied to the overlapping periods.

The server uses the connection context to determine whether the subject has authenticated or not and whether data confidentiality has been applied or not. Subject matching wildcard policies can match on each aspect. If the user has authenticated, then subject matching may happen at increased granularity based on role or device identity.

Each ACE contains the permission set that will be applied for a given Resource requestor. Permissions consist of a combination of CREATE, RETREIVE, UPDATE, DELETE and NOTIFY (CRUDN) actions. Requestors authenticate as a Device and optionally operating with one or more roles. Devices may acquire elevated access permissions when asserting a role. For example, an ADMINISTRATOR role might expose additional Resources and Interfaces not normally accessible.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

5.1.1.1 Use of local ACLs

Servers may host ACL Resources locally. Local ACLs allow greater autonomy in access control processing than remote ACL processing by an Access Management Service (AMS) as described below.

The following use cases describe the operation of access control

Use Case 1: Server Device hosts 4 Resources (R1, R2, R3 and R4). Client Device D1 requests access to Resource R1 hosted at Server Device 5. ACL[0] corresponds to Resource R1 below and includes D1 as an authorized subject. Thus, Device D1 receives access to Resource R1 because the local ACL /oic/sec/acl/0 matches the request.

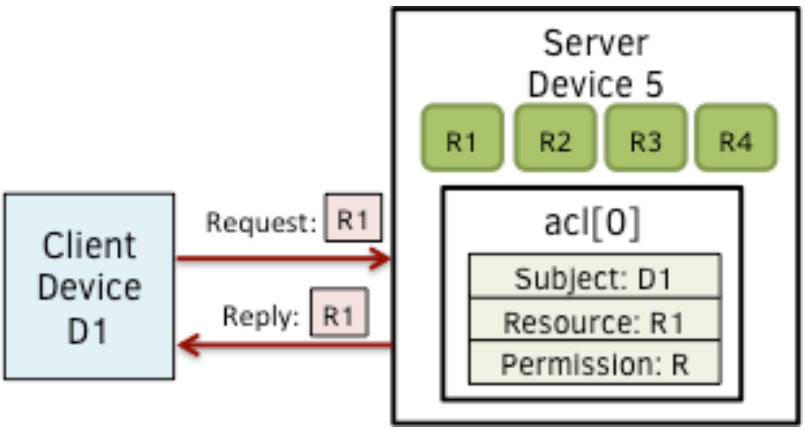

Figure 4 – Use case-1 showing simple ACL enforcement

Use Case 2: Client Device D2 access is denied because no local ACL match is found for subject D2 pertaining Resource R2 and no AMS policy is found.

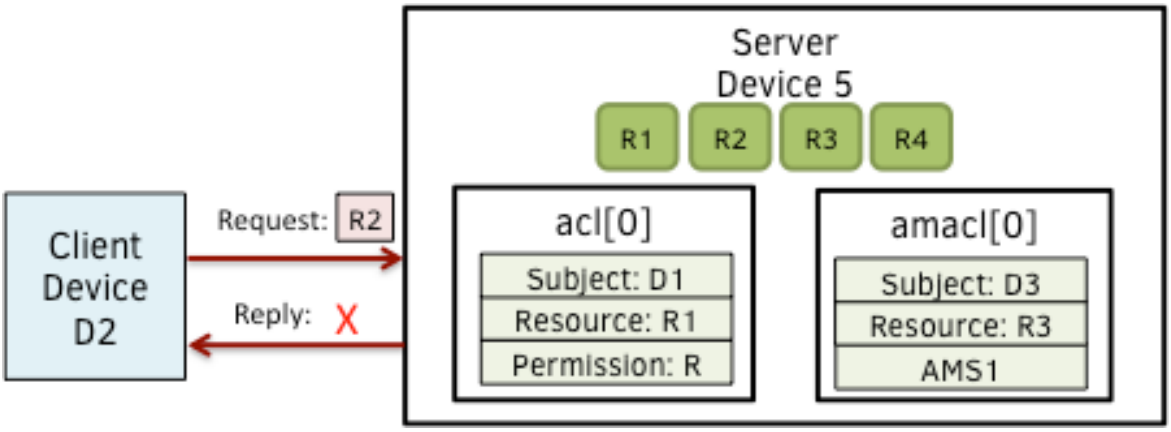

Figure 5 – Use case 2: A policy for the requested Resource is missing

5.1.1.2 Use of Access Manager Service

AMS improves ACL policy management. However, they can become a central point of failure. Due to network latency overhead, ACL processing may be slower through an AMS.

AMS centralizes access control decisions, but Server Devices retain enforcement duties. The Server shall determine which ACL mechanism to use for which Resource set. The /oic/sec/amacl Resource is an ACL structure that specifies which Resources will use an AMS to resolve access decisions. The /oic/sec/amacl may be used in concert with local ACLs (/oic/sec/acl).

The AMS is authenticated by referencing a credential issued to the device identifier contained in /oic/sec/acl2.rowneruuid.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

The Server Device may proactively open a connection to the AMS using the Device ID found in /oic/sec/acl2.rowneruuid. Alternatively, the Server may reject the Resource access request with an error, ACCESS_DENIED_REQUIRES_SACL that instructs the requestor to obtain a suitable ACE policy using a SACL Resource /oic/sec/sacl. The /oic/sec/sacl signature may be validated using the credential Resource associated with the /oic/sec/acl2.rowneruuid.

The following use cases describe access control using the AMS:

Use Case 3: Device D3 requests and receives access to Resource R3 with permission Perm1 because the /oic/sec/amacl/0 matches a policy to consult the Access Manager Server AMS1 service

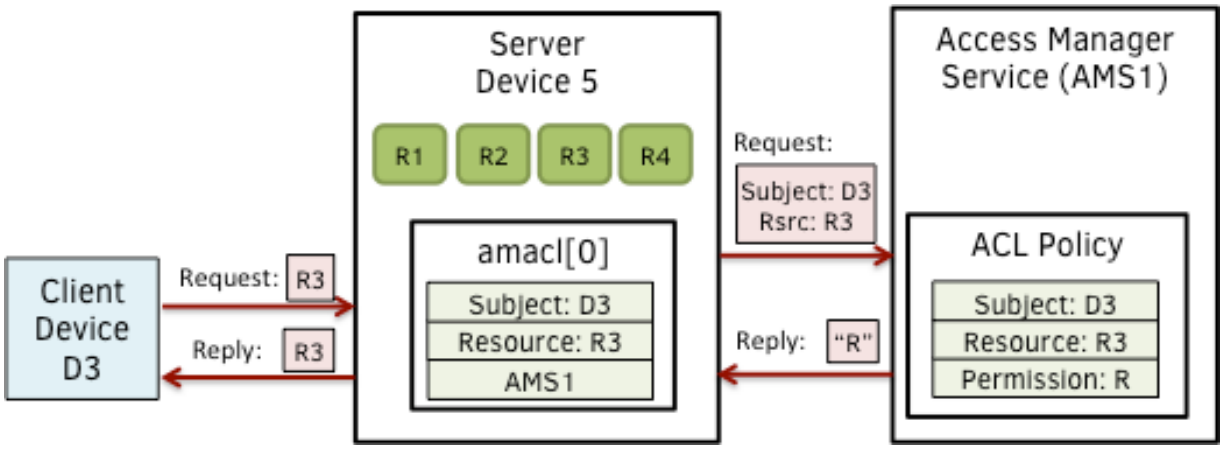

Figure 6 – Use case-3 showing Access Manager Service supported ACL

Use Case 4: Client Device D4 requests access to Resource R4 from Server Device 5, which fails to find a matching ACE and redirects the Client Device D4 to AMS1 by returning an error identifying AMS1 as a /oic/sec/sacl Resource issuer. Device D4 obtains Sacl1 signed by AMS1 and forwards the SACL to Server D5. D5 verifies the signature in the /oic/sec/sacl Resource and evaluates the ACE policy that grants Perm2 access.

ACE redirection may occur when D4 receives an error result with reason code indicating no match exists (i.e. ACCESS_DENIED_NO_ACE). D4 reads the /oic/sec/acl2 Resource to find the rowneruuid which identifies the AMS and then submits a request to be provisioned, in this example the AMS chooses to supply a SACL Resource, however it may choose to re-provision the local ACL Resources /oic/sec/acl and /oic/sec/acl2. The request is reissued subsequently. D4 is presumed to have been introduced to the AMS as part of Device onboarding or through subsequent credential provisioning actions.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

If not, a Credential Management Service (CMS) can be consulted to provision needed credentials

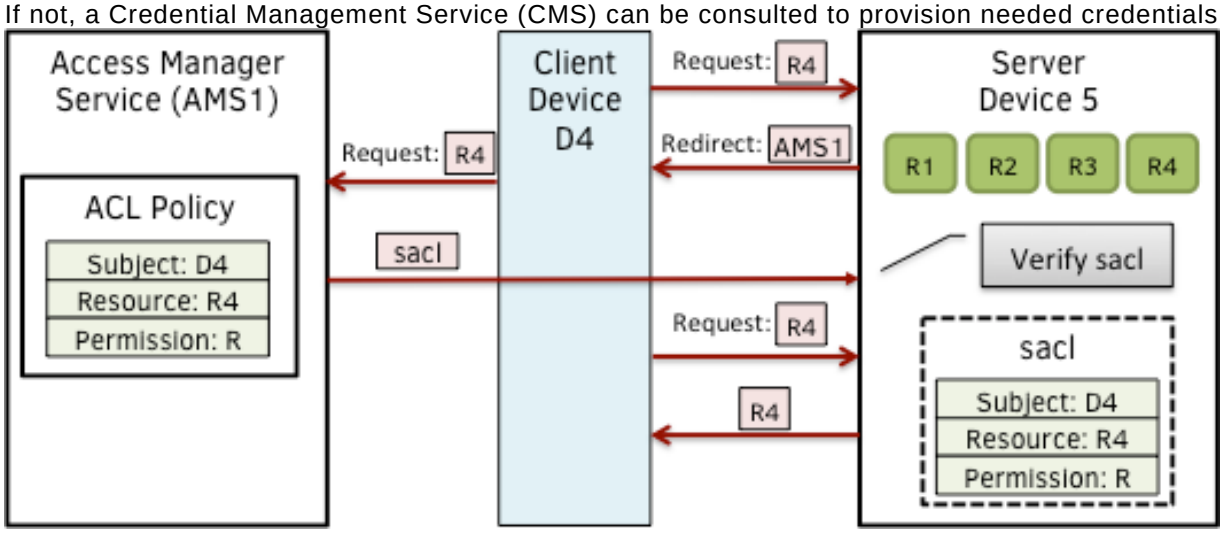

Figure 7 – Use case-4 showing dynamically obtained ACL from an AMS

5.1.2 Access Control Scoping Levels

Group Level Access - Group scope means applying AC to the group of Devices that are grouped for a specific context. Group credentials may be used when encrypting data to the group or authenticating individual Device members into the group. Group Level Access means all group members have access to group data but non-group members must be granted explicit access. Group level access may also be specified using wildcard matching.

OCF Device Level Access – OCF Device scope means applying AC to an individual Device, which may contain multiple Resources. Device level access implies accessibility extends to all Resources available to the Device identified by DeviceID. Credentials used for AC mechanisms at Device are OCF Device-specific.

OCF Resource Level Access – OCF Resource level scope means applying AC to individual Resources. Resource access requires an ACL that specifies how the entity holding the Resource (Server) shall make a decision on allowing a requesting entity (Client) to access the Resource.

Property Level Access - Property level scope means applying AC only to a property that is part of a parent Resource. This is to provide a finer granularity for AC to Resources that may require different permissions for different properties. Property level access control is achieved by creating a Resource that contains a single property. This technique allows the Resource level access control mechanisms to be used to enforce access at a finer level of granularity than would otherwise be possible.

Controlling access to static Resources where it is impractical to redesign the Resource, it may appropriate to introduce a collection Resource that references the child Resources having separate access permissions. An example is shown below, where an "oic.thing" Resource has two properties: Property-1 and Property-2 that would require different permissions.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

```
{"$schema": "http://json-schemas.org/schema#",
 "id": "http://openinterconnect.org oic.things#",
 "definitions": {
    "oic.thing": {
      "type": "object",
      "properties": {
        "Property-1": {"type": "type1"}
        "Property-2": {"type": "type2"}
          ...}
    }
  }
}
```

Properties are opaque to OCF framework

Figure 8 – Example Resource definition with opaque Properties

Currently, OCF framework treats properly level information as opaque; therefore, different permissions cannot be assigned as part of an ACL policy (e.g. read-only permission to Property-1 and write-only permission to Property-2). Thus, the "oic.thing" is split into two new Resource "oic.RsrcProp-1" and "oic.RsrcProp-2". This way, property level ACL can be achieved through use of Resource-level ACLs.

Figure 9 – Property Level Access Control

5.2 Onboarding Overview

Before a Device becomes operational in an OCF environment and is able to interact with other Devices, it needs to be appropriately onboarded. The first step in onboarding a Device is to configure the ownership where the legitimate user that owns/purchases the Device uses an Onboarding tool (OBT) and using the OBT uses one of the Owner Transfer Methods (OTM) to establish ownership. Once ownership is established, the OBT becomes the mechanism through which the Device can then be provisioned, at the end of which the Device becomes operational and is able to interact with other Devices in an OCF environment.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

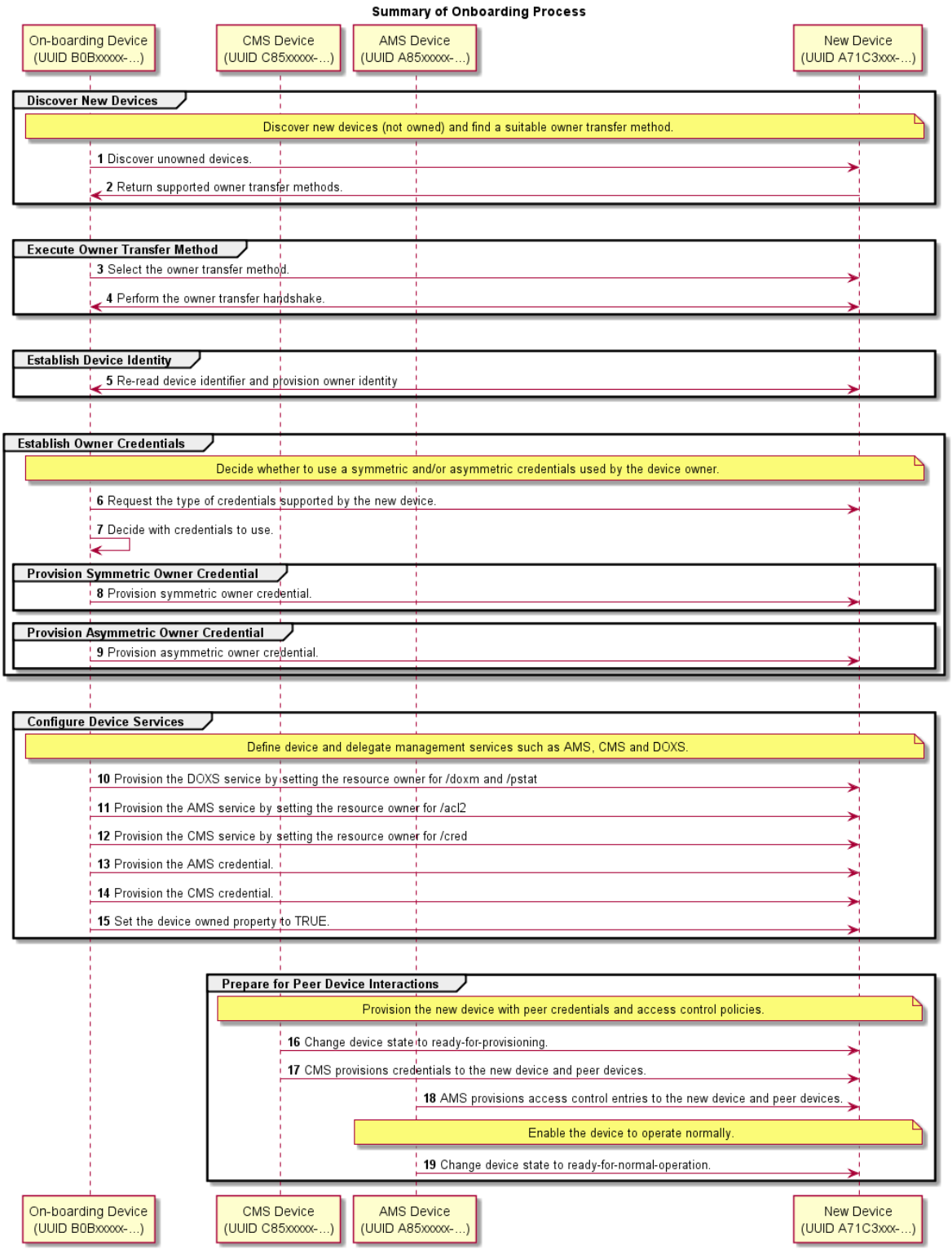

Figure 10 - Onboarding Overview

This section explains the onboarding and security provisioning process but leaves the provisioning of non-security aspects to other OCF specifications. In the context of security, all Devices are required to be provisioned with minimal security configuration that allows the Device to securely

© ISO/IEC 2018 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

interact/communicate with other Devices in an OCF environment. This minimal security configuration is defined as the Onboarded Device "Ready for Normal Operation" and is specified in Section 8.

5.2.1 OnBoarding Steps

The flowchart below shows the typical steps that are involved during onboarding. Although onboarding may include a variety of non-security related steps, the diagram focus is mainly on the security related configuration to allow a new Device to function within an OCF environment. Onboarding typically begins with the Device getting "owned" by the legitimate user/system followed by configuring the Device for the environment that it will operate in. This would include setting information such as who can access the Device and what actions can be performed as well as what permissions the Device has for interacting with other Devices.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

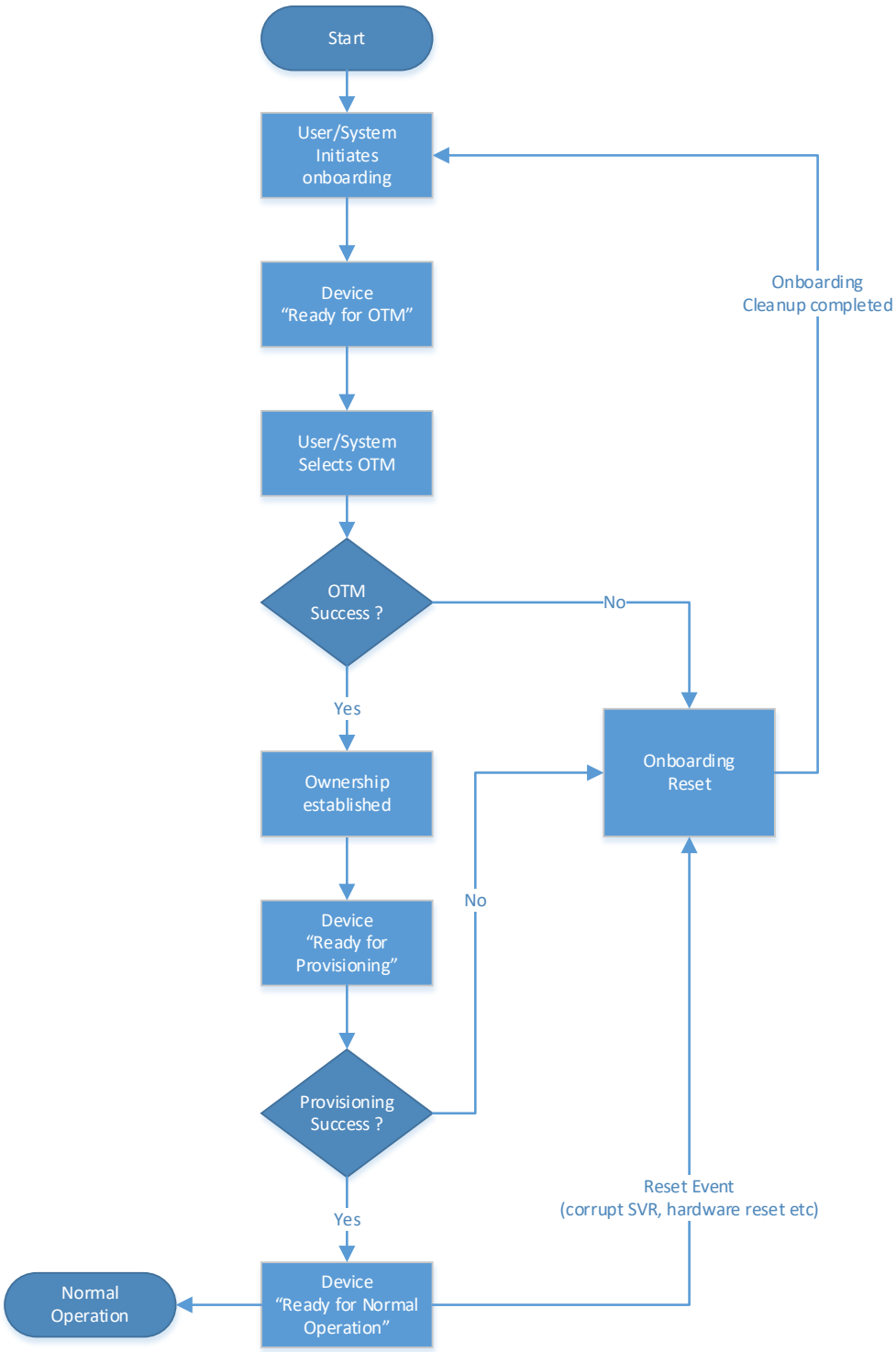

Figure 11 – OCF Onboarding Process

5.2.2 Establishing a Device Owner

The objective behind establishing Device ownership is to allow the legitimate user that owns/purchased the Device to assert itself as the owner and manager of the Device. This is done

© ISO/IEC 2018 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

through the use of an OBT that includes the creation of an ownership context between the new Device and the OBT tool and asserts operational control and management of the Device. The OBT can be considered a logical entity hosted by tools/ Servers such as a network management console, a device management tool, a network-authoring tool, a network provisioning tool, a home gateway device, or a home automation controller. A physical device hosting the OBT will be subject to some security hardening requirements, thus preserving integrity and confidentiality of any credentials being stored. The tool/Server that establishes Device ownership is referred to as the OBT.

The OBT uses one of the Owner Transfer method specified in Section 7.3 to securely establish Device ownership. The term owner transfer is used since it is assumed that even for a new Device, the ownership is transferred from the manufacturer/provider of the Device to the buyer/legitimate user of the new Device.

An owner transfer method establishes a new owner (the operator of OBT) that is authorized to manage the Device. Owner transfer establishes the following

- An Owner Credential (OC) that is provisioned by the OBT in the /oic/sec/doxm Resource of the Device. This OC allows the Device and OBT to mutually authenticate during subsequent interactions. The OC asserts the user/system's ownership of the Device by recording the credential of the OBT as the owner. The OBT also records the identity of Device as part of ownership transfer.
- The Device owner establishes trust in the Device through the OTM.
- Preparing the Device for provisioning by providing credentials that may be needed.

5.2.2.1 Preparing the Device for provisioning

Once Device ownership is established, the Device needs to be prepared for provisioning. This could be in the form of getting bootstrapping parameters (BP) that allow the Device to contact the bootstrap server (BS) and establish a secure session with the BS. The typical bootstrap parameters are as follows

- Bootstrap server (BS)/ tool metadata: This information needs to include addressing and access mechanism/ protocol to be used to access the bootstrap server. Addressing information may include Server URI or FQDN if HTTP or TCP/IP is being used to contact the Server.
- Bootstrapping credential (BC): This is the credential that the Device needs to use to contact the BS, authenticate to the BS, and establish a secure session with the BS to receive provisioning parameters from the BS. The BC may be derived from the OC depending on the type of OC.

If the OBT itself acts as the bootstrap server, the metadata for the bootstrap server may point to a service hosted by the OBT itself. In such a scenario additional BC credentials may not be needed.

5.2.3 Provisioning for Normal Operation

Once the Device has the necessary information to initiate provisioning, the next step is to provision additional security configuration that allows the Device to become operational. This can include setting various parameters and may also involve multiple steps. For example if the Device is to receive its configuration from a bootstrapping server, then the provisioning may involve connecting to the bootstrap server and receive its configuration. Also provisioning of ACL's for the various Resources hosted by the Server on the Device is done at this time. Note that the provisioning step is not limited to this stage only. Device provisioning can happen at multiple stages in the Device's operational lifecycle. However specific security related provisioning of Resource and Property state would likely happen at this stage at the end of which, each Device reaches the Onboarded Device "Ready for Normal Operation" State. The "Ready for Normal Operation" State is expected

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

to be consistent and well defined regardless of the specific OTM used or regardless of the variability in what gets provisioned. However individual OTM mechanisms and provisioning steps may specify additional configuration of Resources and Property states. The minimal mandatory configuration required for a Device to be in "Ready for Normal Operation" state is specified in Section 8.

5.3 Provisioning

Note that in general, provisioning may include processes during manufacturing and distribution of the Device as well as processes after the Device has been brought into its intended environment (parts of onboarding process). In this specification, security provisioning includes, processes after ownership transfer (even though some activities during ownership transfer and onboarding may lead to provisioning of some data in the Device) configuration of credentials for interacting with bootstrapping and provisioning services, configuration of any security related Resources and credentials for dealing with any services that the Device need to contact later on.

Once the ownership transfer is complete and bootstrap credentials are established, the Device needs to engage with the bootstrap server to be provisioned with proper security credentials and parameters. These parameters can include

- Security credentials through a credential management service (CMS), currently assumed to be deployed in the same OBT.
- Access control policies and ACLs through an ACL provisioning service (APS), currently assumed to be deployed in the same OBT, but may be part of AMS in future.

As mentioned, to accommodate a scalable and modular design, these functions are considered as services that in future could be deployed as separate servers. Currently, the deployment assumes that these services are all deployed as part of a OBT. Regardless of physical deployment scenario, the same security-hardening requirement) applies to any physical server that hosts the tools and security provisioning services discussed here.

Devices are *aware* of their security provisioning status. Self-awareness allows them to be proactive about provisioning or re-provisioning security Resources as needed to achieve the devices operational goals.

5.3.1 Provisioning a bootstrap service

The Device is discovered or programmed with the bootstrap parameters (BP), including the metadata required to discover and interact with the Bootstrap server (BS). The Device is configured with bootstrap credential (BC) required to communicate with BS securely.

In the Resource structure, the rowneruuid Property in the /oic/sec/pstat Resource identifies the bootstrap service (BSS).

When symmetric keys are used, the OC is used to derive the BC. However, when the Device is capable of using asymmetric keys for ownership transfer and other provisioning processes, there may not be a need for a cryptographic relationship between BC and OC.

Regardless of how the BC is created, the communication between Device and BS (and potentially other servers) must be done securely. For instance when a pre-shared key is used for secure connection with the Device, the oic.sec.bss service includes the oic.sec.cred Resource is provisioned with the PSK.

5.3.2 Provisioning other services

To be able to support the use of potentially different device management service hosts, each Device Secure Virtual Resource (SVR) has an associated Resource owner. The onboarding Device, also known as DOXS, provisions rowneruuid Properties with the appropriate provider identity.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

- Credential Management Service (CMS) : (/oic/sec/cred.rowneruuid)
- Access Manager Service (AMS) : (/oic/sec/acl.rowneruuid and /oic/sec/acl2.rowneruuid)

When these services are populated the Device may proactively request provisioning and verify provisioning requests are authorized. Each of the services above must be performed securely and thus require specific credentials to be provisioned. The DOXS service may initiate of any services above by signaling the service provider Device(s) or by setting the appropriate vector in the 'tm' Property of the Device's /oic/sec/pstat Resource. This will cause the Device to re-provision its credential and or access Resources

5.3.3 Credential provisioning

Several types of credential may be configured in a /oic/sec/cred Resource. Currently, they include at least the following credential types; pairwise symmetric keys, group symmetric keys, certificates, asymmetric keys and signed asymmetric keys. Keys may be provisioned by a CMS (e.g. "oic.sec.cms") or dynamically using a Diffie-Hellman key agreement protocol or through other means.

The following describe an example on how a Device can update a PSK for a secure connection. A Device may discover the need to update credentials, e.g. because a secure connection attempt fails. The Device will then need to request credential update from a CMS. The Device may enter credential-provisioning mode (e.g. /oic/sec/pstat.Cm=16) and may configure operational mode (e.g. /oic/sec/pstat.Om="1") to request an update to its credential Resource. The CMS responds with a new pairwise pre-shared key (PSK).

5.3.4 Role assignment and provisioning

The Servers, receiving requests for Resources they host, need to examine the role asserted by the Client requesting the Resource and compare that role with the constraints described in their ACLs corresponding to the services. Thus, a Client Device may need to be provisioned with one or more role credentials.

Each Device holds the role information as a Property within the credential Resource. Thus, it is possible that a Client, seeking a role provisioning, enters a mode where both its credentials and ACLs can be provisioned (if they are provisioned by the same sever!). The provisioning mode/status is typically indicated by the content of /oic/sec/pstat.

Once provisioned, the Client can assert the role it is using as described in Section 10.3.1, if it has a certificate role credential.

Alternatively, if the server has been provisioned with role information for a client, or the client has previously asserted roles to the server, the client can assert a specific role with the CoAP payload:

e.g. GET /a/light?roleid={"role":"Role-A"}

The client has no way to know in advance what roles are provisioned on the server, and must attempt an action and observe the server's response. If the response is permission denied, the client learns that either the server is not provisioned with the role, or the ACLs are misconfigured. If no specific role is specified in the CoAP payload, all provisioned roles are used in ACL enforcement. When a server has multiple roles provisioned for a client, access to a Resource is granted if it would be granted under any of the roles.

5.3.5 ACL provisioning

During ACL provisioning, the Device establishes a secure connection to an APS (or bootstrap server, if it is hosting the APS). The APS will instantiate or update Device ACLs according to the ACL policy.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

The Device and APS may establish an observer relationship such that when a change to the ACL policy is detected; the Device is notified triggering ACL provisioning.

The APS (e.g. rt="oic.sec.aps") may digitally sign an ACL as part of issuing a /oic/sec/sacl Resource. The public key used by Servers to verify the signature may be provisioned as part of credential provisioning. A /oic/sec/cred Resource with an asymmetric key type or signed asymmetric key type is used. The PublicData Property contains the APS's public key.

5.4 Secure Resource Manager (SRM)

SRM plays a key role in the overall security operation. In short, SRM performs both management of SVR and access control for requests to access and manipulate Resources. SRM consists of 3 main functional elements:

- A Resource manager (RM): responsible for 1) Loading SVRs from persistent storage (using PSI) as needed. 2) Supplying the Policy Engine (PE) with Resources upon request. 3) Responding to requests for SVRs. While the SVRs are in SRM memory, the SVRs are in a format that is consistent with device-specific data store format. However, the RM will use JSON format to marshal SVR data structures before be passed to PSI for storage, or travel off-device.

- A Policy Engine (PE) that takes requests for access to SVRs and based on access control policies responds to the requests with either "ACCESS_GRANTED" or "ACCESS_DENIED". To make the access decisions, the PE consults the appropriate ACL and looks for best Access Control Entry (ACE) that can serve the request given the subject (Device or role) that was authenticated by DTLS.

- Persistent Storage Interface (PSI): PSI provides a set of APIs for the RM to manipulate files in its own memory and storage. The SRM design is modular such that it may be implemented in the Platform's secure execution environment; if available.

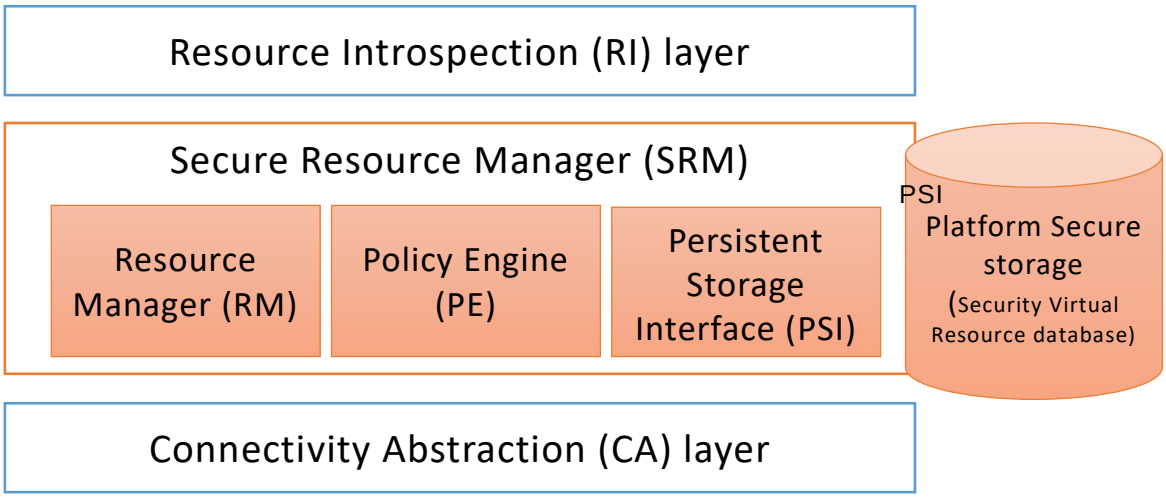

Figure 12 – OCF's SRM Architecture

5.5 Credential Overview

Devices may use credentials to prove the identity and role(s) of the parties in bidirectional communication. Credentials can be symmetric or asymmetric. Each device stores secret and public parts of its own credentials where applicable, as well as credentials for other devices that have been provided by the OBT or a CMS. These credentials are then used in the establishment of

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30118-2:2018

secure communication sessions (e.g. using DTLS) to validate the identities of the participating parties. Role credentials are used once an authenticated session is established, to assert one or more roles for a device.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

6 Security for the Discovery Process

The main function of a discovery mechanism is to provide Universal Resource Identifiers (URIs, called links) for the Resources hosted by the Server, complemented by attributes about those Resources and possible further link relations. (in accordance to Section 10 in OCF Core Specification)

6.1 Security Considerations for Discovery

When defining discovery process, care must be taken that only a minimum set of Resources are exposed to the discovering entity without violating security of sensitive information or privacy requirements of the application at hand. This includes both data included in the Resources, as well as the corresponding metadata.

To achieve extensibility and scalability, this specification does not provide a mandate on discoverability of each individual Resource. Instead, the Server holding the Resource will rely on ACLs for each Resource to determine if the requester (the Client) is authorized to see/handle any of the Resources.

The /oic/sec/acl2 Resource contains ACL entries governing access to the Server hosted Resources. (See Section 13.4)

Aside from the privacy and discoverability of Resources from ACL point of view, the discovery process itself needs to be secured. This specification sets the following requirements for the discovery process:

1. Providing integrity protection for discovered Resources.

2. Providing confidentiality protection for discovered Resources that are considered sensitive.

The discovery of Resources is done by doing a RETRIEVE operation (either unicast or multicast) on the known Resource "/oic/res".

The discovery request is sent over a non-secure channel (multicast or unicast without DTLS), a Server cannot determine the identity of the requester. In such cases, a Server that wants to authenticate the Client before responding can list the secure discovery URI (e.g. coaps://IP:PORT/oic/res) in the unsecured /oic/res response. This means the secure discovery URI is by default discoverable by any Client. The Client will then be required to send a separate unicast request using DTLS to the secure discovery URI.

For secure discovery, any Resource that has an associated ACL2 will be listed in the response to /oic/res if and only if the Client has permissions to perform at least one of the CRUDN operations (i.e. the bitwise OR of the CRUDN flags must be true).

For example, a Client with DeviceId "d1" makes a RETRIEVE request on the "/door" Resource hosted on a Server with DeviceId "d3" where d3 has the ACL2s below:

```
{
    "aclist2": [
      {
        "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
        "resources": [{"href":"/door"}],
        "permission": 2, // RETRIEVE
        "aceid": 1
      }
    ],
    "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
```


© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

```
{
    "aclist2": [
      {
        "subject": {"authority": "owner", "role": "owner"}
        "resources": [{"href":"/door"}],
        "permission": 2, // RETRIEVE
        "aceid": 2
      }
    ],
    "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
{
    "aclist2": [
      {
        "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
        "resources": [{"href":"/door/lock"}],
        "permission": 4, // UPDATE
        "aceid": 3
      }
    ],
    "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
{
    "aclist2": [
      {
        "subject": {"conntype": "anon-clear"},
        "resources": [{"href":"/light"}],
        "permission": 2, // RETRIEVE
        "aceid": 4
      }
    ],
    "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
```

The ACL indicates that Client "d1" has RETRIEVE permissions on the Resource. Hence when device "d1" does a discovery on the /oic/res Resource of the Server "d3", the response will include the URI of the "/door" Resource metadata. Client "d2" will have access to both the Resources. ACE2 will prevent "d4" from update.

Discovery results delivered to d1 regarding d3's /oic/res Resource from the secure Interface:

```
[
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.b", "oic.ll"],
     "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1",
  }
]
```

Discovery results delivered to d2 regarding d3's /oic/res Resource from the secure Interface:

```
[
  {
    "href": "/door",
    "rt": ["oic.r.door"],
    "if": ["oic.if.b", "oic.ll"],
     "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
```


© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

```
  },
  {
    "href": "/door/lock",
    "rt": ["oic.r.lock"],
    "if": ["oic.if.b"],
    "type": ["application/json", "application/exi+xml"]
  }
]
```

Discovery results delivered to d4 regarding d3's /oic/res Resource from the secure Interface:

```
[
  {
    "href": "/door/lock",
    "rt": ["oic.r.lock"],
    "if": ["oic.if.b"],
    "type": ["application/json", "application/exi+xml"],
    "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
  }
]
```

Discovery results delivered to any device regarding d3's /oic/res Resource from the unsecure Interface:

```
[
  {
    "di": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1",
    "href": "/light",
    "rt": ["oic.r.light"],
    "if": ["oic.if.s"]
  }
]
```


© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

7 Security Provisioning

7.1 Device Identity

Each Device, which is a logical device, is identified with a device ID.

Devices shall be identified by a Device ID value that is established as part of device onboarding. The /oic/sec/doxm Resource specifies the Device ID format (e.g. urn:uuid). Device IDs shall be unique within the scope of operation of the corresponding OCF network, and should be universally unique. Device ID uniqueness within the network shall be enforced at device onboarding. A Device OBT shall verify the chosen new device identifier does not conflict with other devices previously introduced into the network.

Devices maintain an association of Device ID and cryptographic credential using a /oic/sec/cred Resource. Devices regard the /oic/sec/cred Resource as authoritative when verifying authentication credentials of a peer device.

A Device maintains its device ID in the /oic/sec/doxm Resource. It maintains a list of credentials, both its own and other device credentials, in the /oic/sec/cred Resource. The device ID can be used to distinguish between a device's own credential, and credentials for other devices. Furthermore, the /oic/sec/cred Resource may contain multiple credentials for the device.

Device ID shall be:

- Unique
- Immutable
- Verifiable

When using manufacturer certificates, the certificate should bind the ID to the stored secret in the device as described later in this section.

A physical device, referred to as a Platform in OCF specifications, may host multiple Devices. The Platform is identified by a Platform ID. The Platform ID shall be globally unique and inserted in the device in an integrity protected manner (e.g. inside secure storage or signed and verified).

Note: An OCF Platform may have a secure execution environment, which shall be used to secure unique identifiers and secrets. If a Platform hosts multiple devices, some mechanism is needed to provide each Device with the appropriate and separate security.

7.1.1 Device Identity for Devices with UAID

When a manufacturer certificate is used with certificates chaining to an OCF root CA (as specified in Section 7.1.1), the manufacturer shall include a Platform ID inside the certificate subject CN field. In such cases, the device ID may be created according to the Unique Authenticable IDentifier (UAID) scheme defined in this section.

For identifying and protecting Devices, the Platform Secure Execution Environment (SEE) may opt to generate new Dynamic Public Key Pair (DPKP) for each Device it is hosting, or it may opt to simply use the same public key credentials embedded by manufacturer; Embedded Platform Credential (EPC). In either case, the Platform SEE will use its Random Number Generator (RNG) to create a device identity called UAID for each Device. The UAID is generated using eitherEPC only or the combnation of DPC and EPC if both are available. When both are available, the Platform shall use both key pairs to generate the UAID as described in this section.

The Device ID is formed from the device's public keys and associated OCF Cipher Suite. The Device ID is formed by:

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

1. Determining the OCF Cipher Suite of the Dynamic Public Key. The Cipher Suite curve must match the usage of the AlgorithmIdentifier used in SubjectPublicKeyInfo as intended for use with Device security mechanisms. Use the encoding of the CipherSuite as the 'csid' value in the following calculations. Note that if the OCF Cipher Suite for Dynamic Public key is different from the ciphersuite indicated in the Platform certificate (EPC), the OCF Cipher Suite shall be used below.

2. From EPC extract the value of embedded public key. The value should correspond to the value of subjectPublicKey defined in SubjectPublicKeyInfo of the certificate. In the following we refer to this as EPK. If the public key is extracted from a certificate, validate that the AlgorithmIdentifier matches the expected value for the CipherSuite within the certificate.

3. From DPC Extract the value of the public key. The value should correspond to the value of subjectPublicKey defined in SubjectPublicKeyInfo. In the following we refer to this as DPK.

4. Using the hash for the Cipher Suite calculate:
   h = hash('uaid' | csid | EPK| DPK | <other_info>)

Other_info could be 1) device type as indicated in /oic/d (could be read-only and set by manufacturer), 2) in case there are two sets of public key pairs (one embedded, and one dynamically generated), both public keys would be included.

5. Truncate to 128 bits by taking the first 128 bits of h
   UAID = h[0:16] # leftmost 16 octets

6. Convert the binary UAID to a ASCII string by
   USID = base27encode(UAID)

```
def base_N_encode(octets, alphabet):
long_int = string_to_int( octets )
    text_out = ''
    while long_int > 0:
        long_int, remainder = divmod(long_int, len(alphabet))
        text_out = alphabet[remainder] + text_out
    return text_out

b27chars = 'ABCDEFGHJKMNPQRTWXYZ2346789'
def b27encode(octet_string):
    """Encode a octet string using 27 characters. """

    return base_N_encode(octet_string, _b27chars )
```

7. Append the string value of USID to 'urn:usid:' to form the final string value of the Device ID
   urn:usid:ABXW....

Whenever the public key is encoded the format described in RFC 7250 for SubjectPublicKeyInfo shall be used.

7.1.1.1 Validation of UAID

To be able to use the newly generated Device ID (UAID) and public key pair (DPC), the device Platform shall use the embedded private key (corresponding to manufacturer embedded public key and certificate) to sign a token vouching for the fact that it (the Platform) has in fact generated the DPC and UAID and thus deferring the liability of the use of the DPC to the new device owner. This also allows the ecosystem to extend the trust from manufacturer certificate to a device issued certificate for use in the new DPC and UAID. The degree of trust is in dependent of the level of hardening of the device SEE.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

Dev_Token=Info, Signature(hash(info))

Signature algorithm=ECDSA (can be same algorithm as that in EPC or that possible for DPC)

Hash algorithm=SHA256

Info=UAID| <Platform ID> | UAID_generation_data | validity

UAID_generation_data=data passed to the hash algorithm used to generate UAID.

Validity=validity period in days (how long the token will be valid)

7.2 Device Ownership

This is an informative section. Devices are logical entities that are security endpoints that have an identity that is authenticable using cryptographic credentials. A Device is 'un-owned' when it is first initialized. Establishing device ownership is a process by which the device asserts it's identity to an OBT and the OBT asserts its identity to the device. This exchange results in the device changing its ownership state, thereby preventing a different OBT from asserting administrative control over the device.

The ownership transfer process starts with the OBT discovering a new device that is "un-owned" through examination of the "Owned" Property of the /oic/sec/doxm Resource of the new device. At the end of ownership transfer, the following is accomplished:

1. Establish a secure session between new device and the OBT.
2. Optionally asserts any of the following:
   a. Proximity (using PIN) of the OBT to the Platform.
   b. Manufacturer's certificate asserting Platform vendor, model and other Platform specific attributes.
3. Determines the device identifier.
4. Determines the device owner.
5. Specifies the device owner (e.g. Device ID of the OBT).
6. Provisions the device with owner's credentials.
7. Sets the 'Owned" state of the new device to TRUE.

7.3 Device Ownership Transfer Methods

7.3.1 OTM implementation requirements

This document provides specifications for several methods for ownership transfer. Implementation of each individual ownership transfer method is considered optional. However, each device shall implement at least one of the ownership transfer methods not including vendor specific methods.

All owner transfer methods (OTMs) included in this document are considered optional. Each vendor is required to choose and implement at least one of the OTMs specified in this specification. The OCF, does however, anticipate vendor-specific approaches will exist. Should the vendor wish to have interoperability between an vendor-specific owner transfer method and and OBTs from other vendors, the vendor must work directly with OBT vendors to ensure interoperability. Notwithstanding, standardization of OTMs is the preferred approach. In such cases, a set of guidelines is provided below to help vendors in designing vendor-specific OTMs. (See Section 7.3.6).

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

The device owner transfer method (doxm) Resource is extensible to accommodate vendor-defined methods. All OTM methods shall facilitate allowing the OBT to determine which OC is most appropriate for a given new device within the constraints of the capabilities of the device. The OBT will query the credential types that the new device supports and allow the OBT to select the credential type from within device constraints.

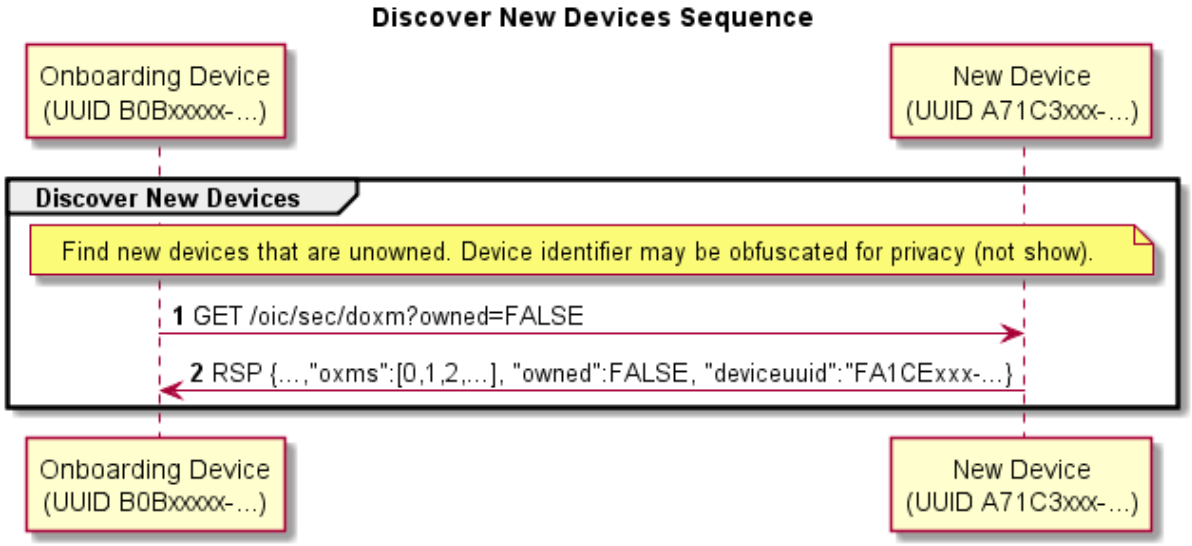

Figure 13 - Discover New Device Sequence

Step	Description
1	The OBT queries to see if the new device is not yet owned.
2	The new device returns the /oic/sec/doxm Resource containing ownership status and supported owner transfer methods. It also contains a temporal device ID that may change subsequent to successful owner transfer. The device should supply a temporal ID to facilitate discovery as a guest device. Section 7.3.9 provides security considerations regarding selecting an owner transfer method.

Table 2 - Discover New Device Details

Vendor-specific device owner transfer methods shall adhere to the /oic/sec/doxm Resource specification for OCs that results from vendor-specific device owner transfer. Vendor-specific methods should include provisions for establishing trust in the new device by the OBT an optionally establishing trust in the OBT by the new device.

The end state of a vendor-specific owner transfer method shall allow the new device to authenticate to the OBT and the OBT to authenticate to the new device.

Additional provisioning steps may be applied subsequent to owner transfer success leveraging the established session, but such provisioning steps are technically considered provisioning steps that an OBT may not anticipate hence may be invalidated by OBT provisioning.

7.3.2 SharedKey Credential Calculation

The SharedKey credential is derived using a PRF that accepts the key_block value resulting from the DTLS handshake used for onboarding. The Server and Device OBT shall use the following calculation to ensure interoperability across vendor products:

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

SharedKey = *PRF*(Secret, Message);

Where:

- PRF shall use TLS 1.2 PRF defined by RFC5246 section 5.
- Secret is the key_block resulting from the DTLS handshake
  - See RFC5246 Section 6.3
  - The length of key_block depends on cipher suite.
    - (e.g. 96 bytes for TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
      40 bytes for TLS_PSK_WITH_AES_128_CCM_8)
- Message is a concatenation of the following:
  - DoxmType string for the current onboarding method (e.g. "oic.sec.doxm.jw")
    - See "Section 13.1.1 OCF defined owner transfer methods for specific DoxmTypes"
  - OwnerID is a UUID identifying the device owner identifier and the device that maintains SharedKey.
    - Use raw bytes as specified in RFC4122 section 4.1.2
  - Device ID is new device's UUID Device ID
    - Use raw bytes as specified in RFC4122 section 4.1.2
- SharedKey Length will be 32 octets.
  - If subsequent DTLS sessions use 128 bit encryption cipher suites the leftmsot 16 octets will be used. DTLS sessions using 256 bit encryption cipher suites will use all 32 octets.

7.3.3 Certificate Credential Generation

The Certificate Credential will be used by Devices for secure bidirectional communication. The certificates will be issued by a CMS or an external certificate authority (CA). This CA will be used to mutually establish the authenticity of the Device. The onboarding details for certificate generation will be specified in a later version of this specification.

7.3.4 Just-Works Owner Transfer Method

Just-works owner transfer method creates a symmetric key credential that is a pre-shared key used to establish a secure connection through which a device should be provisioned for use within the owner's network. Provisioning additional credentials and Resources is a typical step following ownership establishment. The pre-shared key is called SharedKey.

The ownership transfer process starts with the OBT discovering a new device that is "un-owned" through examination of the "owned" Property of the /oic/sec/doxm Resource at the Device hosted by the new device.

Once the OBT asserts that the device is un-owned, when performing the Just-works owner transfer method, the OBT relies on DTLS key exchange process where an anonymous Elliptic Curve Diffie-Hellman (ECDH) is used as a key agreement protocol.

The following OCF-defined vendor-specific ciphersuites are used for the Just-works owner transfer method.

TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256

These are not registered in IANA, the ciphersuite values are assigned from the reserved area for private use (0xFF00 ~ 0xFFFF). The assigned values are 0xFF00 and 0xFF01, respectively.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

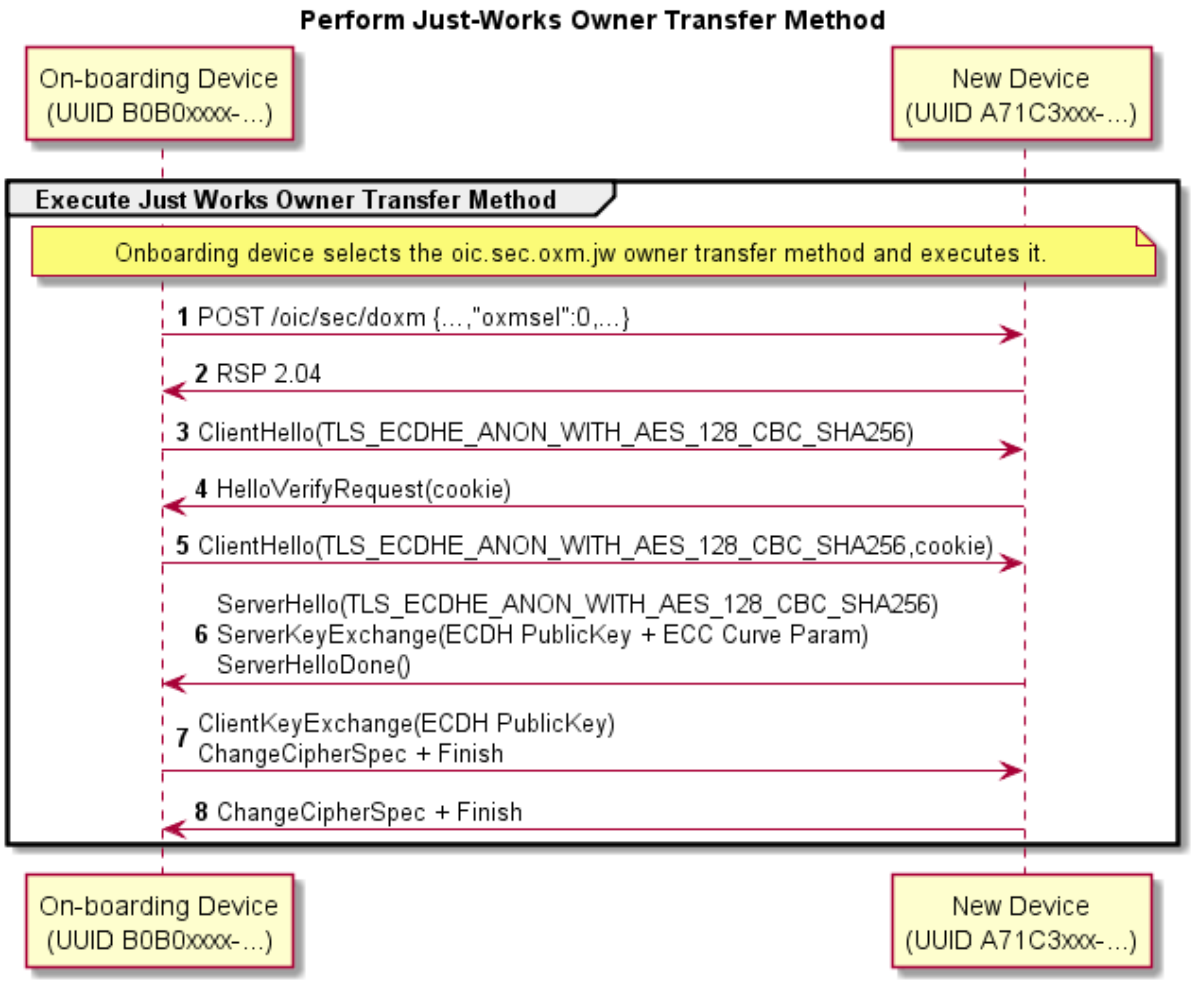

Figure 14 – A Just Works Owner Transfer Method

Step	Description
1, 2	The OBT notifies the Device that it selected the 'Just Works' method.
3 - 8	A DTLS session is established using anonymous Diffie-Hellman. Note: This method assumes the operator is aware of the potential for man-in-the-middle attack and has taken precautions to perform the method in a clean-room network.

Table 3 – A Just Works Owner Transfer Method Details

7.3.4.1 Security Considerations

Anonymous Diffie-Hellman key agreement is subject to a man-in-the-middle attacker. Use of this method presumes that both the OBT and the new device perform the 'just-works' method assumes onboarding happens in a relatively safe environment absent of an attack device.

This method doesn't have a trustworthy way to prove the device ID asserted is reliably bound to the device.

The new device should use a temporal device ID prior to transitioning to an owned device while it is considered a guest device to prevent privacy sensitive tracking. The device asserts a non-temporal device ID that could differ from the temporal value during the secure session in which

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018

owner transfer exchange takes place. The OBT will verify the asserted Device ID does not conflict with a Device ID already in use. If it is already in use the existing credentials are used to establish a secure session.

An un-owned Device that also has established device credentials might be an indication of a corrupted or compromised device.

7.3.5 Random PIN Based Owner Transfer Method

The Random PIN method establishes physical proximity between the new device and the OBT can prevent man-in-the-middle attacks. The Device generates a random number that is communicated to the OBT over an out-of-band channel. The definition of out-of-band communications channel is outside the scope of the definition of device owner transfer methods. The OBT and new Device use the PIN in a key exchange as evidence that someone authorized the transfer of ownership by having physical access to the new Device via the out-of-band-channel.

7.3.5.1 Random PIN Owner Transfer Sequence

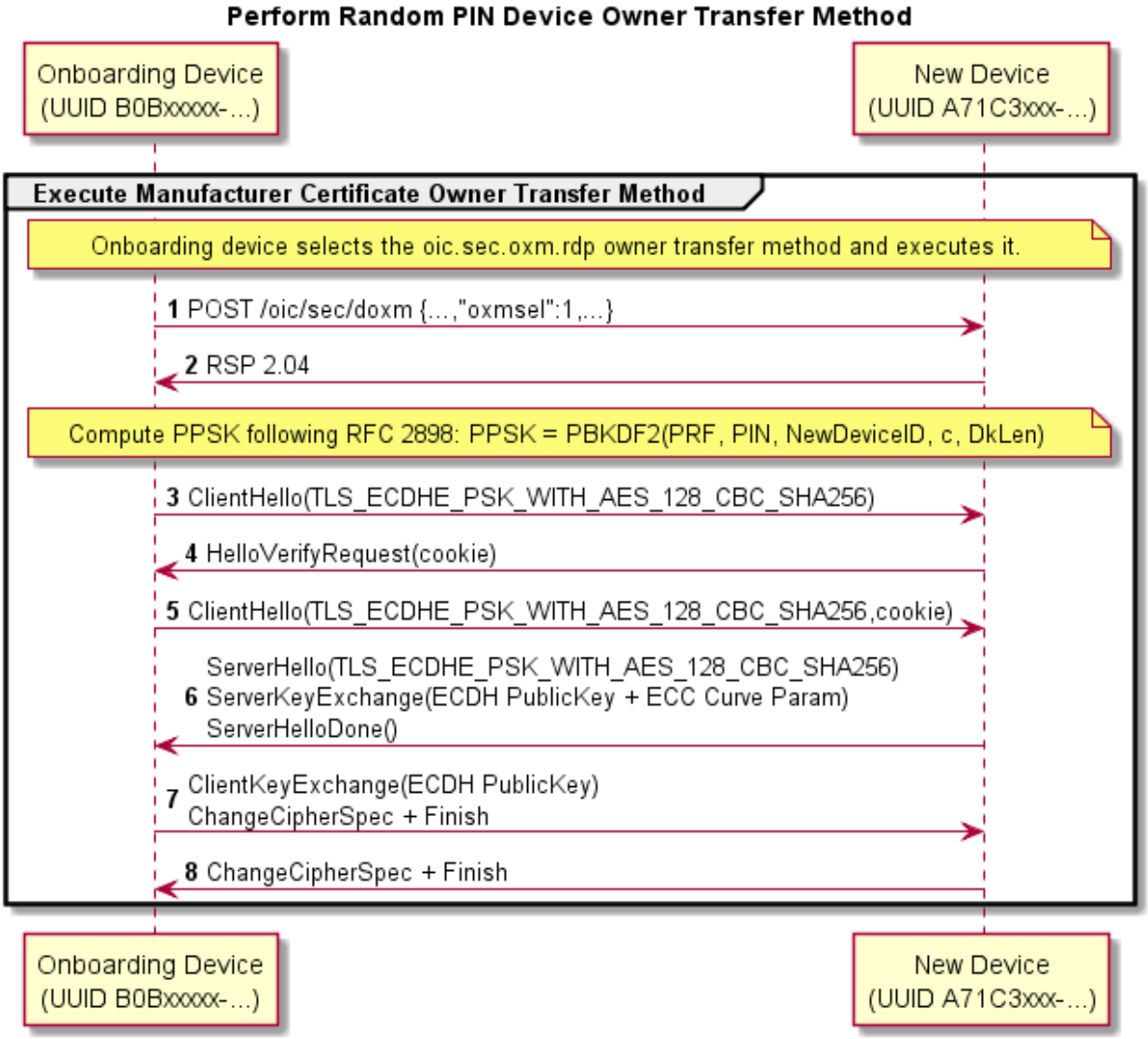

Figure 15 – Random PIN-based Owner Transfer Method

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30118-2:2018