
**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

*IT Standards
(<https://standards.iteh.ai>)
Document Preview*

[ISO/IEC 30118-2:2018](https://standards.iteh.ai/catalog/standards/iso/af8de57a-4264-4bdf-afe3-c79aefcc03d8/iso-iec-30118-2-2018)

<https://standards.iteh.ai/catalog/standards/iso/af8de57a-4264-4bdf-afe3-c79aefcc03d8/iso-iec-30118-2-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 30118-2:2018](https://standards.iteh.ai/catalog/standards/iso/af8de57a-4264-4bdf-afe3-c79aefcc03d8/iso-iec-30118-2-2018)

<https://standards.iteh.ai/catalog/standards/iso/af8de57a-4264-4bdf-afe3-c79aefcc03d8/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

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.

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

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