
**Information technology — Open
Connectivity Foundation (OCF)
Specification —**

**Part 2:
Security specification**

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

Partie 2: Spécification de sécurité





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	ix
Introduction.....	x
1 Scope	1
2 Normative References	1
3 Terms, definitions and abbreviated terms.....	3
3.1 Terms and definitions	3
3.2 Symbols and abbreviated terms.....	5
4 Document conventions and organization.....	7
4.1 Conventions	7
4.2 Notation.....	7
4.3 Data types	8
4.4 Document structure	8
5 Security overview	8
5.1 Preamble	8
5.2 Access control	10
5.2.1 Access control general.....	10
5.2.2 ACL architecture.....	11
5.3 Onboarding overview.....	12
5.3.1 Onboarding general.....	12
5.3.2 Onboarding steps	14
5.3.3 Establishing a Device Owner	15
5.3.4 Provisioning for Normal Operation.....	16
5.3.5 OCF Compliance Management System.....	16
5.4 Provisioning.....	16
5.4.1 Provisioning general	16
5.4.2 Access control provisioning	17
5.4.3 Credential provisioning.....	17
5.4.4 Role provisioning	17
5.5 Secure Resource Manager (SRM).....	17
5.6 Credential overview	18
5.7 Event logging	18
5.7.1 Event logging general	18
6 Security for the discovery process.....	19
6.1 Preamble	19
6.2 Security considerations for discovery.....	19
7 Security provisioning	21
7.1 Device identity	21
7.1.1 General Device identity	21
7.1.2 Device identity for devices with UAID [Deprecated]	21
7.2 Device ownership.....	21
7.3 Device Ownership Transfer Methods	22
7.3.1 OTM implementation requirements.....	22
7.3.2 SharedKey credential calculation	23
7.3.3 Certificate credential generation	24
7.3.4 Just-Works OTM	24

7.3.5	Random PIN based OTM.....	25
7.3.6	Manufacturer Certificate Based OTM.....	28
7.3.7	Vendor specific OTMs	30
7.3.8	Establishing Owner Credentials	31
7.3.9	Security profile assignment	34
7.4	Provisioning.....	35
7.4.1	Provisioning flows.....	35
8	Device Onboarding state definitions	36
8.1	Device Onboarding general.....	36
8.2	Device Onboarding-Reset state definition.....	37
8.3	Device Ready-for-OTM State definition.....	38
8.4	Device Ready-for-Provisioning State Definition.....	39
8.5	Device Ready-for-Normal-Operation state definition	39
8.6	Device Soft Reset State definition	40
9	Security Credential management.....	41
9.1	Preamble	41
9.2	Credential lifecycle	41
9.2.1	Credential lifecycle general	41
9.2.2	Creation	41
9.2.3	Deletion.....	41
9.2.4	Refresh.....	41
9.2.5	Revocation	42
9.3	Credential types	42
9.3.1	Preamble	42
9.3.2	Pair-wise symmetric key credentials	42
9.3.3	Group symmetric key credentials	42
9.3.4	Asymmetric authentication key credentials	43
9.3.5	Asymmetric Key Encryption Key credentials	43
9.3.6	Certificate credentials	44
9.3.7	Password credentials	44
9.4	Certificate based key management	44
9.4.1	Overview	44
9.4.2	X.509 digital certificate profiles	45
9.4.3	Certificate Revocation List (CRL) Profile [deprecated].....	54
9.4.4	Resource model.....	54
9.4.5	Certificate provisioning.....	54
9.4.6	CRL provisioning [deprecated]	55
10	Device authentication.....	55
10.1	Device authentication general.....	55
10.2	Device authentication with symmetric key credentials.....	56
10.3	Device authentication with raw asymmetric key credentials	56
10.4	Device authentication with certificates.....	56
10.4.1	Device authentication with certificates general.....	56
10.4.2	Role assertion with certificates	57
10.4.3	OCF PKI Roots	58
10.4.4	PKI Trust Store	58
10.4.5	Path Validation and extension processing.....	59

11	Message integrity and confidentiality	59
11.1	Preamble	59
11.2	Session protection with DTLS	59
11.2.1	DTLS protection general	59
11.2.2	Unicast session semantics	59
11.3	Cipher suites	59
11.3.1	Cipher suites general	59
11.3.2	Cipher suites for Device Ownership Transfer	60
11.3.3	Cipher Suites for symmetric keys	60
11.3.4	Cipher auites for asymmetric credentials	61
12	Access control	62
12.1	ACL generation and management	62
12.2	ACL evaluation and enforcement	62
12.2.1	ACL evaluation and enforcement general	62
12.2.2	Host reference matching	62
12.2.3	Resource wildcard matching.....	62
12.2.4	Multiple criteria matching	63
12.2.5	Subject matching using wildcards.....	63
12.2.6	Subject matching using roles	64
12.2.7	ACL evaluation	64
13	Security Resources	66
13.1	Security Resources general	66
13.2	Device Owner Transfer Resource.....	68
13.2.1	Device Owner Transfer Resource General	68
13.2.2	OCF defined OTMs.....	71
13.3	Credential Resource	71
13.3.1	Credential Resource general.....	71
13.3.2	Properties of the Credential Resource	76
13.3.3	Key formatting	78
13.3.4	Credential Refresh Method details [deprecated].....	79
13.4	Certificate Revocation List	79
13.4.1	CRL Resource definition [deprecated]	79
13.5	ACL Resources	79
13.5.1	ACL Resources general.....	79
13.5.2	OCF Access Control List (ACL) BNF defines ACL structures.	79
13.5.3	ACL Resource	80
13.6	Access Manager ACL Resource [deprecated]	85
13.7	Signed ACL Resource [deprecated]	85
13.8	Provisioning Status Resource.....	85
13.9	Certificate Signing Request Resource	91
13.10	Roles Resource	91
13.11	Auditable Events List Resource	93
13.11.1	Auditable Events List Resource general	93
13.12	Security Virtual Resources (SVRs) and Access Policy	96
13.13	SVRs, discoverability and OCF Endpoints	97
13.14	Additional privacy consideration for Core Resources	97
13.15	Easy Setup Resource Device state	98

13.16	List of Auditable Events	100
13.17	Security Domain Information Resource	102
14	Security hardening guidelines/ execution environment security	103
14.1	Preamble	103
14.2	Execution environment elements	103
14.2.1	Execution environment elements general	103
14.2.2	Secure storage	103
14.2.3	Secure execution engine	106
14.2.4	Trusted input/output paths	106
14.2.5	Secure clock	106
14.2.6	Approved algorithms	107
14.2.7	Hardware tamper protection	107
14.3	Secure Boot	107
14.3.1	Concept of software module authentication	107
14.3.2	Secure Boot process	109
14.3.3	Robustness requirements	109
14.4	Attestation	110
14.5	Software Update	110
14.5.1	Overview	110
14.5.2	Recognition of current differences	110
14.5.3	Software Version Validation	111
14.5.4	Software Update	111
14.5.5	Recommended usage	112
14.6	Non-OCF Endpoint interoperability	112
14.7	Security levels	112
14.8	Security Profiles	113
14.8.1	Security Profiles general	113
14.8.2	Identification of Security Profiles (Normative)	114
14.8.3	Security Profiles	115
15	Device Type specific requirements	120
15.1	Bridging security	120
15.1.1	Universal requirements for Bridging to another Ecosystem	120
15.1.2	Additional security requirements specific to bridged protocols	121
Annex A (informative)	Access control examples	123
A.1	Example OCF ACL Resource	123
Annex B (informative)	Execution environment security profiles	124
Annex C (normative)	Resource Type definitions	125
C.1	List of Resource Type definitions	125
C.2	Access Control List-2	125
C.2.1	Introduction	125
C.2.2	Well-known URI	125
C.2.3	Resource type	125
C.2.4	OpenAPI 2.0 definition	125
C.2.5	Property definition	133
C.2.6	CRUDN behaviour	133
C.3	Credential	134
C.3.1	Introduction	134
C.3.2	Well-known URI	134

C.3.3	Resource type	134
C.3.4	OpenAPI 2.0 definition	134
C.3.5	Property definition	143
C.3.6	CRUDN behaviour	143
C.4	Certificate Signing Request	143
C.4.1	Introduction	143
C.4.2	Well-known URI	143
C.4.3	Resource type	143
C.4.4	OpenAPI 2.0 definition	144
C.4.5	Property definition	145
C.4.6	CRUDN behaviour	145
C.5	Device Owner Transfer Method	146
C.5.1	Introduction	146
C.5.2	Well-known URI	146
C.5.3	Resource type	146
C.5.4	OpenAPI 2.0 definition	146
C.5.5	Property definition	149
C.5.6	CRUDN behaviour	150
C.6	Device provisioning status	151
C.6.1	Introduction	151
C.6.2	Well-known URI	151
C.6.3	Resource type	151
C.6.4	OpenAPI 2.0 definition	151
C.6.5	Property definition	154
C.6.6	CRUDN behaviour	158
C.7	Asserted roles	158
C.7.1	Introduction	158
C.7.2	Well-known URI	158
C.7.3	Resource type	158
C.7.4	OpenAPI 2.0 definition	158
C.7.5	Property definition	166
C.7.6	CRUDN behaviour	167
C.8	Security Profile	167
C.8.1	Introduction	167
C.8.2	Well-known URI	167
C.8.3	Resource type	167
C.8.4	OpenAPI 2.0 definition	167
C.8.5	Property definition	169
C.8.6	CRUDN behaviour	170
C.9	Auditable Event List	170
C.9.1	Introduction	170
C.9.2	Well-known URI	170
C.9.3	Resource type	170
C.9.4	OpenAPI 2.0 definition	170
C.9.5	Property definition	174
C.9.6	CRUDN behaviour	177
C.10	OCF Security Domain information	177
C.10.1	Introduction	177

C.10.2	Well-known URI.....	177
C.10.3	Resource type.....	177
C.10.4	OpenAPI 2.0 definition.....	177
C.10.5	Property definition.....	179
C.10.6	CRUDN behaviour.....	180
Annex D (informative) OID definitions		181
Annex E (informative) Security considerations specific to Bridged Protocols		183
E.1	Security considerations specific to the AllJoyn Protocol	183
E.2	Security considerations specific to the Bluetooth LE Protocol	183
E.3	Security considerations specific to the oneM2M Protocol	184
E.4	Security considerations specific to the U+ Protocol.....	184
E.5	Security considerations specific to the Z-Wave Protocol.....	184
E.6	Security considerations specific to the Zigbee Protocol.....	186
E.7	Security considerations specific to the the EnOcean Radio Protocol	186

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the Open Connectivity Foundation (OCF) (as OCF Security Specification, version 2.2.0) 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*.

This second edition cancels and replaces the first edition (ISO/IEC 30118-2:2018), which has been technically revised.

The main changes compared to the previous edition are as follows:

- movement of some text to onboarding tool specification;
- movement of some text to cloud security specification;
- addition of certificate profiles for identity and role X509 certificates;
- addition of text for: software update, end of life, end of service and auditable events;
- improvements to access control;
- addition of OCF cloud security sections;
- addition of clarifications throughout.

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

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 and www.iec.ch/national-committees.

Introduction

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

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

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

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

ISO/IEC 30118 consists of eighteen parts, under the general title Information technology — Open Connectivity Foundation (OCF) Specification. The parts fall into logical groupings as described herein:

- Core framework
 - Part 1: Core Specification
 - Part 2: Security Specification
 - Part 13: Onboarding Tool Specification
- Bridging framework and bridges
 - Part 3: Bridging Specification
 - Part 6: Resource to Alljoyn Interface Mapping Specification
 - Part 8: OCF Resource to oneM2M Resource Mapping Specification
 - Part 14: OCF Resource to BLE Mapping Specification
 - Part 15: OCF Resource to EnOcean Mapping Specification
 - Part 16: OCF Resource to UPlus Mapping Specification
 - Part 17: OCF Resource to Zigbee Cluster Mapping Specification
 - Part 18: OCF Resource to Z-Wave Mapping Specification
- Resource and Device models
 - Part 4: Resource Type Specification
 - Part 5: Device Specification

- Core framework extensions
 - Part 7: Wi-Fi Easy Setup Specification
 - Part 9: Core Optional Specification
- OCF Cloud
 - Part 10: Cloud API for Cloud Services Specification
 - Part 11: Device to Cloud Services Specification
 - Part 12: Cloud Security Specification

Information technology — Open Connectivity Foundation (OCF) Specification —

Part 2: Security specification

1 Scope

This document defines security objectives, philosophy, Resources and mechanism that impacts OCF base layers of ISO/IEC 30118-1. ISO/IEC 30118-1 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 documents.

2 Normative References

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

ISO/IEC 30118-1 Information technology -- Open Connectivity Foundation (OCF) Specification -- Part 1: Core specification
<https://www.iso.org/standard/53238.html>

ISO/IEC 30118-3 Information technology -- Open Connectivity Foundation (OCF) Specification -- Part 3: Bridging specification
<https://www.iso.org/standard/74240.html>

OCF Wi-Fi Easy Setup, Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification

OCF Cloud Specification, Information technology – Open Connectivity Foundation (OCF) Specification – Part 8: Cloud Specification

OCF Cloud Security Specification - Open Connectivity Foundation (OCF) Specification – Cloud Security Specification

OCF Onboarding Tool Specification - Open Connectivity Foundation (OCF) Specification – Onboarding Tool Specification

JSON SCHEMA, draft version 4, <http://json-schema.org/latest/json-schema-core.html>.

IETF RFC 2315, *PKCS #7: Cryptographic Message Syntax Version 1.5*, March 1998,
<https://tools.ietf.org/html/rfc2315>

IETF RFC 2898, *PKCS #5: Password-Based Cryptography Specification Version 2.0*, September 2000, <https://tools.ietf.org/html/rfc2898>

IETF RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*, November 2000,
<https://tools.ietf.org/html/rfc2986>

ISO/IEC 30118-2:2021(E)

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, July 2005,
<https://tools.ietf.org/html/rfc4122>

IETF RFC 4279, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, December 2005,
<https://tools.ietf.org/html/rfc4279>

IETF RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*,
May 2006, <https://tools.ietf.org/html/rfc4492>

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008,
<https://tools.ietf.org/html/rfc5246>

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008, <https://tools.ietf.org/html/rfc5280>

IETF RFC 5489, *ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)*, March 2009,
<https://tools.ietf.org/html/rfc5489>

IETF RFC 5545, *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*,
September 2009, <https://tools.ietf.org/html/rfc5545>

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization*, January 2010,
<https://tools.ietf.org/html/rfc5755>

IETF RFC 6347, *Datagram Transport Layer Security Version 1.2*, January 2012,
<https://tools.ietf.org/html/rfc6347>

IETF RFC 6655, *AES-CCM Cipher Suites for Transport Layer Security (TLS)*, July 2012,
<https://tools.ietf.org/html/rfc6655>

IETF RFC 6749, *The OAuth 2.0 Authorization Framework*, October 2012,
<https://tools.ietf.org/html/rfc6749>

IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*, October 2012,
<https://tools.ietf.org/html/rfc6750>

IETF RFC 7228, *Terminology for Constrained-Node Networks*, May 2014,
<https://tools.ietf.org/html/rfc7228>

IETF RFC 7250, *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, June 2014, <https://tools.ietf.org/html/rfc7250>

IETF RFC 7251, *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS*, June 2014,
<https://tools.ietf.org/html/rfc7251>

IETF RFC 7515, *JSON Web Signature (JWS)*, May 2015, <https://tools.ietf.org/html/rfc7515>

IETF RFC 7519, *JSON Web Token (JWT)*, May 2015, <https://tools.ietf.org/html/rfc7519>

IETF RFC 8323, *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets*,
February 2018, <https://tools.ietf.org/html/rfc8323>

IETF RFC 8392, *CBOR Web Token (CWT)*, May 2018, <https://tools.ietf.org/html/rfc8392>

IETF RFC 8520, *Manufacturer Usage Description Specification*, Mar 2019,
<https://tools.ietf.org/html/rfc8520>

oneM2M Release 3 Specifications, <http://www.onem2m.org/technical/published-drafts>

OpenAPI specification, aka *Swagger RESTful API Documentation Specification*, Version 2.0
<https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md>