INTERNATIONAL STANDARD

ISO/IEC 30118-12

First edition

Information technology — Open Connectivity Foundation (OCF) —

Part 12: Cloud security specification

PROOF/ÉPREUVE

Reference number
ISO/IEC 30118-12:2021(E)

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 v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms, definitions and abbreviated terms 2
3.1 Terms and definitions 2
3.2 Abbreviated terms 2
4 Document conventions and organization 3
4.1 Conventions 3
4.2 Notation 3
4.3 Data types 4
5 Security overview 4
5.1 Preamble 4
5.2 OCF Cloud architecture alignment with ISO IEC 17789 4
5.3 Device provisioning for OCF Cloud and Device registration overview 5
5.4 Credential overview 5
6 Device provisioning for OCF Cloud 5
6.1 OCF Cloud provisioning general 5
6.2 Device provisioning by Mediator 6
7 Device authentication with OCF Cloud 8
7.1 Device authentication with OCF Cloud general 8
7.2 Device connection with the OCF Cloud 8
7.3 Security considerations 9
8 Message integrity and confidentiality 10
8.1 OCF Cloud session semantics 10
8.2 Cipher suites for OCF Cloud Credentials 10
9 Security Resources 10
9.1 Account Resource 10
9.2 Account Session Resource 12
9.3 Account Token Refresh Resource 13
10 Security hardening guidelines 14
10.1 Security hardening guidelines general 14
Annex A (normative) Resource Type definitions 15
A.1 List of Resource Type definitions 15
A.2 Account Token 15
A.2.1 Introduction 15
A.2.2 Well-known URI 15
A.2.3 Resource type 15
A.2.4 OpenAPI 2.0 definition 15
A.2.5 Property definition 18
A.2.6 CRUDN behaviour 19
A.3 Session 20
A.3.1 Introduction 20
A.3.2 Well-known URI 20

A.3.3 Resource type 20
A.3.4 OpenAPI 2.0 definition 20
A.3.5 Property definition 22
A.3.6 CRUDN behaviour 23
A.4 Token Refresh 23
A.4.1 Introduction 23
A.4.2 Well-known URI 23
A.4.3 Resource type 23
A.4.4 OpenAPI 2.0 definition 24
A.4.5 Property definition 26
A.4.6 CRUDN behaviour 27

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 Cloud 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*.

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 Specifiction
- 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) —

Part 12:
Cloud security specification

1 Scope

The OCF Cloud specifications are divided into a series of documents:

– OCF Cloud security specification (this document): The cloud security specification document specifies the security recuirements and definitions for OCF devices and OCF clouds implementations.

– OCF Device to Cloud Specification: The OCF Device to Cloud Specification document defines functional extensions and capabilities to meet the requirements of the OCF Cloud. This document specifies new Resource Types to enable the functionality and any extensions required to connect an OCF device to an OCF cloud.

– OCF Cloud API for cloud services specification: The Cloud API for cloud services specification defines the OCF cloud API.

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.

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

ISO/IEC 30118-2, Information technology – Open Connectivity Foundation (OCF) Document – *Part 2: Security specification*
https://www.iso.org/standard/74239.html

ISO/IEC 30118-8, *Information technology – Open Connectivity Foundation (OCF) Document – Part 8: Device to Cloud Services*,
https://www.iso.org/standard/79360.html

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

oneM2M Release 3 Documents, http://www.onem2m.org/technical/published-drafts

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1, ISO/IEC 30118-2, ISO/IEC 30118-8 and the following apply.

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

– ISO Online browsing platform: available at https://www.iso.org/obp

– IEC Electropedia: available at http://www.electropedia.org/

3.1.1
Access Token
credential used to authorize the connection with the OCF Cloud and access protected Resources

Note 1 to entry: An Access Token is a string while the OCF Device has no internal logic based on its contents and only forwards the token as-is

3.1.2
Authorization Provider
server issuing Access Tokens (3.1.1) via a Mediator to the Client after successfully authenticating the *OCF Cloud User* (3.1.4) and obtaining authorization

Note 1 to entry: Also known as authorization server in IETF RFC 6749.

3.1.3
Device Registration
process by which Device is enrolled/registered to the OCF Cloud infrastructure (using Device certificate and unique credential) and becomes ready for further remote operation through the cloud interface (e.g. connection to remote Resources or publishing of its own Resources for access)

3.1.4
OCF Cloud User
person or organization authorizing a set of Devices to interact with each other via an OCF Cloud

Note 1 to entry: For each of the Devices, the OCF Cloud User is either the same as, or a delegate of, the person or organization that onboarded that Device. The OCF Cloud User delegates, to the OCF Cloud authority, authority to route between Devices registered by the OCF Cloud User. The OCF Cloud delegates, to the OCF Cloud User, authority to select the set of Devices which can register and use the services of the OCF Cloud.

3.2 Abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 30118-1, ISO/IEC 30118-2 and ISO/IEC 30118-8 apply.

4 Document conventions and organization

4.1 Conventions

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

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

4.2 Notation

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

Required (or shall or mandatory)(M).

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

Recommended (or should)(S).

– These features add functionality supported by Core Architecture and should be implemented. Recommended features take advantage of the capabilities 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 behaviour that is permitted but not recommended.

Allowed (may or allowed)(O).

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

DEPRECATED.

– Although these features are still described in this document, they should not be implemented except for backward compatibility. The occurrence of a deprecated feature during operation of an implementation compliant with the current document 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 document.

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.

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

Words that are emphasized are printed in italic.

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

4.3 Data types

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

5 Security overview

5.1 Preamble

A Device is authorized to communicate with an OCF Cloud if a trusted Mediator has provisioned the Device.

– Device and Mediator connect over DTLS using "/oic/sec/cred"

– Device is provisioned by Mediator with following information:

  – the URL of OCF Cloud

  – Authorization Provider Name to identify the origin of the Access Token

  – Access Token / Authorization Code that is validated / exchanged by the OCF Cloud

  – UUID of the OCF Cloud

The OpenAPI 2.0 definitions (Annex A) used in this document are normative. This includes that all defined payloads shall comply with the indicated OpenAPI 2.0 definitions. Annex A contains all of the OpenAPI 2.0 definitions for Resource Types defined in this document.

5.2 OCF Cloud architecture alignment with ISO IEC 17789

Reference ISO/IEC 17789 defines a cloud computing reference architecture (CCRA) which can be described in terms of one of four architectural viewpoints; user, functional, implementation, and deployment. Of the four viewpoints, implementation and deployment are explicitly out of scope of ISO/IEC 17789.

OCF defines an application capabilities type cloud service, providing Communication as a Service (CaaS) (reference ISO/IEC 17788). This cloud service is provided by a cloud service provider, the mechanisms used by the cloud service provider in managing their overall cloud infrastructure are outside the scope of the OCF defined cloud service. The OCF definition is specific to the interface offered by the cloud service to the cloud service customer, specifically the cloud service user.

There are three different user views defined. In the case where the cloud service customer is an OCF Device as specified in OCF Device to Cloud Services then the views provided are:

- Interface for the OCF Device to provide information to the cloud service

- Interface for the OCF Device to retrieve information that has been provided to the cloud service