INTERNATIONAL STANDARD

ISO/IEC 30118-10

First edition

Information technology — Open Connectivity Foundation (OCF) —

Part 10: Cloud API for cloud services specification

PROOF/ÉPREUVE

Reference number
ISO/IEC 30118-10:2021(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

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 API for Cloud Services, 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 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) —

Part 10:
Cloud API for cloud services specification

1 Scope

This document defines functional requirements for the OCF Cloud to Cloud Application Programming Interface (API).

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.

IETF RFC 2818, *HTTP over TLS,* May 2000
https://tools.ietf.org/html/rfc2818

IETF RFC 5646, *Tags for Identifying Languages*, September 2009
https://www.rfc-editor.org/info/rfc5646

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://www.rfc-editor.org/info/rfc6750

IETF RFC 7628, *A Set of Simple Authentication and Security Layer (SASL) Mechanisms for OAuth,* August 2015
https://www.rfc-editor.org/info/rfc7628

ISO/IEC 17788 *Information technology – Cloud computing – Overview and vocabulary*
https://www.iso.org/standard/60544.html

ISO/IEC 17789 *Information technology – Cloud computing – Reference architecture*
https://www.iso.org/standard/60545.html

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

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

OCF Cloud Security, *Open Connectivity Foundation Cloud Security, Version 2.2.0*
Available at: https://openconnectivity.org/specs/OCF_Cloud_Security_Specification_v2.2.0.pdf

OCF Device to Cloud Services, *Open Connectivity Foundation Device to Cloud Services Specification, Version 2.2.0*
Available at:
https://openconnectivity.org/specs/OCF_Device_To_Cloud_Services_Specification_v2.2.0.pdf

OCF Cloud API for Cloud Services

https://github.com/openconnectivityfoundation/core-extensions/blob/ocfcloud-openapi/swagger2.0/oic.r.cloudopenapi.swagger.json

OpenAPI 2.0, *fka 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, OCF Device to Cloud Services 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
API Endpoint
defined URL to which requests defined in this document are sent

3.1.2
Bearer Token
OAuth2.0 access token as defined within IETF RFC 6750

3.1.3
Origin Cloud
OCF Cloud through which the user works with his OCF Devices

3.1.4
Subscription ID
unique identity that is associated with an instance of a subscription to an event (or events)

3.1.5
Target Cloud
OCF Cloud to which OCF Servers (OCF Devices) are connected which the user wants to control via the *Origin Cloud* (3.1.2)

3.2 Symbols and abbreviated terms

API	Application Programming Interface
HMAC	Hash-based Message Authentication Code

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.

5 Overview

5.1 Introduction

This document defines the OCF Cloud API for Cloud Services. In this document Origin Cloud refers to the OCF Cloud through which the user works with his OCF Devices, Target Cloud refers to the OCF Cloud to which OCF Servers (OCF Devices) are connected which the user wants to control via the Origin Cloud.

An OCF Device is a collection of Resources, each Resource being an OpenAPI 2.0 defined object that represents a physical property or characteristic of the Device (e.g. temperature sensed, light colour, power on switch). The Device itself has an associated Device Type that provides an indication of what the Device is, for example a Light is represented as a Device Type of "oic.d.light".

Please see Figure 1 for a representation of the target architecture.

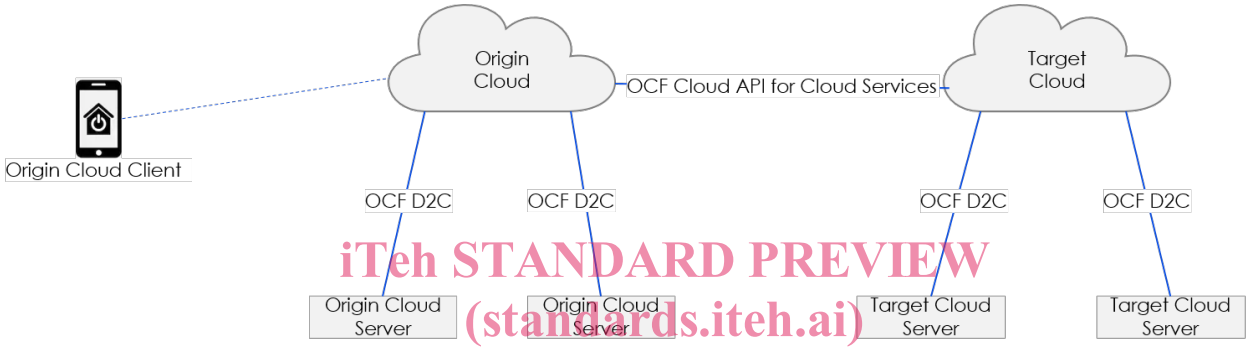

Figure 1 – OCF Cloud overview

The OCF Cloud API for Cloud Services supports the following cases:

- Account Linking API (clause 7)
  - Initial Account Linking
  - Removal of linked account
- Devices API (clause 8)
  - Retrieval of all Devices associated with a User (clause 8.3)
  - Retrieval of a single Device associated with a User (clause 8.4)
  - Retrieval of a single Resource (clause 8.5)
  - Update of a single Resource (clause 8.6)
- Events API (clause 9)
  - Subscription to an event: establishment of a subscription (clause 9.4.1)
  - Notification: event generated on an established subscription (clause 9.4.3)

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

In the case where the cloud service customer is another instance of a cloud service as specified in this document then the view provided is:

- Interface for the other cloud service instance to retrieve and update the information that is provided via the cloud service

The OCF Cloud service pertains specifically to a cloud service user, there is a single applicable cloud service activity, that of "Use cloud service" defined in clause 8.2.21 of ISO/IEC 17789.

Credentials for the user of the cloud service are provided using OAUTH2.0 as defined by RFC 6749. The cloud service, either itself, or leveraging an external authorization server, provides a bearer token that is required in all requests from all cloud users. Please see clause 7 and OCF Cloud Security.

All connectivity between a cloud user and the OCFCloud service is via mutually authenticated TLS; see clause 7.1 of OCF Cloud Security.

5.3 General OCF Cloud API for Cloud Services elements

The OCF Cloud API for Cloud Services is a RESTful API over HTTPS (IETF RFC 2818). The API is defined using OpenAPI 2.0.

The Origin Cloud communicates with the Target Cloud using the domain name or URI it has obtained from the initial OAuth 2.0 (IETF RFC 6749) Client Setup, covered in clause 7. Communication between OCF Devices and OCF Clouds is defined in OCF Device to Cloud Services.

All URIs presented within a "href" Link Parameter present in any payload shall be in the form "/<deviceId>/<resourcehref>"; where <deviceId> is the identity of the Device as provided in the "di" Property of "/oic/d" and "resourcehref" is the "href" of the Resource as provided by the Target Cloud.

An Origin Cloud shall obtain a Bearer Token from the Target Cloud using standard OAuth2.0 (IETF RFC 6749) mechanisms. All subsequent requests from an Origin Cloud to the Target Cloud shall include this Bearer Token for the user in question.

Any query parameters received by an Origin Cloud in a request from an OCF Client shall be passed through clean (i.e. are part of the URI) in any request that is sent to a Target Cloud.

Each request may contain an optional HTTP Correlation-ID header, which carries a unique identifier value that provides a reference to a particular transaction or event chain in the Target Cloud. If the request does contain a Correlation-ID header, a Correlation-ID populated with the same value shall be present in any response to that request. If the request does not contain a Correlation-ID header, one should be present in the response.

All requests shall include an HTTP Accept header with the exception of a DELETE (as there is no payload expected in the response). All requests or responses that carry content shall include an HTTP Content-Type header. At a minimum media-types "application/json" and "application/vnd.ocf+cbor" shall be supported. If the recipient of a request cannot provide a response that is encoded according to the content of the Accept header, then a HTTP 406 (not acceptable) response should be sent in accordance with IETF RFC 2818. On reception of a 406 response the originator of the request may re-attempt the request using an alternative Content-Type if supported.

5.4 Cloud to Cloud operational overview

5.4.1 Introduction

This clause provides an informative overview of the flows that are enabled by the detailed API defined in clauses 6, 7, 8, and 9. Clause 5.4 provides references to the applicable clauses within this document that define the API specifics.

5.4.2 Conceptual architecture

Figure 2 describes the overall conceptual architecture.

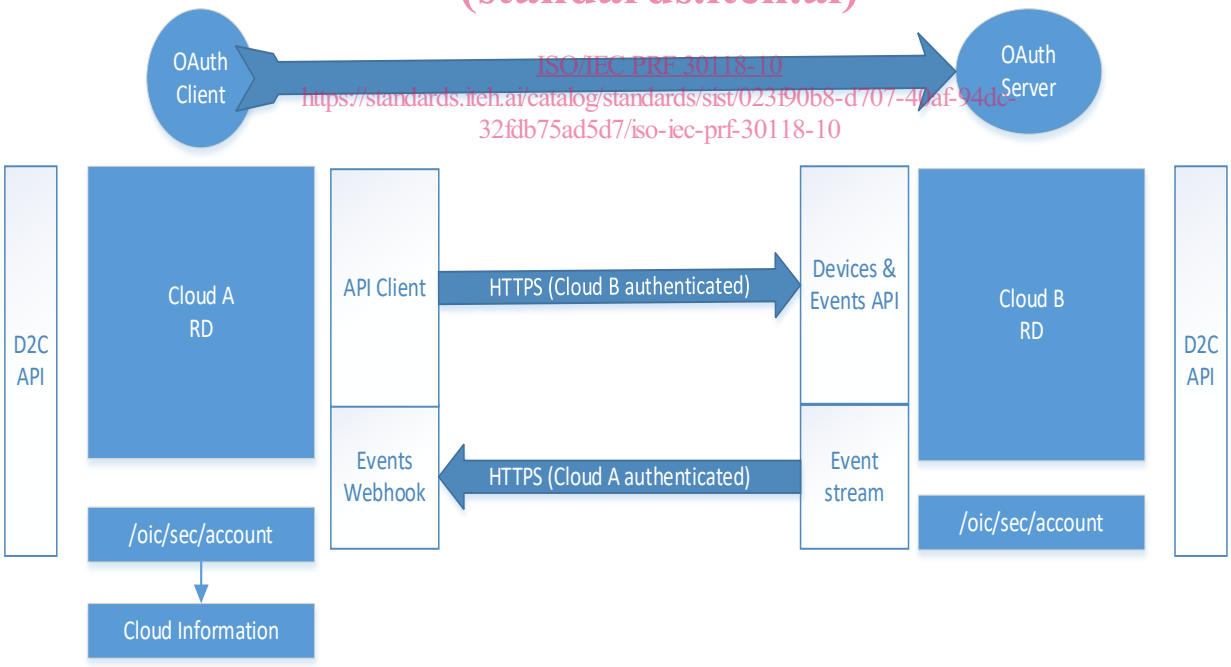

Figure 2 – Conceptual architecture

5.4.3 Authorizing OCF Cloud connectivity

Consider a user who has accounts on two distinct, separately owned OCF Clouds, and devices associated with each of those accounts on those OCF Clouds. The user wants to have a unified view of all of their devices from a single client rather than having a client per cloud. The user via the client they want to use for all devices indicates to the directly connected OCF Cloud (Origin Cloud) that they want to link this account with an account on the other OCF Cloud (Target Cloud). This initiates a

standard OAuth2.0 authorization code grant type flow, see IETF RFC 6749, clause 1.3.1. Application of this flow is described in clause 7.

5.4.4 Synchronization of user's set of Devices

After completion of the authorization code grant type flow from clause 5.4.3 the Origin Cloud (that is the OCF Cloud to which the user is connected) is authorized to use the Device API to obtain on behalf of the user the complete list of devices hosted on the Target Cloud for which the user has access. The API is described in clause 8, and the flow is further illustrated in clause A.4.

The result of the invocation of the Device API is a complete set of device information that may then be provided in a response to a RETRIEVE on "/oic/res" from the Origin Cloud.

5.4.5 Keeping up-to-date: Notifications of changes on other OCF Clouds

Once the set of devices has been obtained, the Origin Cloud can subscribe to the events to which it is interested across the user's complete device set ("/devices"), or per device in that set ("/devices/{deviceid}"). See clause 9 for details of the API itself.

The subscription to "/devices" enables the Origin Cloud to be notified whenever a new device is added or an existing device removed from the Target Cloud.

The subscription to "/devices/{deviceid}" enables the Origin Cloud to be notified whenever there is a change in the state of a device (e.g. it has de-registered).

When a new Device registers on the Target Cloud, and a subscription exists for that event, then a notification is sent to the Origin Cloud with an event type of "devices_registered" and a payload which contains the "di" of the newly registered device. The Origin Cloud may then RETRIEVE the Links exposed by the newly added device using "/devices/{deviceid}" where "deviceid" was provided in the payload of the notification. See clause A.10 for a flow illustrating this interaction.

5.4.6 Handling of requests and responses for connected Devices

From the perspective of the client connected to the Origin Cloud there is no distinction between devices and their Resources hosted by the Origin Cloud itself and devices and their resources that are hosted by a Target Cloud reached via this API.

Thus all requests for a target resource are formed using the mechanisms described in OCF Device to Cloud Services.

The Origin Cloud identifies the Target Cloud for the requested Resource via the "deviceid" that is in the request URI which is matched to the "di" Property in "/oic/sec/account". The request is then effectively proxied to the Target Cloud via the "/devices/{deviceid}/{resourcehref}" API exposed by the Target Cloud (see clause 8.5 and 8.6). Any query parameters received over the Device to OCF Cloud connection are included in the URI unaltered. The content-type of the payload in the request or response is honoured. See clauses A.6 and A.7 for illustrative flows of this mechanism for both RETRIEVE and UPDATE cases.

6 Authentication and authorization

A Target Cloud shall only expose secure endpoints; any requests received over an unsecured connection (i.e. HTTP) shall be redirected to the secure equivalent of that endpoint. The Origin Cloud shall use the "Bearer" authentication scheme inside the "Authorization" request header field to transmit the access token, as per IETF RFC 6750 clause 2.1. For definition of the "Authorization" request header field, see IETF RFC 2818.

Bearer Tokens issued by the Target Cloud shall identify the user as well as the client that is sending requests on behalf of the user to the Target Cloud.