INTERNATIONAL STANDARD

ISO/IEC 30118-13

First edition

Information technology — Open Connectivity Foundation (OCF) —

Part 13: Onboarding tool specification

PROOF/ÉPREUVE

Reference number
ISO/IEC 30118-13:2021(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 Onboarding Tool 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 13: Onboarding tool specification

1 Scope

This document defines mechanisms supported by an OCF Onboarding Tool (OBT). This document contains security normative content for the OBT and may contain informative content related to the OCF base or OCF Security Specification 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. 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 30118-2, *Information technology – Open Connectivity Foundation (OCF) Specification – Part 2: Security specification*
https://www.iso.org/standard/74239.html

NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

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 and [1] 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/

3.2 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 30118-1, ISO/IEC 30118-2 and [1] 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 Services and availability in the OBT

5.1 Purpose of the OBT

The purpose of an OBT is to provide the foundation of trust for an OCF Security Domain. An OBT is an OCF Device which can provide a variety of functions. The OBT functions fall into two main categories: establishing ownership of Devices being added to the OCF Security Domain; and provisioning of Devices in the OCF Security Domain. The intent is that a single OBT can provide all these functions, but there is no prohibition against these functions being distributed across multiple OBTs.

OCF Security Domain is associated with its UUID, determined by an OBT. The OBT is responsible for maintaining the OCF Security Domain UUID, and provisions the same value to each Device that is part of the same OCF Security Domain.

The term (OCF) Onboarding refers to the initial establishment of ownership over a Device, and initial provisioning of the Device for normal operation (see clause 5.3 of ISO/IEC 30118-2). A Device can be reset to enable subsequent Onboarding of the Device, for example following a subsequent sale to another person. A Device can also be further provisioned without repeating the entire Onboarding process.

The following OBT functions are specified:

- A Device Ownership Transfer Service (DOTS) establishes ownership of Devices being added to the OCF Security Domain. This function is described in clause 5.3.

- A Credential Management Service (CMS) manages the credentials and Roles of Devices in the OCF Security Domain. This function is described in clause 5.4.

- An Access Management Service (AMS) manages the access of Devices in the OCF Security Domain. This function is described in clause 5.5.

- Optional: A Mediator facilitates further configuration of Devices in the OCF Security Domain for various purposes including Wi-Fi configuration (see [2]) and OCF Cloud access (see [3]).

The OBT demands a higher level of security hardening than regular OCF Devices in order to preserve integrity and confidentiality of sensitive credentials being stored.

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

The Device Onboarding States are defined in clause 8 of ISO/IEC 30118-2. Table 1 provides an overview of the access granted to the OBT components according to the Device Onboarding States.

Table 1 – Overview of OBT access in Device Onboarding States

Device Onboarding State	Description		Applicable Resources & Access	Entity Authorized to READ/WRITE	Purpose	"/oic/sec/doxm:owned"
RESET	Full reset of OCF Device to manufacturer default.		No Access	No Access	Remove info in SVRs.	FALSE
RFOTM	Ready for Ownership Transfer Mechanism.	Prior to successful OTM	"/oic/sec/doxm" (R: all, W: oxmsel)	Any	R: Determine supported OTMs W: Select an OTM	FALSE
		After successful OTM	"/oic/sec/doxm" (RW) "/oic/sec/cred"(RW)	DOTS	Claim ownership. Establish credentials for authenticating DOTS, AMS, CMS & optionally other Devices	
			(At discretion of End User of DOTS) "/oic/sec/sp" (RW)	DOTS	R: Determine supported Security Profiles. W: Set current security profile.	
			(At discretion of End User of DOTS) "/oic/sec/acl2" (RW)	DOTS	Configure further ACEs	
			"/oic/sec/pstat" (RW)	DOTS	Transition to RFPRO or RESET	
RFPRO	Ready for Provisioning.		"/oic/sec/cred" (RW)	CMS or matching ACE	Establish credentials for authenticating Devices in normal operation, including Roles	TRUE
			"/oic/sec/acl2" (RW)	AMS or matching ACE	Establish ACEs for normal operation	
			"/oic/sec/sp" (RW)	DOTS or matching ACE	R: Determine supported Security Profiles. W: Set current security profile	
			"/oic/sec/pstat" (RW)	DOTS, CMS, AMS or matching ACE	Transition to RFNOP	
RFNOP	Ready for Normal Operation.		"/oic/sec/pstat"	DOTS, CMS, AMS or matching ACE	Transition to RFPRO, SRESET or RESET	TRUE
			Vertical Resources	Matching ACE	Normal Operation	
SRESET	Soft RESET.		"/oic/sec/cred" (RW)	CMS	Corrections as needed	TRUE
			"/oic/sec/acl2" (RW)	AMS	Corrections as needed	
			"/oic/sec/doxm" (RW)	DOTS	Corrections as needed	
			"/oic/sec/pstat" (RW)	DOTS, CMS or AMS	Transition to RFPRO or RESET	