OCF Onboarding Tool Specification

VERSION 2.2.1 | December 2020

CONTACT admin@openconnectivityfoundation.org

LEGAL DISCLAIMER

NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY ANY OF THE AUTHORS OR DEVELOPERS OF THIS DOCUMENT. THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AUTHORS AND DEVELOPERS OF THIS SPECIFICATION HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OPEN INTERCONNECT CONSORTIUM, INC. FURTHER DISCLAIMS ANY AND ALL WARRANTIES OF NON-INFRINGEMENT, ACCURACY OR LACK OF VIRUSES.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

CONTENTS

Tables

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.

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.

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
Latest version available at:
https://openconnectivity.org/specs/OCF_Core_Specification.pdf

ISO/IEC 30118-2, *Information technology – Open Connectivity Foundation (OCF) Specification – Part 2: Security specification*
https://www.iso.org/standard/74239.html
Latest version available at: https://openconnectivity.org/specs/OCF_Security_Specification.pdf

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

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.

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

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.

193 **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	

194

195 ## 5.2 General OBT requirements

196 An OBT shall be hosted on an OCF Device.

197 An OBT shall host at least one of a DOTS, AMS and CMS.

198 All DOTS, AMS and CMS shall be hosted on an OBT.

An OBT may change the Device state of a Device by updating "s" field in the "dos" Property object of the "/oic/sec/pstat" Resource to the desired value. The allowed Device state transitions are defined in 13.8 of ISO/IEC 30118-2.

After successful OTM, but before placing the newly-onboarded Device in RFNOP, the OBT shall remove all SVR entries in the "resources" array for ACEs where the Subject is "anon-clear" or "auth-crypt".

The OBT should support all mandatory and optional cipher suites in clauses 11.3.3 and 11.3.4 of ISO/IEC 30118-2.

5.3 DOTS

5.3.1 Assuming ownership of a Device

The DOTS shall support all OTMs in clause 7.

An overview is provided in clauses 5.3.3 and 7.2 of ISO/IEC 30118-2.

The following steps shall be performed to take ownership of a Device. The Device is presumed to be in RFOTM.

1) The DOTS performs a multicast RETRIEVE on the "/oic/sec/doxm" Resource using "owned=false" query parameter as described in ISO/IEC 30118-2.
2) Before proceeding, the DOTS shall obtain acknowledgement from the OBT End User that the OBT End User approves the DOTS assuming ownership of the discovered Device(s). See security considerations in clause 5.3.3.
3) The DOTS selects a mutually supported OTM from the "oxms" Property of the "/oic/sec/doxm" Resource. See security considerations in clause 5.3.3.
4) The DOTS shall UPDATE the "oxmsel" Property of "/oic/sec/doxm" the value corresponding to the OTM being used, before performing other OTM steps.
5) The DOTS shall initiate a DTLS Session as specified for the OTM configured to the oxmsel Property of the "/oic/sec/doxm" Resource. Details are provided in clause 7.
6) The DOTS shall send an UPDATE request message to "/oic/sec/pstat" to set the value of "om" to 0b 0000 0100 to select Client-directed provisioning.
7) The DOTS shall UPDATE the "devowneruuid" Property of the "/oic/sec/doxm" Resource with the UUID of the DOTS.
8) The DOTS may RETRIEVE the updated "deviceuuid" Property of the "/oic/sec/doxm" Resource after the DOTS has updated the "devowneruuid" Property value of the "/oic/sec/doxm" Resource to a non-nil-UUID value.
9) The DOTS shall UPDATE the "deviceuuid" of the "/oic/sec/doxm" Resource. The updated value shall be a value that the DOTS has generated. The DOTS should use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient entropy.
10) The DOTS shall provision the ownership credential as follows:
    a) The DOTS shall generate a Shared Key using the SharedKey Credential Calculation method described in clause 7.3.2 of ISO/IEC 30118-2.
    b) The DOTS shall add an entry to the "creds" array to the new Device's "/oic/sec/cred" Resource, identified as a symmetric pair-wise key, with an empty "privatedata" Properties, and with the value of the "subjectuuid" Property set to the value of "devowneruuid" Property of the "/oic/sec/doxm" Resource. See clause 13.3.1 of ISO/IEC 30118-2 for details of such a request.
    c) Upon receipt of the DOTS's symmetric Owner Credential, the new Device independently generates the Shared Key using the SharedKey Credential Calculation method described in clause 7.3.2 of ISO/IEC 30118-2 and stores it with the Owner Credential.

11) The following steps are applied subsequent to successful establishment of Owner Credential, and prior to transitioning to RFPRO. These steps may occur in any order.

- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/doxm" Resource with the UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has "oic.d.dots" value in "rt" Property of its "/oic/d" Resource. The DOTS shall expose "oic.d.dots" value in “rt" Property of its "/oic/d" Resource.
- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/pstat" Resource with the UUID of the DOTS. The DOTS shall only do so, if the OCF Device, which hosts DOTS has "oic.d.dots" value in "rt" Property of its "/oic/d" Resource. The DOTS shall expose "oic.d.dots" value in “rt" Property of its "/oic/d" Resource.
- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the UUID of the CMS. The DOTS shall only do so, if the OCF Device, which hosts CMS has "oic.d.cms" value in "rt" Property of its "/oic/d" Resource. The CMS shall expose "oic.d.cms" value in “rt" Property of its "/oic/d" Resource.
- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/acl2" Resource with the UUID of the AMS. The DOTS shall only do so, if the OCF Device, which hosts AMS has "oic.d.ams" value in "rt" Property of its "/oic/d" Resource. The AMS shall expose "oic.d.ams" value in "rt" Property of its "/oic/d/" Resource.
- The DOTS shall update the "owned" Property of the "/oic/sec/doxm" Resource with value "true".
- The DOTS shall provision the "/oic/sec/cred" Resource with credentials that enable secure connections between OCF Services (e.g. DOTS, CMS, AMS, Mediator) and the new Device. The DOTS shall provision credentials according to the supported credential types shown in the "sct" Property of the "/oic/sec/doxm" Resource.
- The DOTS may UPDATE the "/oic/sec/acl2" Resource with ACEs and may UPDATE the "/oic/sec/cred" Resource with further credentials.
- If the provisioned Device exposes ''/oic/sec/sdi" Resource, then an OBT hosting DOTS shall:
  - Provision "uuid" Property of "/oic/sec/sdi" Resource with OCF Security Domain UUID. If the OCF Security Domain UUID has not been derived yet, the DOTS shall generate the UUID value randomly. DOTS shall use the same UUID value when Onboarding a Device into the same OCF Security Domain.
  - Provision "name" Property of "/oic/sec/sdi" Resource with a human readable name, received from an OCF Security Domain Owner. The DOTS should implement a user interface to receive this information, when a new OCF Security Domain is being created. If no user interface is implemented the DOTS should provision a copy of the "/oic/d:n" of the DOTS.
  - Provision "priv" Property of "/oic/sec/sdi" Resource with the value selected by the OCF Security Domain Owner or preconfigured by the manufacturer. The DOTS should implement a user interface to receive this information.

NOTE: When the Device is an OCF v1.3 Device, the DOTS is expected to send an UPDATE request to /oic/sec/doxm to change the value of "owned" to true.

12) To transition the Device to RFPRO, the DOTS sends an UPDATE request changing the "dos.s" Property of the "oic/sec/pstat" Resource to RFPRO.

5.3.2 DOTS and Bridging

Bridge Platforms, their Bridge and VOD components are specified in [1]. Bridges and VODs are individually onboarded to an OCF Security Domain. Unowned VODs on a Bridge Platform are not discoverable while the Bridge on that Bridge Platform is Unowned. In other words, the VODs can only be onboarded while the Bridge is Owned. The implication is that the DOTS onboards the Bridge first, and then onboard the VODs. For details, see [1].

5.3.3 Security considerations regarding selecting an Ownership Transfer Method

A DOTS and/or DOTS operator might have strict requirements for the list of OTMs that are acceptable when transferring ownership of a new Device. Some of the factors to be considered when determining those requirements are:

- The security considerations described for each of the OTMs.
- The probability that a man-in-the-middle attacker might be present in the environment used to perform the ownership transfer.

For example, the operator of a DOTS might require that all of the Devices being onboarded support either the Random PIN based OTM or the Manufacturer Certificate based OTM.

5.4 CMS

An introduction to the credential management is provided in clause 5.4.3 of ISO/IEC 30118-2.

The credential types are specified in clause 9.3 of ISO/IEC 30118-2.

The supported credential types with which the Device can be provisioned are provided in the "sct" Property of the "/oic/sec/doxm" Resource. The CMS shall provision credentials according to the credential types supported.

NOTE: The value of "sct" has no correlation to supported OTMs.

The CMS shall support adding certificate entries ("credtype" value of "8") to the "creds" Property to the "/oic/sec/cred" Resource as defined in clause 13.3 of ISO/IEC 30118-2. The CMS shall support removing entries from the "creds" Property to the "/oic/sec/cred" Resource as defined in clause 13.3 of ISO/IEC 30118-2. The CMS may support changing existing entries in the "creds" Property to the "/oic/sec/cred" Resource as defined in 13.3 of ISO/IEC 30118-2.

Certificate provisioning of local Credentials is described in clause 9.4.5 of ISO/IEC 30118-2. The following points are pertinent to the CMS

- The CMS has its own CA certificate and key pair. The certificate is either a) self-signed if it acts as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either case, the certificate has the format described in clause 9.4.2 of ISO/IEC 30118-2.
- The CMS shall support issuing an identity certificate for the Device as described in clause 6.1.
- The CMS shall support issuing role certificates as described in clause 6.1.
- When issuing a role certificate or an identity certificate, the CMS shall include a string of format "uuid:X" in the Common Name component of the Subject Name of the issued certificate, where X is provisioned to match the "deviceuuid" Property of the "/oic/sec/doxm" Resource.
- The CMS shall support provisioning a Trust Anchor as described in clause 6.2.

CRL provisioning is specified in clause 9.4.6 of ISO/IEC 30118-2, using the "/oic/sec/crl" Resource specified in clause 13.4 of ISO/IEC 30118-2. The issuing CMS issues the certificate revocation lists for certificates it issues. If a certificate private key is compromised, the CMS revokes the certificate. If CRLs are used by a Device, the CMS is expected to regularly (for example; every 3 months) update the "/oic/sec/crl" Resource for the Devices it manages.

An introduction to Role Management is provided in clause 5.4.3 of ISO/IEC 30118-2.

5.5 AMS

The AMS shall support adding entries to the "aclist2" Property of the "/oic/sec/acl2" Resource as defined in clause 13.5 of ISO/IEC 30118-2.

The AMS shall support removing existing entries in the "aclist2" Property of the "/oic/sec/acl2" Resource as defined in clause 13.5 of ISO/IEC 30118-2.

The AMS may support changing existing entries in the "aclist2" Property of the "/oic/sec/acl2" Resource as defined in 13.5 of ISO/IEC 30118-2.

The AMS should support other operations as defined in clause 13.5 of ISO/IEC 30118-2.

Clause 6.2 of [3] provides normative requirements on the AMS when configuring ACE entries of a Device which supports OCF Cloud.

The AMS determines an appropriate ACL configuration for each Server based on the rules for ACL evaluation and enforcement at Servers specified in clause 12 of ISO/IEC 30118-2. The formatting of the ACL Resource specified in clause 13.5 of ISO/IEC 30118-2.

To support homogenous behaviour across OCF ecosystem, AMS can provision explicit ACL entries to legacy Devices based on the value of "icv" Property of "/oic/d" Resource, so that they recognize default "oic.role.*" Roles added in later releases. Table 2 enumerates the list of Roles and their access policies to provision per each version.

Table 2 – ACL entries to provision for role usage uniformity

Version	Role	Access Policy: Permission	Access Policy: Resource	Description
"2.4.0" and prior	"oic.role.owner"	-RU--	All SVRs	Grant right to perform all supported operations on all supported SVRs

Certificate management requirements

6.1 Issuing identity certificates and role certificates

A CMS shall perform the following steps to issue an identity certificate or role certificate to a Device.

1) If the Device has the "/oic/sec/csr" Resource, then
   a) The CMS shall send a RETRIEVE request to the "/oic/sec/csr" Resource on the Device, to obtain a certificate signing request for which the CMS will create a certificate.
   b) The CMS shall issue (or otherwise obtain) a certificate chain using the certificate signing request returned by the new Device and complying with clause 9.4.2 of ISO/IEC 30118-2.
2) If the Device does not have the "/oic/sec/csr" Resource, then the CMS shall issue (or otherwise obtain) a certificate chain using the using a public key pair generated by the CMS, and complying with clause 9.4.2 of ISO/IEC 30118-2.
3) The CMS shall send a request to the Device to add an entry to the "creds" Property of the "/oic/sec/cred" Resource of the Device meeting the following criteria:
   – The "subjectuuid" Property shall have the value of "deviceuuid" Property of the "/oic/sec/doxm" Resource.
   – The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with Certificate.
   – The "credusage" Property shall have the value of "oic.sec.cred.cert" or "oic.sec.cred.rolecert" corresponding to an identity certificate or role certificate as respectively.
   – The "publicdata" Property shall contain the newly-created certificate chain.

See clause 13.3.1 of ISO/IEC 30118-2 for details of a request adding an entry to the "creds" Property of the "/oic/sec/cred" Resource.

6.2 Provisioning Trust Anchor certificates

To provision a Trust Anchor certificate to a Device, a CMS shall send a request to the Device to add an entry to the "creds" Property of the "/oic/sec/cred" Resource of the Device meeting the following criteria:

- The "subjectuuid" Property shall have the value of "*" (matching all identities) or a specific UUID (matching a single identity).
- The "credtype" Property shall have the value "8" corresponding to Asymmetric Signing Key with Certificate
- The "credusage" Property shall have the value of "oic.sec.cred.trustca" corresponding to a certificate Trust Anchor
- The "publicdata" Property shall contain the Trust Anchor certificate.

See clause 13.3.1 of ISO/IEC 30118-2 for details of a request adding an entry to the "creds" Property of the "/oic/sec/cred" Resource.

6.3 Provisioning an OSCORE Security Context for End-to-End Security of Unicast Messages

ISO/IEC 30118-2 describes how Object Security for Constrained RESTful Environments (OSCORE) protocol [4] is used for End-to-End Security of Unicast Messages.

OSCORE communication between two Devices is enabled by provisioning an OSCORE Security Context in a credential entry of the "/oic/sec/cred" Resource in each of the two Devices. The present clause provides the requirements on the CMS for this provisioning. For the purposes of this description, let Device A and Device B denote the two Devices.

Prior to provisioning, the CMS generates three values: idA; idB; and an OSCORE Master Secret.

- The CMS selects a value for idA (identifying the OSCORE Security Context for messages sent from Device A to Device B) conforming to the following criteria:
  - The total length of idA in bits shall be a multiple of 8 between 16 and 56 inclusive, which corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14 characters inclusive.
  - The first byte of idA shall be 0x01.

NOTE 1: The value 0x01 is the OSCORE Identifier Namespace Prefix value assigned for "Directly Provisioned OSCORE Security Context" in ISO/IEC 30118-2.

  - The value of idA should be distinct from all values of "recipientid" in credential entries on Device B at the time of provisioning.
- The CMS selects a value for idB (identifying the OSCORE Security Context for messages sent from Device B to Device A) conforming to the following criteria:
  - The total length of idB in bits shall be a multiple of 8 between 16 and 56 inclusive, which corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14 characters inclusive.
  - The first byte of idB shall be 0x01. See Note 1.
  - The value of idB should be distinct from all values of "recipientid" in credential entries on Device A at the time of provisioning.
- The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient entropy.

The CMS then independently provisions credential entries to Device A and Device B.

The CMS provisions the following credential entry to Device A:

- The "subjectuuid" shall be the Device UUID of Device B (that is, the value of "/oic/sec/doxm:deviceuuid" on Device B).

- The "credtype" shall have the value 64.

NOTE 2: The value 64 is the "credtype" value specified for a directly provisioned OSCORE Security Context in ISO/IEC 30118-2.

- The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.
- The "oscore" Property shall be present, and shall include the following Properties:
  - The "senderid" Property shall be set to the lowercase hexadecimal representation of idA with the "0x" encoding prefix omitted.
  - The "recipientid" Property shall be set to the lowercase hexadecimal representation of idB with the "0x" encoding prefix omitted.

The CMS separately provisions the following credential entry to Device B:

- The "subjectuuid" shall be the Device UUID of Device A (that is, the value of "/oic/sec/doxm:deviceuuid" on Device A).
- The "credtype" shall have the value 64. See Note 2.
- The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.
- The "oscore" Property shall be present, and shall include the following Properties:
  - The "senderid" Property shall be set to the lowercase hexadecimal representation of idB with the "0x" encoding prefix omitted.
  - The "recipientid" Property shall be set to the lowercase hexadecimal representation of idA with the "0x" encoding prefix omitted.

6.4 Provisioning Clients and Servers in a Simple Secure Multicast Group

ISO/IEC 30118-2 specifies how Simple Secure Multicast (SSM) secures messages are sent from a Client to multiple Servers in a SSM Group by applying an application layer of in-transit protection below the resource-access authorization layer, using Object Security for Constrained RESTful Environments (OSCORE) [4]. Within the scope of this clause, "Client" refers to the Client of the SSM Group and "Server(s)" refers to a Server(s) in the SSM Group.

SSM is enabled by provisioning an SSM Client Context in a credential entry of the "/oic/sec/cred" Resource of the Client, and provisioning (identical) copies of the SSM Server Context in a credential entry of the "/oic/sec/cred" Resource of the Servers. The present clause provides the requirements on the CMS for this provisioning.

The OBT recognizes during onboarding, by examining the "/oic/sec/doxm:sct" Property, that one or more Devices in the Security Domain support SSM Client Context credentials and/or SSM Server Context credentials. The OBT may prompt the End User to create one or more SSM Groups, or the OBT may create groups without any End User interaction.

On creation of an SSM Group, a corresponding SSM Client Context and SMS Server Context shall be generated by the CMS. The CMS generates four values: idGroup; an associated Device UUID, an OSCORE Master Secret, and SSM Group description.

- The CMS selects a value for idGroup (identifying the OSCORE Security Context for messages sent from the Client to the Servers) conforming to the following criteria:
- The total length of idGroup in bits shall be a multiple of 8 between 16 and 56 inclusive, which corresponds to a hexadecimal representation which is a multiple of 2 between 4 and 14 characters inclusive.
  - The first byte of idGroup shall be 0x02.

NOTE 1: The value 0x02 is the OSCORE Identifier Namespace Prefix value assigned for "Simple Secure Multicast" in ISO/IEC 30118-2.

  - The value of idGroup should be distinct from all values of "recipientid" in credential entries of all Devices in the Security Domain.

- The CMS shall select an SSM-Group-subjectuuid which will be configured in the "subjectuuid" of the credential entry containing the SSM Server Context; the Servers use this "subjectuuid" for access control processing applied to verified SSM Requests as specified in ISO/IEC 30118-2. The SSM-Group-subjectuuid would typically be the Device UUID (that is, the value in "/oic/sec/doxm:deviceuuid") of the Client; this will result in SSM requests from the Client have the same permissions as unicast requests from the Client (e.g. received via DTLS or OSCORE). However, a CMS can select a value for the SSM-Group-subjectuuid, which provides the flexibility for the AMS to configure the Servers with
  - One set of permissions, using ACEs with "subject" matching Client's Device UUID, for unicast requests received from the Client (e.g. received via DTLS or OSCORE), and
  - Another set of permissions, using ACEs with "subject" matching SSM-Group-subjectuuid (and different from the Client's Device UUID), for SSM requests received from the Client.
- The CMS shall generate a 256-bit secret value (the OSCORE Master Secret). The CMS should use a NIST Special Publication 800-90A Revision 1-compliant RNG to guarantee sufficient entropy.
- The CMS or End User should select a human-readable string for identifying the SSM Group. If a value is not selected, then this value defaults to the empty string.

The CMS then independently provisions credential entries to the Client and Servers of the SSM Group.

The CMS provisions the following credential entry, containing the SSM Client Context, to the Client of the SSM Group:

- The "subjectuuid" may be any schema compliant value. This Property serves no purpose when used in an SSM Client Context.
- The "credtype" shall have the value 128.

NOTE 2: The value 128 is the "credtype" value specified for a SSM Client Context in ISO/IEC 30118-2.

- The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.
- The "oscore" Property shall be present, and shall include the following Properties:
  - The "senderid" Property shall be set to the lowercase hexadecimal representation of idGroup with the "0x" encoding prefix omitted.
  - The "desc" Property shall be set to the human-readable description for identifying the SSM Group.

The CMS separately provisions the following credential entry, containing the SSM Server Context, to Servers of the SSM Group:

- The "subjectuuid" shall be set to the SSM-Group-subjectuuid selected by the CMS.
- The "credtype" shall have the value 256.

NOTE 3: The value 256 is the "credtype" value specified for a SSM Server Context in ISO/IEC 30118-2.

- The "privatedata" Property of the credential entry shall be the OSCORE Master Secret generated by the CMS.
- The "oscore" Property shall be present, and shall include the following Properties:
  - The "recipientid" Property shall be set to the lowercase hexadecimal representation of idGroup with the "0x" encoding prefix omitted.
  - The "desc" Property shall be set to the human-readable description for identifying the SSM Group.

These provisioning steps may occur implicitly, that is, without End User interaction.

Ownership Transfer Methods

7.1 Preamble

OTM Implementation requirements are discussed in clause 7.3.1 of ISO/IEC 30118-2.

7.2 Just Works Owner Transfer Method

This OTM is specified in clause 7.3.4.1 of ISO/IEC 30118-2.

All DOTS shall implement the mandatory cipher suites and should implement the optional cipher suites for Devices specified for this OTM in clause 11.3.2.1 of ISO/IEC 30118-2.

Security considerations for this OTM are provided in clause 7.3.4.2 of ISO/IEC 30118-2.

7.3 Random PIN / Shared Credential based Owner Transfer Method

Details of this OTM are provided in clause 7.3.5 of ISO/IEC 30118-2. The following points are pertinent to the DOTS:

- This OTM relies on the Device generating a random number that is communicated to the DOTS over an Out of Band Communication Channel.
  - The Platform hosting a DOTS which supports this OTM shall provide a user interface for manual input of the random number.
  - A DOTS may support other vendor-defined Out of Band Communication Channel for receiving the random number from the Device. Security considerations regarding Out of Band Communication channel are provided in clause 7.3.5.3 of ISO/IEC 30118-2.
- A DOTS shall support receiving a ServerKeyExchange message in the DTLS handshake either with "psk_identity_hint" field formatted as specified in clause 7.3.5.2 of ISO/IEC 30118-2, or with "psk_identity_hint" field comprising only a Device UUID (to ensure backwards compatibility with Devices conforming to older releases). When the DOTS receives the ServerKeyExchange, then
  - The DOTS can identify the new Device with which it is establishing the DOC by matching the "deviceuuid" part of the "psk_identity_hint" field with the "deviceuuid" Property of the "/oic/sec/doxm" Resource being sent in responses when the new Device is in RFOTM and when a Device Onboarding Connection is not currently established. The DOTS shall compute the PIN-authenticated pre-shared key (PPSK) using the algorithm specified in clause 7.3.5.2 of ISO/IEC 30118-2.

Furthermore, the following requirements apply to the DTLS handshake messages for this OTM:

- The DOTS shall set the "psk_identity" field of the ClientKeyExchange message to the string "oic.sec.doxm.rdp".

NOTE: The string "oic.sec.doxm.rdp" is the URN defined for the Random PIN-based OTM in Table 18 of ISO/IEC 30118-2, and is included to allow future OTMs to re-use the DTLS cipher suites without confusion about which OTM should be applied.

All DOTS shall implement the mandatory cipher suites and should implement the optional cipher suites for Devices specified for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2.

Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-2.

7.4 Manufacturer Certificate Based Owner Transfer Method

Details of this OTM are provided in clause 7.3.6 of ISO/IEC 30118-2. The following points are pertinent to the DOTS:

- The DOTS shall validate the certificate presented by the Device in the DTLS handshake against the Trust Anchors contained in its entries of the "/oic/sec/cred" Resource that have a "credusage" Property populated with "oic.sec.cred.mfgtrustca".

- The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2.

All DOTS shall implement the mandatory and optional cipher suites for Devices specified for this OTM in clause 11.3.2.3 of ISO/IEC 30118-2.

Further security considerations for the Manufacturer Certificate Based OTM are provided in clauses 7.3.6.3 and 7.3.6.5 of ISO/IEC 30118-2.

7.5 Vendor-Specific Owner Transfer Methods

Clauses 7.3.1 and 7.3.7 of ISO/IEC 30118-2 provide requirements for Vendor-specific OTMs.

Bibliography

[1] ISO/IEC 30118-3 *Information technology – Open Connectivity Foundation (OCF) Specification – Part 3: Bridging specification*
https://www.iso.org/standard/74240.html
Latest version available at:
https://openconnectivity.org/specs/OCF_Bridging_Specification.pdf

[2] ISO/IEC 30118-7, *Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification*
https://www.iso.org/standard/79175.html
Latest version available at:
https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf

[3] *Open Connectivity Foundation (OCF) Specification – Cloud Security Specification*
Latest version available at:
https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.pdf

[4] IETF RFC 8613, *Object Security for Constrained RESTful Environments (OSCORE)*, July 2019
https://www.rfc-editor.org/info/rfc8613

