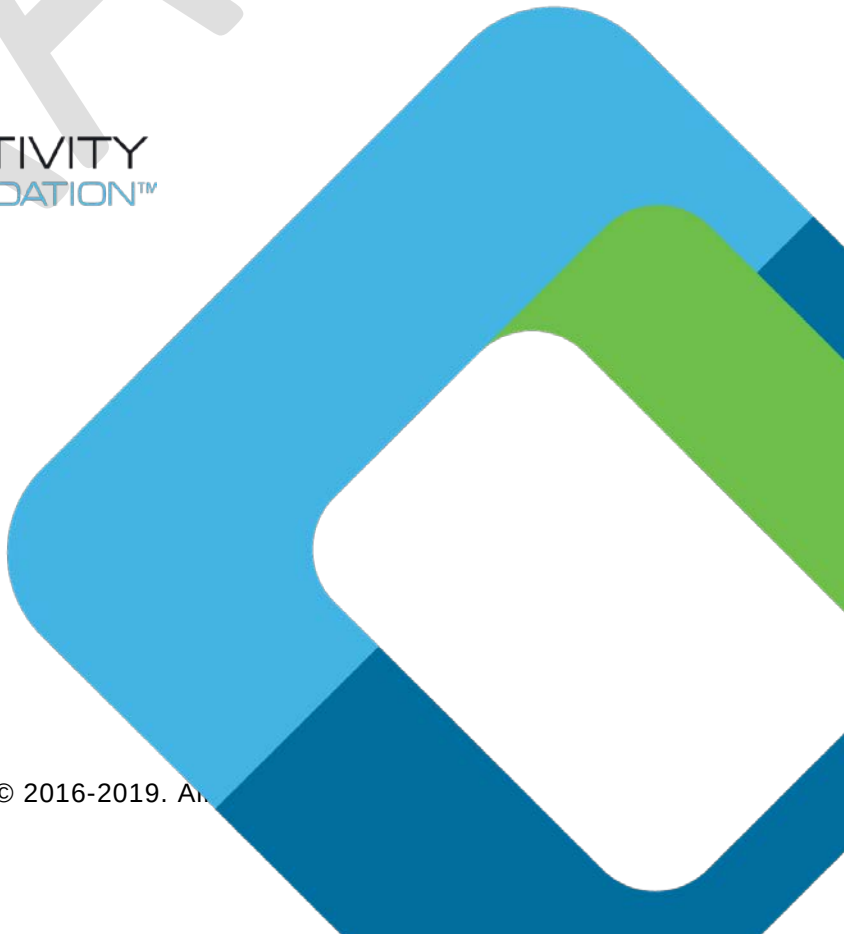
OCF "Essen" – OBT specification – Security WG CR 2857

Legal Disclaimer

OCF Onboarding Tool Specification

VERSION 0.3.6 | June 24, 2019



29

CONTENTS

1 Scope 1
2 Normative References 1
3 Terms, definitions, and abbreviated terms 2
3.1 Terms and definitions 2
3.2 Abbreviated terms 4
4 Document Conventions and Organization 5
5 Services and Availability in the OBT 6
5.1 Purpose of the OBT 6
5.2 General OBT Requirements 7
5.3 DOTS 8
5.3.1 Assuming ownership of a Device 8
5.3.2 DOTS and Bridging 9
5.3.3 Security considerations regarding selecting an Ownership Transfer Method 9
5.4 CMS 10
5.5 AMS 10
6 Certificate Management Requirements 11
6.1 Issuing Identity Certificates and Role Certificates 11
6.2 Provisioning Trust Anchor Certificates 11
7 Ownership Transfer Methods 12
7.1 Preamble 12
7.2 Just Works 12
7.3 Random PIN / Shared Credential Based OTM 12
7.4 Manufacturer Certificate Based OTM 12
7.4.1 Device Onboarding Connection for Manufacturer Certificate Based OTM 12
7.5 Vendor-Specific OTMs 13
Annex: History 13

58 # FIGURES

59 **No table of figures entries found.**

60

61 # Tables

62 Table 1 – Informative overview of OBT access in Device Onboarding States 7

63

64

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, 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 30118-1:2018 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 30118-2:2018 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

ISO/IEC 30118-3:2018 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

OCF Wi-Fi Easy Setup, Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification
Latest version available at:
https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification.pdf

OCF Cloud Specification, Information technology – Open Connectivity Foundation (OCF) Specification – Part 8: Cloud Specification
Latest version available at:
https://openconnectivity.org/specs/OCF_Cloud_Specification.pdf

OCF Cloud Security Specification, Information technology – Open Connectivity Foundation (OCF) Specification – Part X: Cloud Security Specification
Latest version available at:
https://openconnectivity.org/specs/OCF_Cloud_Security_Specification.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 30118-1:2018 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 Control Entry

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.2
Access Control List

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.3
Access Management Service (AMS)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.4
Bridge

Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.5
Bridged Device

Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.1.6
Certified Product List

JSON-formatted list of OCF Certified Products and additional corresponding properties, such as certification status, published on behalf of OCF

3.1.7
Client

Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.8
Credential Management Service (CMS)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.9
Device

Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.10
Device Configuration Resource (DCR)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.11
Device ID

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.12
Device Onboarding Connection (DOC)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.13
Device Ownership Transfer Service (DOTS)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.14
End User

The person using the [particular] product

3.1.15
(OCF) Onboarding

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.16
Onboarding Tool (OBT)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.17
Out-of-Band Communication Channel

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.18
Owned (or "in Owned State")

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.19
Owner Credential (OC)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.20
Property

Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.21
Resource

Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.22
OCF Rooted Certificate Chain

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.23
OCF Security Domain

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.24
Security Virtual Resource (SVR)

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.25
Server

Note 1 to entry: The details are defined in ISO/IEC 30118-1:2018.

3.1.26
Trust Anchor

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.27
Unowned (or "in Unowned State")

Note 1 to entry: The details are defined in ISO/IEC 30118-2:2018.

3.1.28
Virtual OCF Device

Note 1 to entry: The details are defined in ISO/IEC 30118-3:2018.

3.2 Abbreviated terms

3.2.1
ACE
Access Control Entry

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.2
ACL
Access Control List

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.3
AMS
Access Management Service

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.4
CPL
Certified Product List

3.2.5
CMS
Credential Management Service

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.6
DOC
Device Onboarding Connection

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.7
OBT
Onboarding Tool

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.8
OC
Owner Credential

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.9
OTM
Owner Transfer Method

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.10
PIN
Personal Identification Number

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.11
PPSK
PIN-authenticated pre-shared key

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.12
PSK
Pre Shared Key

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.13
SVR
Security Virtual Resource

Note 1 to entry: See ISO/IEC 30118-2:2018.

3.2.14
URI
Uniform Resource Identifier

Note 1 to entry: See ISO/IEC 30118-1:2018.

3.2.15
VOD
Virtual OCF Device

Note 1 to entry: See ISO/IEC 30118-3:2018.

4 Document Conventions and Organization

See ISO/IEC 30118-1:2018.

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.

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 30118-2:2018). 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 facilitiates further configuration of Devices in the OCF Security Domain for various purposes including WiFi configuration (see OCF Wi-Fi Easy Setup) and OCF Cloud access (see OCF Cloud Security Specification).

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 30118-2:2018. Table 1 provides an informative overview of the access granted to the OBT components according the Device Onboarding States.

288 **Table 1 – Informative overview of OBT access in Device Onboarding States**

Device Onboarding State	Description		Applicable Resources & Access	Entity Authorized to READ/WRITE	Purpose
RESET	Full reset of OCF Device to manufacturer default. Unowned		No Access	No Access	Remove info in SVRs.
RFOTM	Ready for Ownership Transfer Mechanism. Unowned	Prior to successful OTM	"/oic/sec/doxm" (R: all, W: oxmsel)	Any	R: Determine supported OTMs W: Select an OTM
		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. Owned.		"/oic/sec/cred" (RW)	CMS or matching ACE	Establish credentials for authenticating Devices in normal operation, including Roles
			"/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. Owned.		"/oic/sec/pstat"	DOTS, CMS, AMS or matching ACE	Transition to RFPRO, SRESET or RESET
			Vertical Resources	Matching ACE	Normal Operation
SRESET	Soft RESET. Owned		"/oic/sec/cred" (RW)	CMS	Corrections as needed
			"/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

289

290 ## 5.2 General OBT Requirements

291 An OBT shall be hosted on an OCF Device.

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

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

The software of an OBT shall be field updatable. (This requirement need not be tested but can be certified via a vendor declaration.)

After successful OTM, but before placing the newly-onboarded Device in RFNOP, the OBT shall remove all ACEs where the Subject is “anon-clear” or “auth-crypt”, and the Resources array includes a SVR.

The OBT is expected to support all mandatory and optional ciphersuite in clauses 11.3.3 and 11.3.4 of ISO/IEC 30118-2:2018.

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 30118-2:2018.

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 30118-2:2018.
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 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 shall 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 may update the "deviceuuid" of the "/oic/sec/doxm" Resource to a value that the DOTS has selected.
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 30118-2:2018.
    b) The DOTS shall add a 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 30118-2:2018 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 30118-2:2018 and stores it with the owner credential

11) .The following steps are applied following successful establishment of ownership credentials, 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 update the "rowneruuid" Property of the "/oic/sec/pstat" Resource with the UUID of the DOTS.
- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/cred" Resource with the UUID of the CMS.
- The DOTS shall update the "rowneruuid" Property of the "/oic/sec/acl2" Resource with the UUID of the AMS.
- 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.

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 [BridgingSpec]. 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 [BridgingSpec].

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 an DOTS might require that all of the Devices being onboarded support either the Random PIN or the Manufacturer Certificate OTM.

5.4 CMS

An introduction to the Credential Management is provided in clause 5.4.3 of ISO/IEC 30118-2:2018.

The Credential Types are specified in clause 9.3 of ISO/IEC 30118-2:2018.

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 30118-2:2018. The CMS shall support removing entries from the "creds" Property to the "/oic/sec/cred" Resource as defined in clauses 13.3 of ISO/IEC 30118-2:2018. 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 30118-2:2018.

Certificate provisioning of local Credentials is described in clause 9.4.5 of ISO/IEC 30118-2:2018. 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 30118-2:2018.
- 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.
- 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 30118-2:2018, using the "/oic/sec/crl" Resource specified in clause 13.4 of ISO/IEC 30118-2:2018. 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 30118-2:2018.

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 30118-2:2018.

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 30118-2:2018.

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 30118-2:2018.

The AMS should support other operations as defined in clause 13.5 of ISO/IEC 30118-2:2018.

Clause 6.2 of OCF Cloud Security Specification 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 evalation and enforcement at Servers specified in clause 12 of ISO/IEC 30118-2:2018. The formatting of the ACL Resource specified in clause 13.5 of ISO/IEC 30118-2:2018.

6 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 30118-2:2018.
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 30118-2:2018.
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.trustca" corresponding to a certificate Trust Anchor
   – The "publicdata" Property shall contain the newly-created certificate chain.

See clause 13.3.1 of ISO/IEC 30118-2:2018 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 30118-2:2018 for details of a request adding an entry to the "creds" Property of the "/oic/sec/cred" Resource.

7 Ownership Transfer Methods

7.1 Preamble

OTM Implementation requirements are discussed in clause 7.3.1 of ISO/IEC 30118-2:2018.

7.2 Just Works

This OTM is specified in clause 7.3.4.1 of ISO/IEC 30118-2:2018.

All DOTS are expected to implement the following ciphersuites:

- The mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.1 of ISO/IEC 30118-2:2018, and
- The OCF-defined vendor-specific ciphersuites (these were used prior to the IETF specifying the ciphersuites listed in clause 11.3.2.1 of ISO/IEC 30118-2:2018):
  - TLS_ECDH_ANON_WITH_AES_128_CBC_SHA256 (with the value 0xFF00).
  - TLS_ECDH_ANON_WITH_AES_256_CBC_SHA256 (with the value 0xFF01).

Security considerations for this OTM are provided in clause 7.3.4.2 of ISO/IEC 30118-2:2018.

7.3 Random PIN / Shared Credential Based OTM

Details of this OTM is provided in clause 7.3.5 of ISO/IEC 30118-2:2018. 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 Communications 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 Communications Channels for receiving the random number from the Device. Security considerations regarding out-of-band communications channels are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.
- The DOTS shall compute the PIN-authenticated pre-shared key (PPSK) using the algorithm specified in clause 7.3.5.2 of ISO/IEC 30118-2:2018.

All DOTS are expected to implement the mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.2 of ISO/IEC 30118-2:2018.

Further security considerations for this OTM are provided in clause 7.3.5.3 of ISO/IEC 30118-2:2018.

7.4 Manufacturer Certificate Based OTM

7.4.1 Device Onboarding Connection for Manufacturer Certificate Based OTM

Details of this OTM are provided in clause 7.3.6 of ISO/IEC 30118-2:2018. The following points are pertinent to the DOTS:

- The DOTS shall validate the certificate presented by the Device in the TLS Handshake against the Trust Anchors configured to the DOTS.

- The certificate profiles are specified in clause 9.4.2 of ISO/IEC 30118-2:2018.

All DOTS are expected to implement the mandatory and optional ciphersuites for Devices specified for this OTM in clause 11.3.2.3 of ISO/IEC 30118-2:2018.

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 30118-2:2018.

7.5 Vendor-Specific OTMs

Clauses 7.3.1 and 7.3.7 of ISO/IEC 30118-2:2018 provide requirements for Vendor-specific OTMs.

Annex: History

Version	Date	Contributors	Changes
0.0.1	2019-03-19	Brian Scriber	Initial version
0.0.1	2019-04-04	Brian Scriber	Added action items
0.0.2	2019-04-10	Phil Hawkes	Added applicable text from Main Security Spec. Added text referring to Main Security Spec where applicable. Also added some other text too.
0.0.3	2019-04-17	Olek and Phil	A couple of rounds of review by Olek & adjustment by Phil. Added Table "Overview of OBT access in Device Onboarding States" in clause 5.1. Added some references, terms and abbreviations.
0.0.4	2019-04-19	Olek	Updates based on feedback from SecWG.
0.0.5	2019-05-09	Phil	Updates during the Security F2F, changes tracked.
0.3	2019-05-09	Phil	V0.0.5 with changes accepted. Approved to v0.3 in SecWG on 2019-05-09.
0.3.1	2019-05-30	Phil	Incorporating feedback from other WG. Some rearrangement (most of the content in the subclause formally titled "Establishing Owner Credentials" (under the "DOTS" clause) has become clause 5.3 "Example Flows". Moved text on security profiles to under 6.5 "Manufacturer Certificate Based OTM". Incorporated text from bug 2773.
0.3.2	2019-06-03	Phil	Incorporating feedback from Sec WG call. Added some definitions. Accepted previous changes. Added links to references. Changed clause 5.4.1 into a sequence of steps. Accepted all format changes
0.3.3	2019-06-16	Phil	Accepted previous changes. Applied minor editorial updates.
0.3.4	2019-06-17	Phil	Did not accept changes of previous version. Updated based on review of normative statements for test cases.
0.3.5	2019-06-18	Phil	Did not accept changes of previous version. Updated based on feedback from SecWG at NOLA F2F.
0.3.6	2019-06-20	Phil	Updated based on feedback from SecWG at NOLA F2F.

