



BSI Standards Publication

Information technology — Open Connectivity Foundation (OCF) Specification

Part 2: Security specification

National foreword

This British Standard is the UK implementation of ISO/IEC 30118-2:2021. It supersedes BS ISO/IEC 30118-2:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee ICT/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 16185 4

ICS 35.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**Information technology — Open
Connectivity Foundation (OCF)
Specification —**

**Part 2:
Security specification**

*Technologies de l'information — Specification de la Fondation pour la
connectivité ouverte (Fondation OCF) —*

Partie 2: Spécification de sécurité



Reference number
ISO/IEC 30118-2:2021(E)

Documents
AVA Document Sharing Hub
© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	ix
Introduction.....	x
1 Scope	1
2 Normative References	1
3 Terms, definitions and abbreviated terms.....	3
3.1 Terms and definitions	3
3.2 Symbols and abbreviated terms.....	5
4 Document conventions and organization.....	7
4.1 Conventions	7
4.2 Notation.....	7
4.3 Data types	8
4.4 Document structure	8
5 Security overview	8
5.1 Preamble	8
5.2 Access control	10
5.2.1 Access control general.....	10
5.2.2 ACL architecture.....	11
5.3 Onboarding overview.....	12
5.3.1 Onboarding general.....	12
5.3.2 Onboarding steps	14
5.3.3 Establishing a Device Owner	15
5.3.4 Provisioning for Normal Operation	16
5.3.5 OCF Compliance Management System	16
5.4 Provisioning.....	16
5.4.1 Provisioning general	16
5.4.2 Access control provisioning	17
5.4.3 Credential provisioning.....	17
5.4.4 Role provisioning	17
5.5 Secure Resource Manager (SRM).....	17
5.6 Credential overview	18
5.7 Event logging	18
5.7.1 Event logging general	18
6 Security for the discovery process.....	19
6.1 Preamble	19
6.2 Security considerations for discovery.....	19
7 Security provisioning	21
7.1 Device identity	21
7.1.1 General Device identity	21
7.1.2 Device identity for devices with UAID [Deprecated]	21
7.2 Device ownership.....	21
7.3 Device Ownership Transfer Methods	22
7.3.1 OTM implementation requirements.....	22
7.3.2 SharedKey credential calculation	23
7.3.3 Certificate credential generation	24
7.3.4 Just-Works OTM	24

7.3.5	Random PIN based OTM	25
7.3.6	Manufacturer Certificate Based OTM	28
7.3.7	Vendor specific OTMs	30
7.3.8	Establishing Owner Credentials	31
7.3.9	Security profile assignment	34
7.4	Provisioning	35
7.4.1	Provisioning flows	35
8	Device Onboarding state definitions	36
8.1	Device Onboarding general	36
8.2	Device Onboarding-Reset state definition	37
8.3	Device Ready-for-OTM State definition	38
8.4	Device Ready-for-Provisioning State Definition	39
8.5	Device Ready-for-Normal-Operation state definition	39
8.6	Device Soft Reset State definition	40
9	Security Credential management	41
9.1	Preamble	41
9.2	Credential lifecycle	41
9.2.1	Credential lifecycle general	41
9.2.2	Creation	41
9.2.3	Deletion	41
9.2.4	Refresh	41
9.2.5	Revocation	42
9.3	Credential types	42
9.3.1	Preamble	42
9.3.2	Pair-wise symmetric key credentials	42
9.3.3	Group symmetric key credentials	42
9.3.4	Asymmetric authentication key credentials	43
9.3.5	Asymmetric Key Encryption Key credentials	43
9.3.6	Certificate credentials	44
9.3.7	Password credentials	44
9.4	Certificate based key management	44
9.4.1	Overview	44
9.4.2	X.509 digital certificate profiles	45
9.4.3	Certificate Revocation List (CRL) Profile [deprecated]	54
9.4.4	Resource model	54
9.4.5	Certificate provisioning	54
9.4.6	CRL provisioning [deprecated]	55
10	Device authentication	55
10.1	Device authentication general	55
10.2	Device authentication with symmetric key credentials	56
10.3	Device authentication with raw asymmetric key credentials	56
10.4	Device authentication with certificates	56
10.4.1	Device authentication with certificates general	56
10.4.2	Role assertion with certificates	57
10.4.3	OCF PKI Roots	58
10.4.4	PKI Trust Store	58
10.4.5	Path Validation and extension processing	59

11	Message integrity and confidentiality.....	59
11.1	Preamble	59
11.2	Session protection with DTLS	59
11.2.1	DTLS protection general	59
11.2.2	Unicast session semantics	59
11.3	Cipher suites	59
11.3.1	Cipher suites general	59
11.3.2	Cipher suites for Device Ownership Transfer	60
11.3.3	Cipher Suites for symmetric keys.....	60
11.3.4	Cipher suites for asymmetric credentials	61
12	Access control.....	62
12.1	ACL generation and management	62
12.2	ACL evaluation and enforcement	62
12.2.1	ACL evaluation and enforcement general	62
12.2.2	Host reference matching	62
12.2.3	Resource wildcard matching.....	62
12.2.4	Multiple criteria matching	63
12.2.5	Subject matching using wildcards.....	63
12.2.6	Subject matching using roles	64
12.2.7	ACL evaluation	64
13	Security Resources	66
13.1	Security Resources general	66
13.2	Device Owner Transfer Resource.....	68
13.2.1	Device Owner Transfer Resource General	68
13.2.2	OCF defined OTMs.....	71
13.3	Credential Resource	71
13.3.1	Credential Resource general.....	71
13.3.2	Properties of the Credential Resource	76
13.3.3	Key formatting	78
13.3.4	Credential Refresh Method details [deprecated].....	79
13.4	Certificate Revocation List	79
13.4.1	CRL Resource definition [deprecated]	79
13.5	ACL Resources	79
13.5.1	ACL Resources general.....	79
13.5.2	OCF Access Control List (ACL) BNF defines ACL structures.	79
13.5.3	ACL Resource	80
13.6	Access Manager ACL Resource [deprecated]	85
13.7	Signed ACL Resource [deprecated]	85
13.8	Provisioning Status Resource.....	85
13.9	Certificate Signing Request Resource	91
13.10	Roles Resource	91
13.11	Auditable Events List Resource	93
13.11.1	Auditable Events List Resource general	93
13.12	Security Virtual Resources (SVRs) and Access Policy	96
13.13	SVRs, discoverability and OCF Endpoints	97
13.14	Additional privacy consideration for Core Resources	97
13.15	Easy Setup Resource Device state	98

13.16	List of Auditable Events	100
13.17	Security Domain Information Resource	102
14	Security hardening guidelines/ execution environment security	103
14.1	Preamble	103
14.2	Execution environment elements	103
14.2.1	Execution environment elements general	103
14.2.2	Secure storage.....	103
14.2.3	Secure execution engine	106
14.2.4	Trusted input/output paths	106
14.2.5	Secure clock	106
14.2.6	Approved algorithms.....	107
14.2.7	Hardware tamper protection	107
14.3	Secure Boot	107
14.3.1	Concept of software module authentication	107
14.3.2	Secure Boot process	109
14.3.3	Robustness requirements	109
14.4	Attestation.....	110
14.5	Software Update.....	110
14.5.1	Overview	110
14.5.2	Recognition of current differences.....	110
14.5.3	Software Version Validation.....	111
14.5.4	Software Update	111
14.5.5	Recommended usage	112
14.6	Non-OCF Endpoint interoperability.....	112
14.7	Security levels	112
14.8	Security Profiles	113
14.8.1	Security Profiles general.....	113
14.8.2	Identification of Security Profiles (Normative).....	114
14.8.3	Security Profiles	115
15	Device Type specific requirements	120
15.1	Bridging security	120
15.1.1	Universal requirements for Bridging to another Ecosystem	120
15.1.2	Additional security requirements specific to bridged protocols.....	121
Annex A (informative)	Access control examples	123
A.1	Example OCF ACL Resource	123
Annex B (informative)	Execution environment security profiles.....	124
Annex C (normative)	Resource Type definitions.....	125
C.1	List of Resource Type definitions	125
C.2	Access Control List-2	125
C.2.1	Introduction	125
C.2.2	Well-known URI.....	125
C.2.3	Resource type.....	125
C.2.4	OpenAPI 2.0 definition.....	125
C.2.5	Property definition.....	133
C.2.6	CRUDN behaviour.....	133
C.3	Credential.....	134
C.3.1	Introduction	134
C.3.2	Well-known URI.....	134

C.3.3	Resource type.....	134
C.3.4	OpenAPI 2.0 definition.....	134
C.3.5	Property definition.....	143
C.3.6	CRUDN behaviour.....	143
C.4	Certificate Signing Request.....	143
C.4.1	Introduction	143
C.4.2	Well-known URI.....	143
C.4.3	Resource type.....	143
C.4.4	OpenAPI 2.0 definition.....	144
C.4.5	Property definition.....	145
C.4.6	CRUDN behaviour.....	145
C.5	Device Owner Transfer Method	146
C.5.1	Introduction	146
C.5.2	Well-known URI.....	146
C.5.3	Resource type.....	146
C.5.4	OpenAPI 2.0 definition.....	146
C.5.5	Property definition.....	149
C.5.6	CRUDN behaviour.....	150
C.6	Device provisioning status.....	151
C.6.1	Introduction	151
C.6.2	Well-known URI.....	151
C.6.3	Resource type.....	151
C.6.4	OpenAPI 2.0 definition.....	151
C.6.5	Property definition.....	154
C.6.6	CRUDN behaviour.....	158
C.7	Asserted roles.....	158
C.7.1	Introduction	158
C.7.2	Well-known URI.....	158
C.7.3	Resource type.....	158
C.7.4	OpenAPI 2.0 definition.....	158
C.7.5	Property definition.....	166
C.7.6	CRUDN behaviour.....	167
C.8	Security Profile	167
C.8.1	Introduction	167
C.8.2	Well-known URI.....	167
C.8.3	Resource type.....	167
C.8.4	OpenAPI 2.0 definition.....	167
C.8.5	Property definition.....	169
C.8.6	CRUDN behaviour.....	170
C.9	Auditable Event List	170
C.9.1	Introduction	170
C.9.2	Well-known URI.....	170
C.9.3	Resource type.....	170
C.9.4	OpenAPI 2.0 definition.....	170
C.9.5	Property definition.....	174
C.9.6	CRUDN behaviour.....	177
C.10	OCF Security Domain information	177
C.10.1	Introduction	177

C.10.2	Well-known URI.....	177
C.10.3	Resource type.....	177
C.10.4	OpenAPI 2.0 definition.....	177
C.10.5	Property definition.....	179
C.10.6	CRUDN behaviour.....	180
Annex D (informative) OID definitions		181
Annex E (informative) Security considerations specific to Bridged Protocols		183
E.1	Security considerations specific to the AllJoyn Protocol	183
E.2	Security considerations specific to the Bluetooth LE Protocol	183
E.3	Security considerations specific to the oneM2M Protocol	184
E.4	Security considerations specific to the U+ Protocol.....	184
E.5	Security considerations specific to the Z-Wave Protocol.....	184
E.6	Security considerations specific to the Zigbee Protocol	186
E.7	Security considerations specific to the the EnOcean Radio Protocol	186

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 Security Specification, version 2.2.0) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 30118-2:2018), which has been technically revised.

The main changes compared to the previous edition are as follows:

- movement of some text to onboarding tool specification;
- movement of some text to cloud security specification;
- addition of certificate profiles for identity and role X509 certificates;
- addition of text for: software update, end of life, end of service and auditable events;
- improvements to access control;
- addition of OCF cloud security sections;
- addition of clarifications throughout.

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) Specification —

Part 2: Security specification

1 Scope

This document defines security objectives, philosophy, Resources and mechanism that impacts OCF base layers of ISO/IEC 30118-1. ISO/IEC 30118-1 contains informative security content. The OCF Security Specification contains security normative content and may contain informative content related to the OCF base or 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. 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 30118-3 Information technology -- Open Connectivity Foundation (OCF) Specification -- Part 3: Bridging specification
<https://www.iso.org/standard/74240.html>

OCF Wi-Fi Easy Setup, Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification

OCF Cloud Specification, Information technology – Open Connectivity Foundation (OCF) Specification – Part 8: Cloud Specification

OCF Cloud Security Specification - Open Connectivity Foundation (OCF) Specification – Cloud Security Specification

OCF Onboarding Tool Specification - Open Connectivity Foundation (OCF) Specification – Onboarding Tool Specification

JSON SCHEMA, draft version 4, <http://json-schema.org/latest/json-schema-core.html>.

IETF RFC 2315, *PKCS #7: Cryptographic Message Syntax Version 1.5*, March 1998,
<https://tools.ietf.org/html/rfc2315>

IETF RFC 2898, *PKCS #5: Password-Based Cryptography Specification Version 2.0*, September 2000, <https://tools.ietf.org/html/rfc2898>

IETF RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*, November 2000,
<https://tools.ietf.org/html/rfc2986>

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, July 2005, <https://tools.ietf.org/html/rfc4122>

IETF RFC 4279, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, December 2005, <https://tools.ietf.org/html/rfc4279>

IETF RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*, May 2006, <https://tools.ietf.org/html/rfc4492>

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008, <https://tools.ietf.org/html/rfc5246>

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008, <https://tools.ietf.org/html/rfc5280>

IETF RFC 5489, *ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)*, March 2009, <https://tools.ietf.org/html/rfc5489>

IETF RFC 5545, *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*, September 2009, <https://tools.ietf.org/html/rfc5545>

IETF RFC 5755, *An Internet Attribute Certificate Profile for Authorization*, January 2010, <https://tools.ietf.org/html/rfc5755>

IETF RFC 6347, *Datagram Transport Layer Security Version 1.2*, January 2012, <https://tools.ietf.org/html/rfc6347>

IETF RFC 6655, *AES-CCM Cipher Suites for Transport Layer Security (TLS)*, July 2012, <https://tools.ietf.org/html/rfc6655>

IETF RFC 6749, *The OAuth 2.0 Authorization Framework*, October 2012, <https://tools.ietf.org/html/rfc6749>

IETF RFC 6750, *The OAuth 2.0 Authorization Framework: Bearer Token Usage*, October 2012, <https://tools.ietf.org/html/rfc6750>

IETF RFC 7228, *Terminology for Constrained-Node Networks*, May 2014, <https://tools.ietf.org/html/rfc7228>

IETF RFC 7250, *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, June 2014, <https://tools.ietf.org/html/rfc7250>

IETF RFC 7251, *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS*, June 2014, <https://tools.ietf.org/html/rfc7251>

IETF RFC 7515, *JSON Web Signature (JWS)*, May 2015, <https://tools.ietf.org/html/rfc7515>

IETF RFC 7519, *JSON Web Token (JWT)*, May 2015, <https://tools.ietf.org/html/rfc7519>

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

IETF RFC 8392, *CBOR Web Token (CWT)*, May 2018, <https://tools.ietf.org/html/rfc8392>

IETF RFC 8520, *Manufacturer Usage Description Specification*, Mar 2019, <https://tools.ietf.org/html/rfc8520>

oneM2M Release 3 Specifications, <http://www.onem2m.org/technical/published-drafts>

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 30118-1 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 Management Service (AMS)

service that dynamically constructs ACL Resources in response to a Device Resource request

Note 1 to entry: An AMS can evaluate access policies remotely and supply the result to a Server which allows or denies a pending access request. An AMS is authorised to provision ACL Resources.

3.1.2

Credential Management Service (CMS)

name and Resource Type ("oic.sec.cms") given to a Device that is authorized to provision credential Resources

3.1.3

Device Class

IETF RFC 7228 defined device class

3.1.4

Device Ownership Transfer Service (DOTS)

logical entity that establishes device ownership

3.1.5

End-Entity

any certificate holder which is not a Root or Intermediate Certificate Authority

Note 1 to entry: Typically, a device certificate.

3.1.6

Intermediary

Device that implements both Client and Server roles and may perform protocol translation, virtual device to physical device mapping or Resource translation

3.1.7

OCF Cipher Suite

set of algorithms and parameters that define the cryptographic functionality of a Device. The OCF Cipher Suite includes the definition of the public key group operations, signatures, and specific hashing and encoding used to support the public key.

3.1.8

OCF Rooted Certificate Chain

collection of X.509 v3 certificates in which each certificate chains to a trust anchor certificate which has been issued by a certificate authority under the direction, authority, and approval of the Open Connectivity Foundation Board of Directors as a trusted root for the OCF ecosystem.

3.1.9

Onboarding Tool (OBT)

tool that implements *DOTS*(3.1.4), *AMS*(3.1.1), and *CMS*(3.1.2) functionality

3.1.10

Out of Band Communication Channel

any mechanism for delivery of a secret from one party to another, not specified by OCF

3.1.11

Owner Credential (OC)

credential, provisioned to a Device, for the purposes of mutual authentication of the Device and *OBT*(3.1.9) during subsequent interactions, identified by having a Subject UUID matching the Resource Owner Id of the Device Ownership Transfer Resource hosted by a Device that has the credential

3.1.12

Role (Network context)

stereotyped behavior of a Device; one of [Client, Server or Intermediary]

3.1.13

Role Identifier

Property of an OCF credentials Resource or element in a role certificate that identifies a privileged role that a Server Device associates with a Client Device for the purposes of making authorization decisions when the Client Device requests access to Device Resources.

3.1.14

Secure Resource Manager (SRM)

module in the OCF Core that implements security functionality that includes management of security Resources such as ACLs, credentials and Device owner transfer state.

3.1.15

Security Virtual Resource (SVR)

Resource supporting security features.

Note 1 to entry: For a list of all the SVRs please see clause 13.

3.1.16

Trust Anchor

well-defined, shared authority, within a trust hierarchy, by which two cryptographic entities (e.g. a Device and an *OBT*(3.1.9)) can assume trust

3.1.17

Device Configuration Resource (DCR)

Resource that is any of the following:

- a) a Discovery Core Resource, or
- b) a Security Virtual Resource, or
- c) a Wi-Fi Easy Setup Resource ("oic.r.easyssetup", "oic.r.wificonf", "oic.r.devconf"), or
- d) a CoAP Cloud Configuration Resource ("oic.r.coapcloudconf"), or
- e) a Software Update Resource ("oic.r.softwareupdate"), or
- f) a Maintenance Resource ("oic.wk.mnt").

3.1.18**Non-Configuration Resource (NCR)**

Resource that is not a Device Configuration Resource (3.1.17)

3.1.19**OCF Security Domain**

set of onboarded OCF Devices that are provisioned with credentialing information for confidential communication with one another

3.1.20**Owned (or "in Owned State")**

having the "owned" Property of the "/oic/sec/doxm" Resource equal to "TRUE"

3.1.21**Unowned (or "in Unowned State")**

having the "owned" Property of the "/oic/sec/doxm" Resource equal to "FALSE"

3.1.22**OCF Onboarding**

initial establishment of ownership over a Device, and initial provisioning of the Device for normal operation

3.1.23**Auditable Event**

system activity that may be indicative of a violation of security policy

3.1.24**Auditable Event Entry**

record of the details of an Auditable Event

3.1.25**End User**

person using the [particular] product

3.2 Symbols and abbreviated terms

AC	Access Control
ACE	Access Control Entry
ACL	Access Control List
AEE	Auditable Event Entry
AES	Advanced Encryption Standard
AMS	Access Management Service
CMS	Credential Management Service
CRUDN	CREATE, RETREIVE, UPDATE, DELETE, NOTIFY
CSR	Certificate Signing Request
CVC	Code Verification Certificate
ECC	Elliptic Curve Cryptography

ECDSA	Elliptic Curve Digital Signature Algorithm
EKU	Extended Key Usage
DOTS	Device Ownership Transfer Service
ID	Identity/Identifier
JSON	JavaScript Object Notation.
JWS	JSON Web Signature.
KDF	Key Derivation Function
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NVRAM	Non-Volatile Random-Access Memory
OC	Owner Credential
OCSP	Online Certificate Status Protocol
OBT	Onboarding Tool
OID	Object Identifier
OTM	Owner Transfer Method
OWASP	Open Web Application Security Project.
PE	Policy Engine
PIN	Personal Identification Number
PPSK	PIN-authenticated pre-shared key
PRF	Pseudo Random Function
PSI	Persistent Storage Interface
PSK	Pre Shared Key
RBAC	Role Based Access Control
RM	Resource Manager
RNG	Random Number Generator
RFNOP	Ready for Normal Operation
RFOTM	Ready for OTM
RFPRO	Ready for Provisioning
SBAC	Subject Based Access Control
SEE	Secure Execution Environment
SRESET	Soft Reset

SRM	Secure Resource Manager
SVR	Security Virtual Resource
SW	Software
URI	Uniform Resource Identifier
VOD	Virtual OCF Device

4 Document conventions and organization

4.1 Conventions

This document defines Resources, protocols and conventions used to implement security for OCF core framework and applications.

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

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.

Figure 1 depicts interaction between OCF Devices.

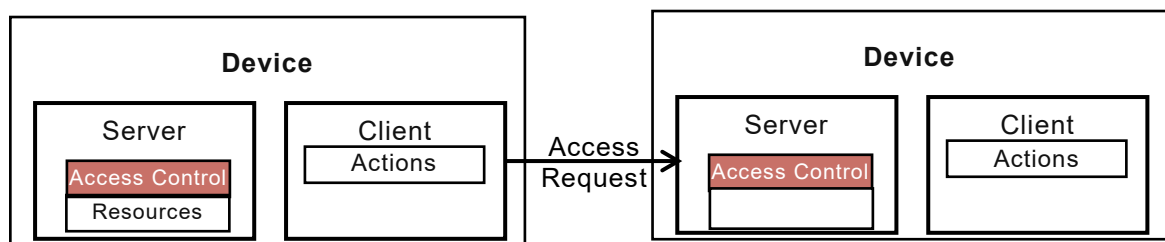


Figure 1 – OCF interaction

Devices may implement a Client role that performs Actions on Servers. Actions access Resources managed by Servers. The OCF stack enforces access policies on Resources. End-to-end Device interaction can be protected using session protection protocol (e.g. DTLS) or with data encryption methods.

4.2 Notation

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

Required (or **shall** or **mandatory**).

These basic features shall be implemented to comply with OCF 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**).

These features add functionality supported by OCF Core Architecture and should be implemented. Recommended features take advantage of the capabilities OCF 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).

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

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.

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.

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

Words that are emphasized are printed in italic.

4.3 Data types

See ISO/IEC 30118-1.

4.4 Document structure

Informative clauses may be found in the Overview clauses, while normative clauses fall outside of those clauses.

The Security Specification may use the OpenAPI specification as the API definition language. The mapping of the CRUDN actions is specified in ISO/IEC 30118-1.

5 Security overview

5.1 Preamble

The goal of OCF's security architecture is to protect the data and device states represented by the OCF Resources. From the OCF perspective, a Device is a certifiable logical entity that participates in an OCF ecosystem. During interactions between Devices, the Device acting as the Server holds and controls the Resources and provides the Device acting as a Client access to those Resources, subject to a set of security mechanisms and conforming to the policies configured by the OCF Security Domain Owner. The Platform hosting the Device may provide security hardening to ensure robustness of the variety of operations described in this document. Multiple Devices may be hosted by the same Platform.

The security model is depicted in Figure 2 and described in the following steps:

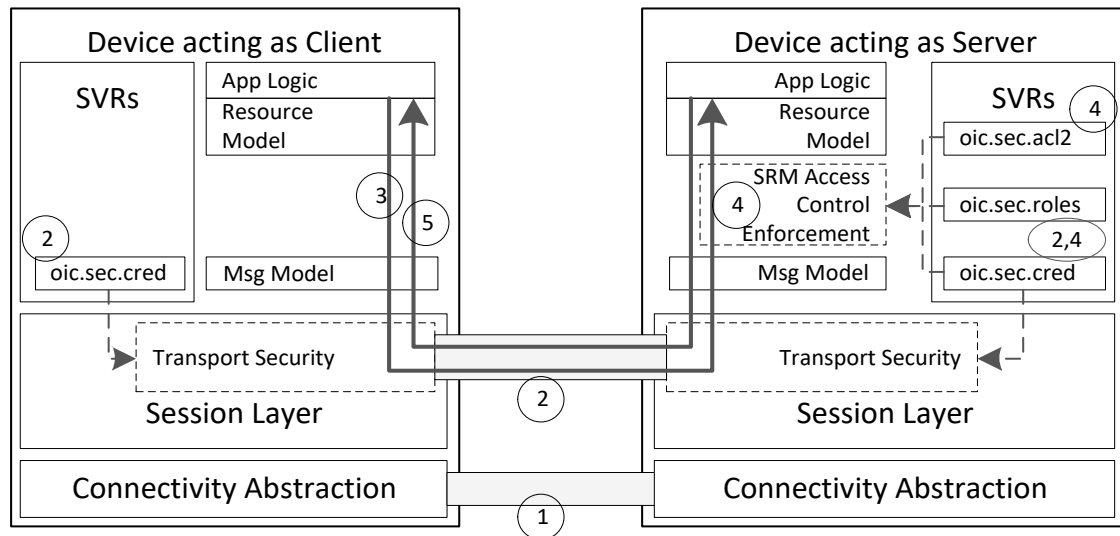


Figure 2 – OCF layers

- 1) The Client establishes a network connection to the Server (Device holding the Resources).
- 2) The Devices (Server and Client) exchange messages either via a mutually-authenticated secure channel between the two Devices or via an unsecured connection.
 - a) The "/oic/sec/cred" Resource on each Device holds the credentials used for mutual authentication and credentials used for role authorization.
 - b) Messages received over a secured channel are associated with a "deviceUUID". In the case of a certificate credential, the "deviceUUID" is part of the certificate received from the other Device. In the case of a symmetric key credential, the "deviceUUID" is associated with the credential in the "/oic/sec/cred" Resource.
 - c) The Client may present its role certificate to request association with a role identifier ("roleid"). The Server may associate the Client with any number of role identifiers.
 - d) Requests received by a Server over an unsecured channel are treated as anonymous and are not associated with any "deviceUUID" or "roleid".
- 3) The Client submits a request to the Server.
- 4) The Server receives the request.
 - a) If the request is received over an unsecured channel, the Server treats the request as anonymous and no "deviceUUID" or "roleid" are associated with the request.
 - b) If the request is received over a secured channel, then the Server associates the request with the "deviceUUID" of the Client and all valid "roleid" values of the Client by default.
 - c) The Server then consults the Access Control List (ACL), and looks for an Access Control Entry (ACE) matching the following criteria:
 - i) The requested Resource matches a Resource reference in the ACE
 - ii) The requested operation is permitted by the "permissions" of the ACE, and

- iii) The "subjectUUID" contains either one of a special set of wildcard values or, if the Device is not anonymous, the subject matches the Client "deviceUUID" associated with the request or a valid "roleid" associated with the request. The special wildcard values authorize all Devices communicating over either authenticated and encrypted sessions or unsecured sessions to interact according to the ACE.

If there is a matching ACE, then access to the Resource is permitted; otherwise access is denied. Access is enforced by the Server's Secure Resource Manager (SRM).

5) The Server sends a response back to the Client.

Resource protection includes protection of data both while at rest and during transit. Aside from access control mechanisms, the OCF Security Specification does not include specification of secure storage of Resources. Secure storage may be accomplished through the use of hardware security or encryption of data at rest. The exact implementation of secure storage is subject to a set of hardening requirements that are specified in clause 14 and may be subject to certification guidelines.

Data in transit protection is specified fully as a normative part of this document. This document only supports in transit data protection at the transport layer through use of mechanisms such as DTLS.

NOTE: DTLS will provide packet by packet protection, rather than protection for the payload as whole. For instance, if the integrity of the entire payload as a whole is required, separate signature mechanisms must have already been in place before passing the packet down to the transport layer.

Figure 3 depicts OCF Security Enforcement Points.

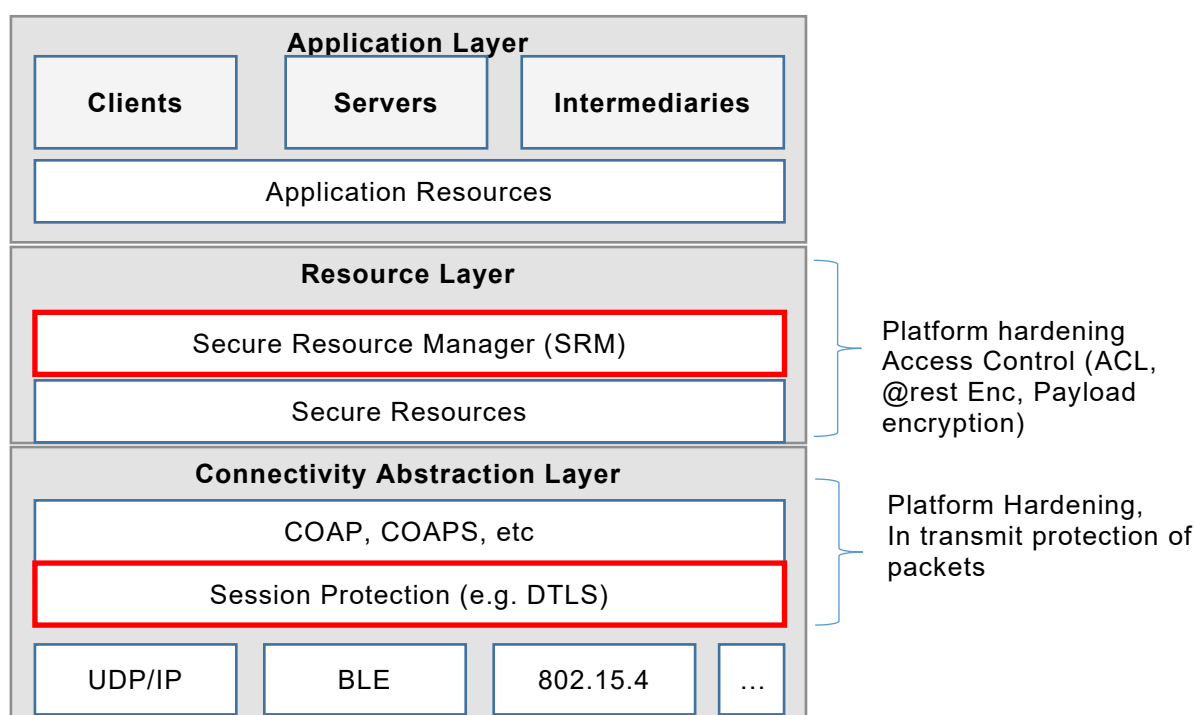


Figure 3 – OCF security enforcement points

5.2 Access control

5.2.1 Access control general

The OCF framework assumes that Resources are hosted by a Server and are made available to Clients subject to access control and authorization mechanisms. The Resources at the Server are protected

through implementation of access control, authentication and confidentiality protection. This clause provides an overview of access control through the use of Access Control Lists. However, access control in OCF is agnostic regarding transport and connectivity abstraction layers.

Implementation of access control relies on a-priori definition of a set of access policies for the Resource. The policies are stored locally in an ACL Resource provisioned by an Access Management Service (AMS) in the form of Access Control Entries (ACE). The lack of such an associated ACE results in the Resource being inaccessible. Multiple types of access control mechanisms may be applied:

- Subject-based access control (SBAC), where the ACE matches the identity of the Client against the subject included in the policy defined for the Resource. Asserting the identity of the Client requires an authentication process.
- Role-based Access Control (RBAC), where the ACE matches a role identifier included in the policy for the Resource to a role identifier associated with the Client.
- Wildcard-based Access Control, where the ACE matches a connection type, used to access the Resource (i.e. any mutually-authenticated connection).

The ACE only applies if the ACE matches both the subject (i.e. Client) and the requested Resource. There are multiple ways a subject could be matched, (1) Device UUID, (2) Role Identifier or (3) wildcard. The way in which the Client connects to the Server may be relevant for making access control decisions. Wildcard matching on authenticated vs. unauthenticated and encrypted vs. unencrypted connection allows an access policy to be broadly applied to subject classes.

Example Wildcard Matching Policy:

```
"aclist2": [
{
  "subject": {"conntype" : "anon-clear" },
  "resources":[
    { "wc":"*" }
  ],
  "permission": 31
},
{
  "subject": {"conntype" : "auth-crypt" },
  "resources":[
    { "wc":"*" }
  ],
  "permission": 31
},
]
```

Details of the format for ACL are defined in clause 12. The ACL is composed of one or more ACEs.

Some Resources, such as Collections, generate requests to linked Resources when appropriate Interfaces are used. In such cases, additional access control considerations are necessary. Additional access control considerations for Collections when using the batch OCF Interface are found in clause 12.2.7.3. ACL Resource requires the same security protection as other sensitive Resources when it comes to both storage and handling by the SRM.

5.2.2 ACL architecture

The Server examines the Resource(s) requested by the client before processing the request. The access control Resource is searched to find one or more ACE entries that match the Client and the requested Resources. If a match is found, then permission and period constraints are applied. If more than one match is found, then each ACE entry is evaluated for a match independently.

The Server uses the connection context to determine whether the subject has authenticated or not and whether data confidentiality has been applied or not. If the user has authenticated, then subject matching may happen at increased granularity based on role or device identity.

Each ACE contains the permission set that will be applied for a given Client. Permissions consist of a combination of CREATE, RETREIVE, UPDATE, DELETE and NOTIFY (CRUDN) actions. Clients authenticate as a Device and optionally operating with one or more roles. Devices may acquire elevated access permissions when asserting a role. For example, an "oic.role.owner" role might expose additional Resources and OCF Interfaces not normally accessible.

Servers host ACL Resources locally. Local ACLs allow greater autonomy in access control processing.

The following use cases describe the operation of access control:

Use Case 1: As depicted in Figure 4, Server Device hosts 4 Resources (R1, R2, R3 and R4). Client Device D1 requests access to Resource R1 hosted at Server Device 5. ACL[0] corresponds to Resource R1 and includes D1 as an authorized subject. Thus, Device D1 receives access to Resource R1 because the local ACL "oic/sec/acl2/0" matches the request.

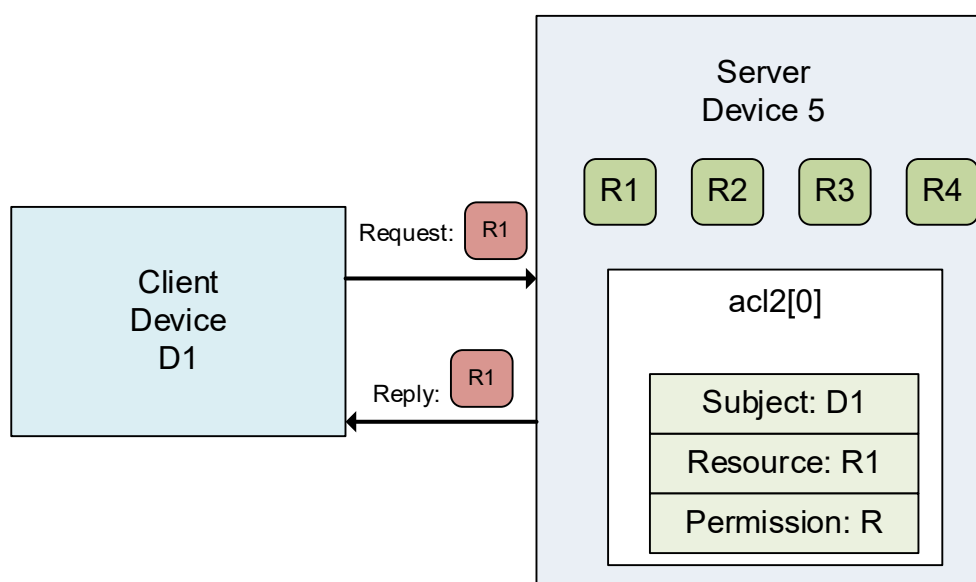


Figure 4 – Use case-1 showing simple ACL enforcement

5.3 Onboarding overview

5.3.1 Onboarding general

Before a Device becomes operational in an OCF environment and is able to interact with other Devices, it needs to be appropriately onboarded. The first step in onboarding a Device is to configure the ownership where the legitimate user that owns/purchases the Device uses an Onboarding tool (OBT) and using the OBT uses one of the Owner Transfer Methods (OTMs) to establish ownership. Once ownership is established, the OBT provisions the Device, at the end of which the Device becomes operational and is able to interact with other Devices in an OCF environment.

Figure 5 depicts an overview of Onboarding.

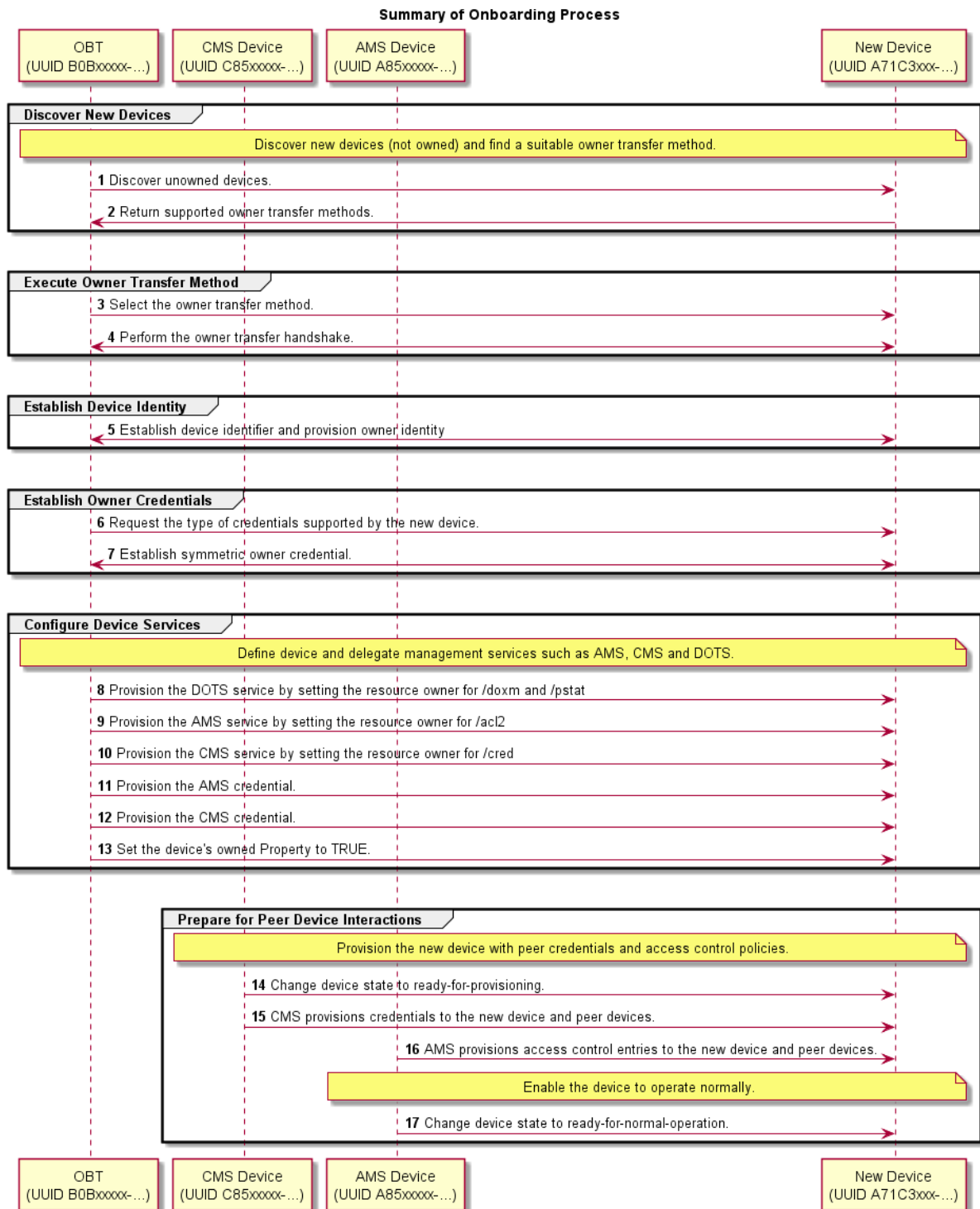


Figure 5 – Onboarding overview

This clause explains the onboarding and security provisioning process but leaves the provisioning of non-security aspects to other OCF documents. In the context of security, all Devices are required to be provisioned with minimal security configuration that allows the Device to securely interact/communicate with other Devices in an OCF environment. This minimal security configuration is defined as the Onboarded Device "Ready for Normal Operation" and is specified in 8.

5.3.2 Onboarding steps

The flowchart in Figure 6 shows the typical steps that are involved during onboarding. Although onboarding may include a variety of non-security related steps, the diagram focus is mainly on the security related configuration to allow a new Device to function within an OCF environment. Onboarding typically begins with the Device becoming an Owned Device followed by configuring the Device for the environment that it will operate in. This would include setting information such as who may access the Device and what actions may be performed as well as what permissions the Device has for interacting with other Devices.

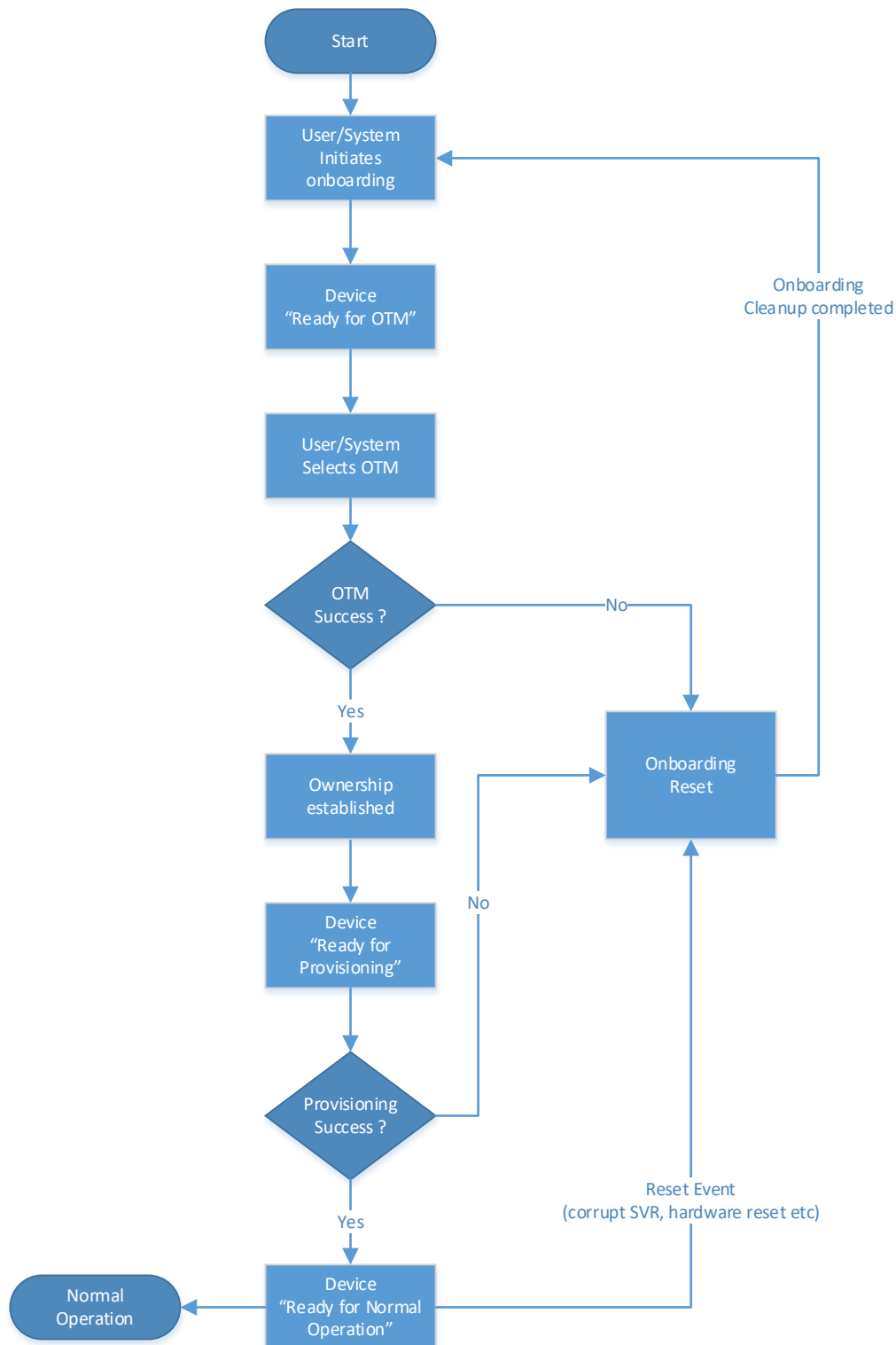


Figure 6 – OCF onboarding process

5.3.3 Establishing a Device Owner

The objective behind establishing Device ownership is to allow the OCF Security Domain Owner to assert itself as the owner and manager of the Device and introduce the Device into the OCF Security Domain. This is done through the use of a DOTS that includes the creation of an ownership context between the new Device and the DOTS and asserts operational control and management of the Device. The DOTS is hosted on an OBT.

The DOTS uses one of the OTMs specified in 7.3 to securely establish Device ownership.

An OTM establishes a new owner (the operator of DOTS) that is authorized to manage the Device. Ownership Transfer accomplishes the following:

- The DOTS provisions an Owner Credential (OC) to the "creds" Property in the "/oic/sec/cred" Resource of the Device. This OC allows the Device and DOTS to mutually authenticate during subsequent interactions. The OC associates the DOTS Device UUID with the "rowneruuid" Property of the "/oic/sec/doxm" Resource establishing it as the Resource owner.
- The Device owner establishes trust in the Device through the OTM.
- Provisioning of appropriate credentials for the Device to be a member of the OCF Security Domain.

5.3.4 Provisioning for Normal Operation

Once the Device has the necessary information to initiate provisioning, the next step is to provision additional security configuration that allows the Device to become operational. This may include setting various parameters and may also involve multiple steps. Also provisioning of ACL's for the various Resources hosted by the Server on the Device is done at this time. The provisioning step is not limited to this stage only. Device provisioning may happen at multiple stages in the Device's operational lifecycle. However specific security related provisioning of Resource and Property state would likely happen at this stage at the end of which, each Device reaches the "Ready for Normal Operation" (RFNOP) State. The RFNOP State is consistent and well defined regardless of the specific OTM used or regardless of the variability in what gets provisioned. However individual OTM mechanisms and provisioning steps may specify additional configuration of Resources and Property states. The minimal mandatory configuration required for a Device to be in RFNOP state is specified in 8.

5.3.5 OCF Compliance Management System

The OCF Compliance Management System (OCMS) is a service maintained by the OCF that provides Certification status and information for OCF Devices.

The OCMS shall provide a JSON-formatted Certified Product List (CPL), hosted at the URI: <https://www.openconnectivity.org/certification/ocms-cpl.json>

The OBT shall possess the Root Certificate needed to enable https connection to the URI <https://www.openconnectivity.org/certification/ocms-cpl.json>.

The OBT should periodically refresh its copy of the CPL via the URI <https://www.openconnectivity.org/certification/ocms-cpl.json>, as appropriate to OCF Security Domain owner policy requirements.

5.4 Provisioning

5.4.1 Provisioning general

OCF security provisioning includes processes during and after the ownership transfer like configuration of credentials for interacting with provisioning services, configuration of any security related Resources and credentials for interacting with any services or Devices that the provisioned Device needs to contact later on.

The Device needs to engage with the CMS and AMS to be provisioned with:

- Security credentials through a CMS, which is currently assumed to be embedded in the same OBT as the DOTS.

- Access control policies and ACLs through an AMS, which is currently assumed to be embedded in the same OBT as the DOTS.

To be able to support the use of distinct device management services, some Device Secure Virtual Resources (SVRs) have an associated Resource owner identified in the Resource's `rowneruuid` Property.

The `"rowneruuid"` Property of the `"/oic/sec/doxm"` and `"/oic/sec/pstat"` Resources identifies the DOTS.

The `"rowneruuid"` Property of the `"/oic/sec/cred"` Resource identifies the CMS.

The `"rowneruuid"` Property of the `"/oic/sec/acl2"` Resource identifies the AMS.

The DOTS provisions credentials that enable secure connections between OCF Services and the new Device. The DOTS initiates client-directed provisioning by signaling the OCF Service.

5.4.2 Access control provisioning

ACL provisioning is performed over a secure connection between the AMS and its Devices. The AMS provisions the ACL by updating the Device's ACL Resource.

5.4.3 Credential provisioning

The CMS securely provisions credentials for Device-to-Device interactions using the CMS credential provisioned by the DOTS during the onboarding procedure. The CMS is also expected to proactively monitor the credentials installed on the Device and update them when needed (e.g. close to the expiration date).

5.4.4 Role provisioning

The Servers, receiving requests for Resources they host, need to verify the role identifier(s) asserted by the Client requesting the Resource and compare that role identifier(s) with the constraints described in the Server's ACLs. Thus, a Client may need to be provisioned with one or more role credentials. Once provisioned, the Client can assert the role it is using as described in 10.4.2, if it has a certificate role credential.

Each Device holds the assertable role(s) information as a Property within the Credential Resource. Each Device holds the asserted role(s) information as Properties within the Roles Resource.

All asserted roles are used in ACL enforcement. When a server has multiple roles asserted for a Client, access to a Resource is granted if it would be granted under any of the roles.

5.5 Secure Resource Manager (SRM)

SRM plays a key role in the overall security operation. In short, SRM performs both management of SVR and access control for requests to access and manipulate Resources. SRM consists of 3 main functional elements:

- A Resource manager (RM): responsible for 1) Loading SVRs from persistent storage (using PSI) as needed. 2) Supplying the Policy Engine (PE) with Resources upon request. 3) Responding to requests for SVRs. While the SVRs are in SRM memory, the SVRs are in a format that is consistent with device-specific data store format. However, the RM will use JSON format to marshal SVR data structures before being passed to PSI for storage, or travel off-device.
- A Policy Engine (PE) that takes requests for access to SVRs and based on access control policies responds to the requests with either `"ACCESS_GRANTED"` or `"ACCESS_DENIED"`. To make the access decisions, the PE consults the appropriate ACL and looks for best Access Control Entry (ACE) that can serve the request given the subject (Device or role) that was authenticated by DTLS.

- Persistent Storage Interface (PSI): PSI provides a set of APIs for the RM to manipulate files in its own memory and storage. The SRM design is modular such that it may be implemented in the Platform's secure execution environment; if available.

Figure 7 depicts OCF's SRM Architecture.

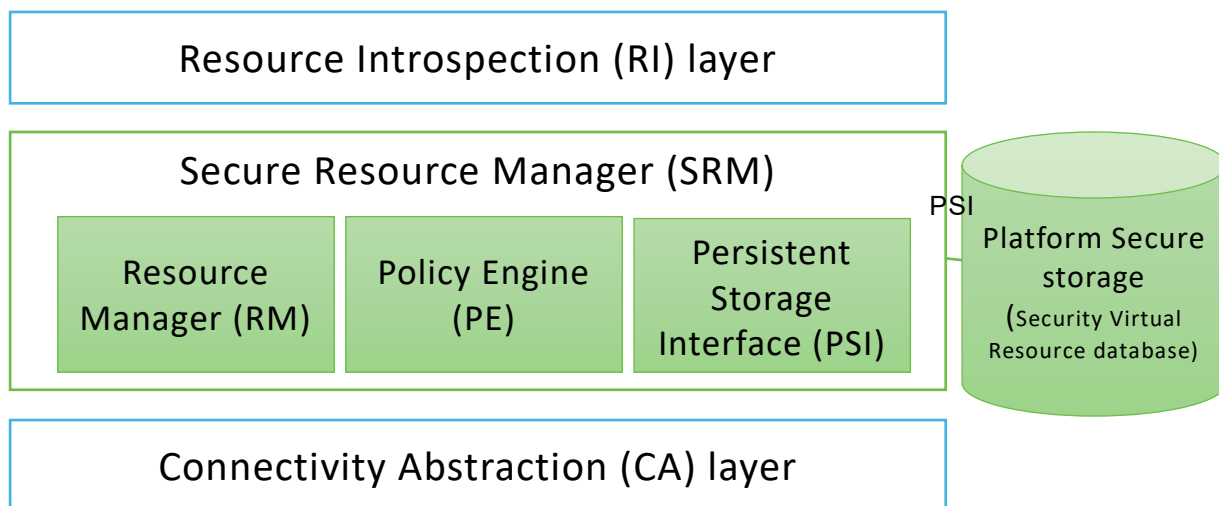


Figure 7 – OCF's SRM architecture

5.6 Credential overview

Devices may use credentials to prove the identity and role(s) of the parties in the Client to Server communication. Credentials may be symmetric or asymmetric. Each Device stores secret and public parts of its own credentials where applicable, as well as credentials for other Devices that have been provisioned by the DOTS or a CMS. These credentials may then be used in the establishment of secure communication sessions (e.g. using DTLS). Role certificates may be used after an authenticated session is established to assert one or more roles for a Device.

The credential types available within this document include:

- Pairwise symmetric keys
- Certificates
- Raw asymmetric keys

Devices may not support all of these credential types. The set of supported credential types for any Device is contained in its "sct" Property of the "/oic/sec/doxm" Resource.

5.7 Event logging

5.7.1 Event logging general

An OCF Platform can generate various kinds of Auditable Events. These Auditable Events can be used for log analysis or for real-time understanding of a system condition. Usually multiple Auditable Events are stored to backtrack problems that have occurred in the system. The storage capacity of IoT devices is typically very limited, so a specific type of data structure such as a ring buffer is often used.

An OCF Device logs Auditable Event Entries (AEE) for all Auditable Events that satisfy the "categoryfilter" and "priorityfilter" Properties of the "/oic/sec/ael" Resource. The AEEs are stored in local storage (see Figure 1). Due to the limited size of the local storage, OCF Security Domain Owner is expected to adjust the filtering options.



Figure 8 – Store Events in local storage

6 Security for the discovery process

6.1 Preamble

The main function of a discovery mechanism is to provide Universal Resource Identifiers (URIs, called links) for the Resources hosted by the Server, complemented by attributes about those Resources and possible further link relations. (in accordance to clause 10 in ISO/IEC 30118-1)

6.2 Security considerations for discovery

When defining discovery process, care must be taken that only a minimum set of Resources are exposed to the discovering entity without violating security of sensitive information or privacy requirements of the application at hand. This includes both data included in the Resources, as well as the corresponding metadata.

To achieve extensibility and scalability, this document does not provide a mandate on discoverability of each individual Resource. Instead, the Server holding the Resource will rely on ACLs for each Resource to determine if the requester (the Client) is authorized to see/handle any of the Resources.

The "/oic/sec/acl2" Resource contains ACL entries governing access to the Server hosted Resources. (See 13.5)

Aside from the privacy and discoverability of Resources from ACL point of view, the discovery process itself needs to be secured. This document sets the following requirements for the discovery process:

- 1) Providing integrity protection for discovered Resources.
- 2) Providing confidentiality protection for discovered Resources that are considered sensitive.

The discovery of Resources is done by doing a RETRIEVE operation (either unicast or multicast) on the known "/oic/res" Resource.

The discovery request is sent over a non-secure channel (multicast or unicast without DTLS), a Server cannot determine the identity of the requester. In such cases, a Server that wants to authenticate the Client before responding can list the secure discovery URI (e.g. coaps://IP:PORT/oic/res) in the unsecured "/oic/res" Resource response. This means the secure discovery URI is by default discoverable by any Client. The Client will then be required to send a separate unicast request using DTLS to the secure discovery URI.

For example, a Client with Device UUID "d1" (UUID:"0685B960-736F-46F7-BEC0-9E6CBD61ADC1") makes a RETRIEVE request on the "/door" Resource hosted on a Server with Device UUID "d3" where d3 has the ACL2s:

```
{
  "aclist2": [
    {
      "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
      "resources": [{"href": "/door"}],
      "permission": 2, // RETRIEVE
      "aceid": 1
    },
    {
      "subject": {"authority": "owner", "role": "owner"}
      "resources": [{"href": "/door"}],
      "permission": 2, // RETRIEVE
      "aceid": 2
    },
    {
      "subject": {"uuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"},
      "resources": [{"href": "/door/lock"}],
      "permission": 4, // UPDATE
      "aceid": 3
    }
  ],
  "rowneruuid": "0685B960-736F-46F7-BEC0-9E6CBD61ADC1"
}
```

The ACL indicates that Client "d1" has RETRIEVE permissions on the Resource. Hence when device "d1" does a discovery on the "/door" Resource of the Server "d3", the response will include all the URIs in the "/door" Resource. Client "d2" without a Role ID "owner" will get an error response that includes no URI.

Discovery results delivered to d1 regarding d3's "/door" Resource from the secure interface:

```
[
  {
    "href": "/door",
    "rel": "self",
    "rt": ["oic.wk.col"],
    "if": ["oic.if.ll", "oic.if.b", "oic.if.baseline"],
    "eps": [{"ep": "coaps://[2001:db8:a::b1d4]:55555}"]
  },
  {
    "href": "/door/lock",
    "rt": ["oic.r.lock.status"],
    "if": ["oic.if.a", "oic.if.baseline"],
    "eps": [{"ep": "coaps://[2001:db8:a::b1d4]:55555}"]
  }
]
```

7 Security provisioning

7.1 Device identity

7.1.1 General Device identity

A Device shall be identified by a Device UUID value that is established as part of the device onboarding and contained in the "deviceuuid" Property of the "/oic/sec/doxm" Resource. Device UUIDs shall be unique within the scope of the corresponding OCF Security Domain, and are expected to be randomly generated and provisioned by the OBT. The DOTS is expected to verify that the chosen new Device UUID does not conflict with Device UUIDs previously introduced into the OCF Security Domain.

Devices maintain an association of their Device UUIDs and their own cryptographic credential(s) via "/oic/sec/cred" Resource. The identity is cryptographically bound in case of a certificate credential, or is bound via internal mappings in the "/oic/sec/cred" Resource otherwise. The "/oic/sec/cred" Resource maintains a list of a Device's own and other Device's credentials. Multiple credentials may be associated with the same Device UUID. A Device is expected to only present credentials associated with its own Device UUID for peer authentication purposes. Devices regard the "/oic/sec/cred" Resource as authoritative when verifying authentication credentials of a peer Device.

In case of an authenticated connection, the Device UUID is treated as a Client's identity for purposes of the Access Control check for the target Resource. The Device UUID of a Client is matched against the Subject UUIDs in the pre-provisioned entries of Server's "/oic/sec/acl2" Resource. The Server determines Client's Device UUID based on the credential used for the establishment of the session.

An OCF Platform, which may host multiple Devices, is identified by a Platform ID. The Platform ID is globally unique and inserted in the device in an integrity protected manner (e.g. inside secure storage or signed and verified).

An OCF Platform may have a secure execution environment, used to secure unique identifiers and secrets. If a Platform hosts multiple Devices, some mechanism is needed to provide each Device with the appropriate and separate security context.

7.1.2 Device identity for devices with UAID [Deprecated]

This clause is intentionally left blank.

7.2 Device ownership

This is an informative clause. Devices are logical entities that are security endpoints that have an identity that is authenticable using cryptographic credentials. A Device is Unowned when it is first initialized. Establishing device ownership is a process by which the device asserts its identity to the DOTS and the DOTS provisions an owner identity. This exchange results in the device changing its ownership state, thereby preventing a different DOTS from asserting administrative control over the device.

The ownership transfer process starts with the OBT discovering a new device that is in Unowned state through examination of the "Owned" Property of the "/oic/sec/doxm" Resource of the new device. At the end of ownership transfer, the following is accomplished:

- 1) The DOTS establishes a secure session with new device.
- 2) Optionally asserts any of the following:
 - a) Proximity (using PIN) of the OBT to the Platform.
 - b) Manufacturer's certificate asserting Platform vendor, model and other Platform specific attributes.

- 3) Determines the device identifier.
- 4) Determines the device owner.
- 5) Specifies the device owner (e.g. Device UUID of the OBT).
- 6) Provisions the device with owner's credentials.
- 7) Sets the "Owned" state of the new device to TRUE.

7.3 Device Ownership Transfer Methods

7.3.1 OTM implementation requirements

This document provides specifications for several methods for ownership transfer. Implementation of each individual ownership transfer method is considered optional. However, each device shall implement at least one of the ownership transfer methods not including vendor specific methods.

All OTMs included in this document are considered optional. Each vendor is required to choose and implement at least one of the OTMs specified in this document. The OCF, does however, anticipate vendor-specific approaches will exist. Should the vendor wish to have interoperability between a vendor-specific OTM and OBTs from other vendors, the vendor must work directly with OBT vendors to ensure interoperability. Notwithstanding, standardization of OTMs is the preferred approach. In such cases, a set of guidelines is provided in 7.3.7 to help vendors in designing vendor-specific OTMs.

The "/oic/sec/doxm" Resource is extensible to accommodate vendor-defined owner transfer methods (OTM). The DOTS determines which OTM is most appropriate to onboard the new Device. All OTMs shall represent the onboarding capabilities of the Device using the "oxms" Property of the "/oic/sec/doxm" Resource. The DOTS queries the Device's supported credential types using the "credtype" Property of the "/oic/sec/cred" Resource. The DOTS and CMS provision credentials according to the credential types supported.

Figure 9 depicts new Device discovery sequence.

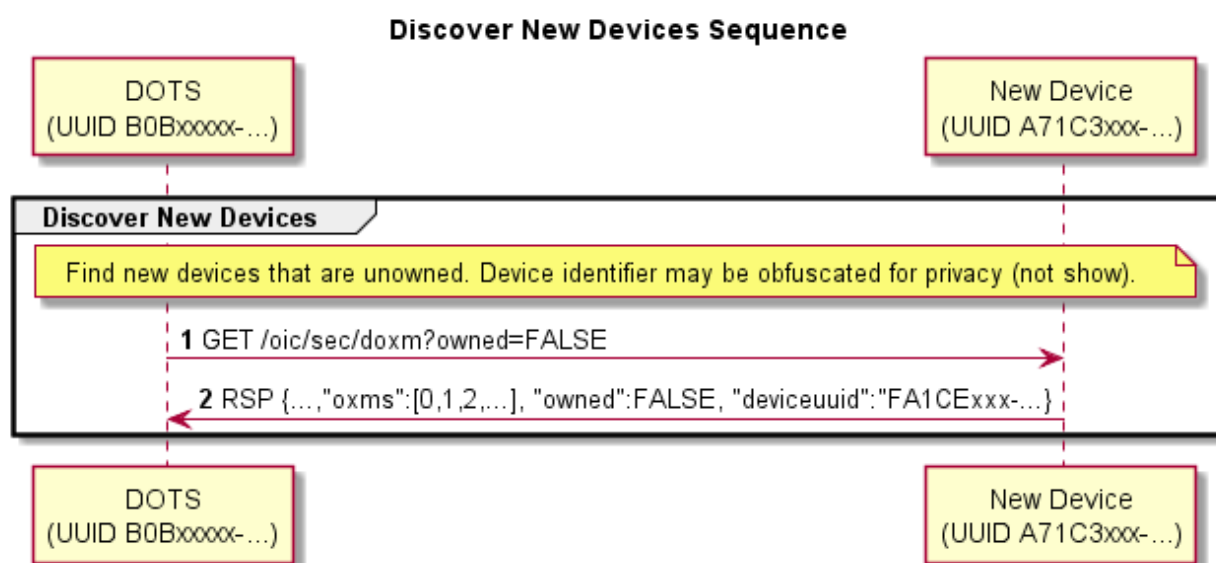


Figure 9 – Discover new Device sequence

Table 1 – Discover new Device details

Step	Description
1	The DOTS queries to see if the new device is not yet owned.
2	The new device returns the "/oic/sec/doxm" Resource containing ownership status and supported OTMs. It also contains a temporal Device UUID that may change subsequent to successful owner transfer. The device should supply a temporal ID to facilitate discovery as a guest device. The OCF Onboarding Tool Specification provides security considerations regarding selecting an OTM.

Vendor-specific device OTMs shall adhere to the "/oic/sec/doxm" Resource Specification for OCs that results from vendor-specific device OTM. Vendor-specific OTM should include provisions for establishing trust in the new Device by the DOTS and optionally establishing trust in the OBT by the new Device.

The new device may have to perform some initialization steps at the beginning of an OTM. For example, if the Random PIN Based OTM is initiated, the new device may generate a random PIN value. The DOTS updates the oxmsel property of "/oic/sec/doxm" to the value corresponding to the OTM being used, before performing other OTM steps. This update notifies the new device that ownership transfer is starting.

The end state of a vendor-specific OTM shall allow the new Device to authenticate to the OBT and the OBT to authenticate to the new device.

Additional provisioning steps may be performed subsequent to owner transfer success leveraging the established OTM session.

7.3.2 SharedKey credential calculation

The SharedKey credential is derived using a PRF that accepts the key_block value resulting from the DTLS handshake used for onboarding. The new Device shall use the following calculation to ensure interoperability across vendor products (the DOTS performs the same calculation):

SharedKey = PRF(Secret, Message);

Where:

- PRF shall use TLS 1.2 PRF defined by IETF RFC 5246 clause 5.
- Secret is the key_block resulting from the DTLS handshake
 - See IETF RFC 5246 clause 6.3
 - The length of key_block depends on cipher suite.
 - (e.g. 96 bytes for TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - 40 bytes for TLS_PSK_WITH_AES_128_CCM_8)
- Message is a concatenation of the following:
 - DoxmType string for the current onboarding method (e.g. "oic.sec.doxm.jw")
 - See clause 13.2.2 for specific DoxmTypes
 - Owner ID is a UUID identifying the device owner identifier and the device that maintains SharedKey.
 - Use raw bytes as specified in IETF RFC 4122 clause 4.1.2
 - Device UUID is new device's UUID
 - Use raw bytes as specified in IETF RFC 4122 clause 4.1.2
- SharedKey Length will be 32 octets.
 - If subsequent DTLS sessions use 128 bit encryption cipher suites the left most 16 octets will be used. DTLS sessions using 256-bit encryption cipher suites will use all 32 octets.

7.3.3 Certificate credential generation

The Certificate Credential will be used by Devices for secure bidirectional communication. The certificates will be issued by a CMS or an external certificate authority (CA). This CA will be used to mutually establish the authenticity of the Device.

7.3.4 Just-Works OTM

7.3.4.1 Just-Works OTM general

Just-works OTM creates a symmetric key credential that is a pre-shared key used to establish a secure connection through which a device should be provisioned for use within the owner's OCF Security Domain. Provisioning additional credentials and Resources is a typical step following ownership establishment. The pre-shared key is called SharedKey.

The DOTS selects the Just-works OTM using the "oxmsel" Property of the "/oic/sec/doxm" Resource and establishes a DTLS session using a cipher suite defined for the Just-works OTM.

Just Works OTM sequence is shown in Figure 10 and steps described in Table 2.

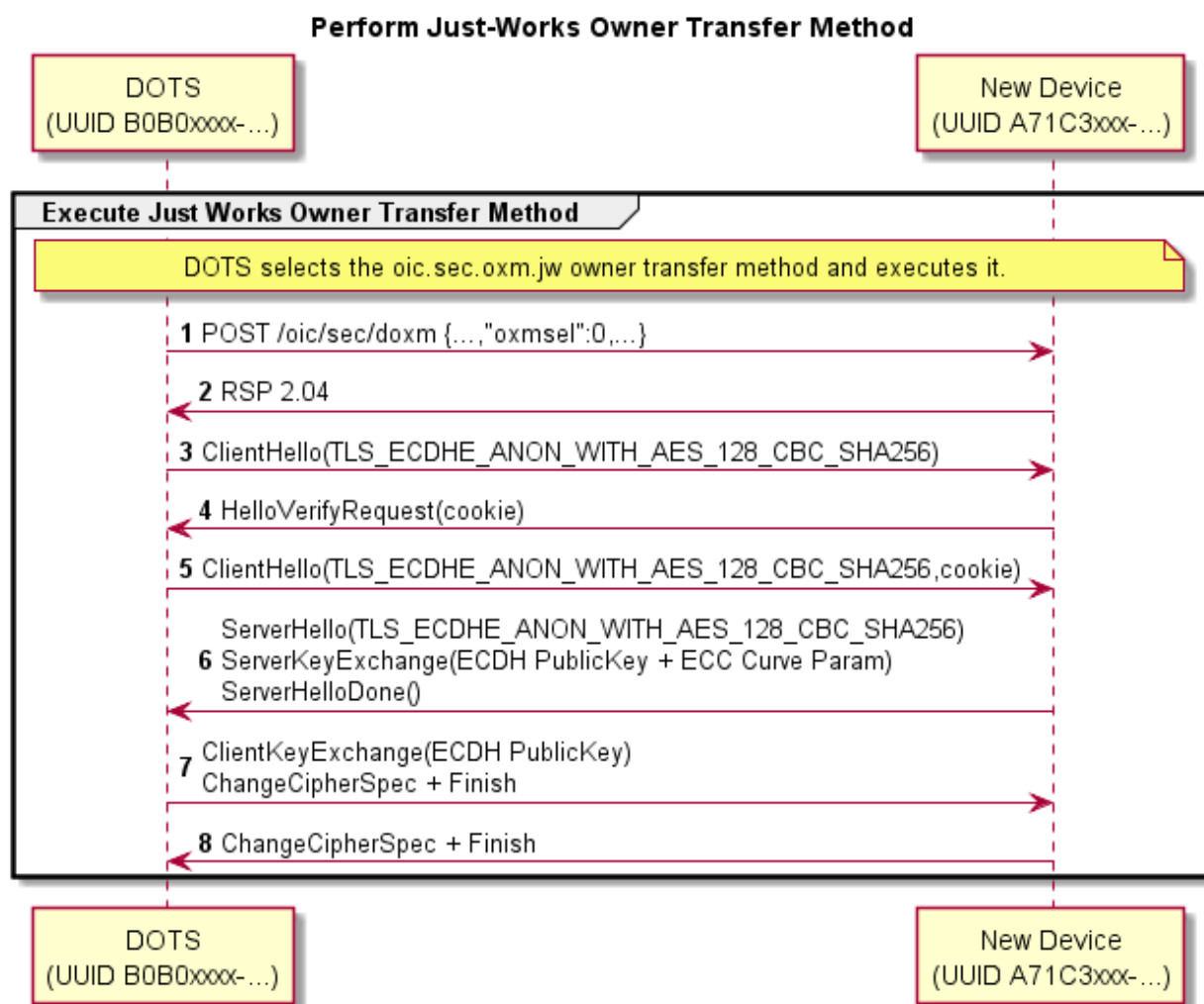


Figure 10 – A Just Works OTM

Table 2 – A Just Works OTM details

Step	Description
1, 2	The DOTS notifies the Device that it selected the "Just Works" method.
3 – 8	A DTLS session is established using anonymous Diffie-Hellman. ^a
^a This method assumes the operator is aware of the potential for man-in-the-middle attack and has taken precautions to perform the method in a clean-room network.	

7.3.4.2 Security considerations

Anonymous Diffie-Hellman key agreement is subject to a man-in-the-middle attacker. Use of this method presumes that both the DOTS and the new device perform the "just-works" method assumes onboarding happens in a relatively safe environment absent of an attack device.

This method doesn't have a trustworthy way to prove the Device UUID asserted is reliably bound to the device.

The new device should use a temporal Device UUID prior to transitioning to an owned device while it is considered a guest device to prevent privacy sensitive tracking. The device asserts a non-temporal Device UUID that could differ from the temporal value during the secure session in which owner transfer exchange takes place. The DOTS verifies the asserted Device UUID does not conflict with a Device UUID already in use. If it is already in use the existing credentials are used to establish a secure session.

An un-owned Device that also has established device credentials might be an indication of a corrupted or compromised device.

7.3.5 Random PIN based OTM

7.3.5.1 Random PIN based OTM general

The Random PIN method establishes physical proximity between the new device and the OBT can prevent man-in-the-middle attacks. The Device generates a random number that is communicated to the DOTS over an Out of Band Communication Channel. The definition of an Out of Band Communication Channel is outside the scope of the definition of device OTMs. The DOTS and new Device use the PIN in a key exchange as evidence that an End User authorized the transfer of ownership by having physical access to the new Device via the Out-of-Band Communication Channel.

7.3.5.2 Random PIN based Owner Transfer sequence

Random PIN-based OTM sequence is shown in Figure 11 and steps described in Table 3.

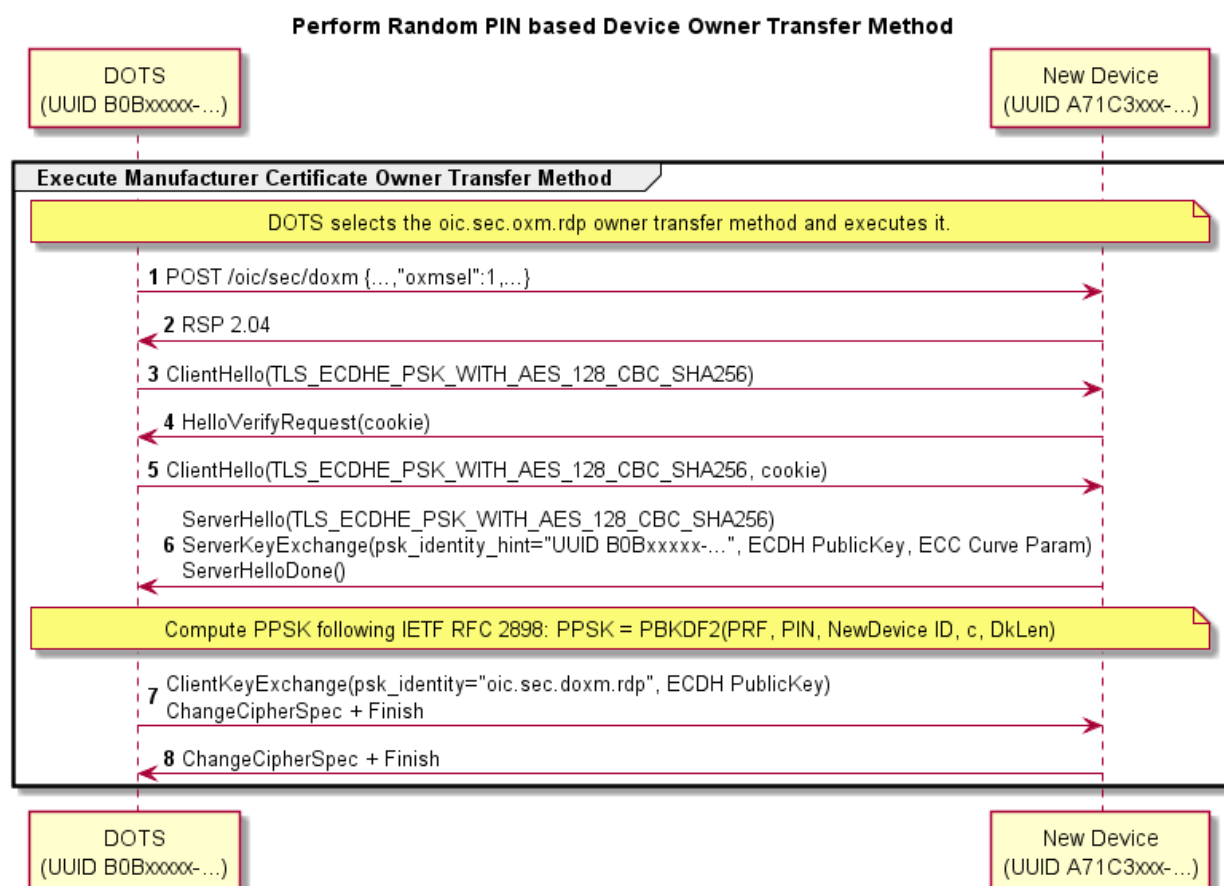


Figure 11 – Random PIN-based OTM

Table 3 – Random PIN-based OTM details

Step	Description
1, 2	The DOTS notifies the Device that it selected the "Random PIN" method.
3 - 8	A DTLS session is established using PSK-based Diffie-Hellman cipher suite. The PIN is supplied as the PSK parameter. The PIN is randomly generated by the new device then communicated via an Out of Band Communication Channel that establishes proximal context between the new device and the DOTS. The security principle is the attack device will be unable to intercept the PIN due to a lack of proximity.

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

- The new Device shall set the "psk_identity_hint" field of the ServerKeyExchange message to 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 new Device determines that the Random PIN-based OTM is being applied if that the "psk_identity" field of the ClientKeyExchange message matches the string "oic.sec.doxm.rdp". If the Random PIN-based OTM is being applied, then the new Device shall apply the key derivation below.

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

This OTM uses a pseudo-random function (PBKDF2) defined by IETF RFC 2898 and a PIN exchanged via an Out of Band Communication Channel to generate a pre-shared key. The PIN-authenticated pre-shared key (PPSK) is supplied to TLS cipher suites that accept a PSK.

- PPSK = PBKDF2(PRF, PIN, Device UUID, c, dkLen)

The PBKDF2 function has the following parameters:

- PRF – Uses the TLS 1.2 PRF defined by IETF RFC 5246.
- PIN – obtained via Out of Band Communication Channel.
- Device UUID – 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.

Use raw bytes as specified in IETF RFC 4122 clause 4.1.2

- c – Iteration count initialized to 1000
- dkLen – Desired length of the derived PSK in octets.

7.3.5.3 Security considerations

Security of the Random PIN mechanism depends on the entropy of the PIN. Using a PIN with insufficient entropy may allow a man-in-the-middle attack to recover any long-term credentials provisioned as a part of onboarding. In particular, learning the provisioned symmetric key credentials allows an attacker to masquerade as the onboarded device.

It is recommended that the entropy of the PIN be enough to withstand an online brute-force attack, 40 bits or more. For example, a 12-digit numeric PIN, or an 8-character alphanumeric (0-9a-z), or a 7-character case-sensitive alphanumeric PIN (0-9a-zA-Z). A man-in-the-middle attack (MITM) is when the attacker is active on the network and can intercept and modify messages between the DOTS and device. In the MITM attack, the attacker must recover the PIN from the key exchange messages in "real time", i.e., before the peer's time out and abort the connection attempt. Having recovered the PIN, he can complete the authentication step of key exchange. The guidance given here calls for a minimum of 40 bits of entropy, however, the assurance this provides depends on the resources available to the attacker. Given the parallelizable nature of a brute force guessing attack, the attack enjoys a linear speedup as more cores/threads are added. A more conservative amount of entropy would be 64 bits. Since the Random PIN OTM requires using a DTLS cipher suite that includes an ECDHE key exchange, the security of the Random PIN OTM is always at least equivalent to the security of the JustWorks OTM.

The Random PIN OTM also has an option to use PBKDF2 to derive key material from the PIN. The rationale is to increase the cost of a brute force attack, by increasing the cost of each guess in the attack by a tuneable amount (the number of PBKDF2 iterations). In theory, this is an effective way to reduce the entropy requirement of the PIN. Unfortunately, it is difficult to quantify the reduction, since an X-fold increase in time spent by the honest peers does not directly translate to an X-fold increase in time by the attacker. This asymmetry is because the attacker may use specialized implementations and hardware not available to honest peers. For this reason, when deciding how much entropy to use for a PIN, it is recommended that implementers assume PBKDF2 provides no security, and ensure the PIN has sufficient entropy.

The Random PIN device OTM security depends on an assumption that a secure Out of Band Communication Channel for communicating a randomly generated PIN from the new device to the OBT exists. If the Out of Band Communication Channel leaks some or the entire PIN to an attacker, this

reduces the entropy of the PIN, and the attacks described above apply. The Out of Band Communication Channel should be chosen such that it requires proximity between the DOTS and the new device. The attacker is assumed to not have compromised the Out of Band Communication Channel. As an example Out of Band Communication Channel, the device may display a PIN to be entered into the OBT software. Another example is for the device to encode the PIN as a 2D barcode and display it for a camera on the DOTS device to capture and decode.

7.3.6 Manufacturer Certificate Based OTM

7.3.6.1 Manufacturer Certificate Based OTM general

The manufacturer certificate-based OTM shall use a certificate embedded into the device by the manufacturer and may use a signed OBT, which determines the Trust Anchor between the device and the DOTS.

Manufacturer embedded certificates do not necessarily need to chain to an OCF Root CA trust anchor.

For some environments, policies or administrators, additional information about device characteristics may be sought. This list of additional attestations that OCF may or may not have tested (understanding that some attestations are incapable of testing or for which testing may be infeasible or economically unviable) can be found under the OCF Security Claims x509.v3 extension described in 9.4.2.2.6.

When utilizing certificate-based ownership transfer, devices shall utilize asymmetric keys with certificate data to authenticate their identities with the DOTS in the process of bringing a new device into operation on an OCF Security Domain. The onboarding process involves several discrete steps:

- 1) Pre-on-board conditions
 - a) The credential element of the Device's credential Resource ("/oic/sec/cred") containing the manufacturer certificate shall be identified by the "credusage" Property containing the string "oic.sec.cred.mfgcert" to indicate that the credential contains a manufacturer certificate.
 - b) The manufacturer certificate chain shall be contained in the identified credential element's "publicdata" Property.
 - c) The device shall contain a unique and immutable ECC asymmetric key pair.
 - d) If the device requires authentication of the DOTS as part of ownership transfer, it is presumed that the DOTS has been registered and has obtained a certificate for its unique and immutable ECC asymmetric key pair signed by the predetermined Trust Anchor.
 - e) An End User has configured the DOTS app with network access info and account info (if any).
- 2) The DOTS authenticates the Device using ECDSA to verify the signature. Additionally, the Device may authenticate the DOTS to verify the DOTS signature.
- 3) If authentication fails, the Device shall indicate the reason for failure and return to the Ready for OTM state. If authentication succeeds, the Device shall establish an encrypted link with the DOTS in accordance with the negotiated cipher suite.

7.3.6.2 Certificate Profiles

See 9.4.2 for details.

7.3.6.3 Certificate Owner Transfer sequence security considerations

The OBT shall authenticate the device during onboarding. The device will not authenticate the OBT. During the DTLS handshake the server shall not send a Certificate Request.

7.3.6.4 Manufacturer Certificate Based OTM sequence

Manufacturer Certificate Based OTM sequence is shown in Figure 12 and steps described in Table 4.

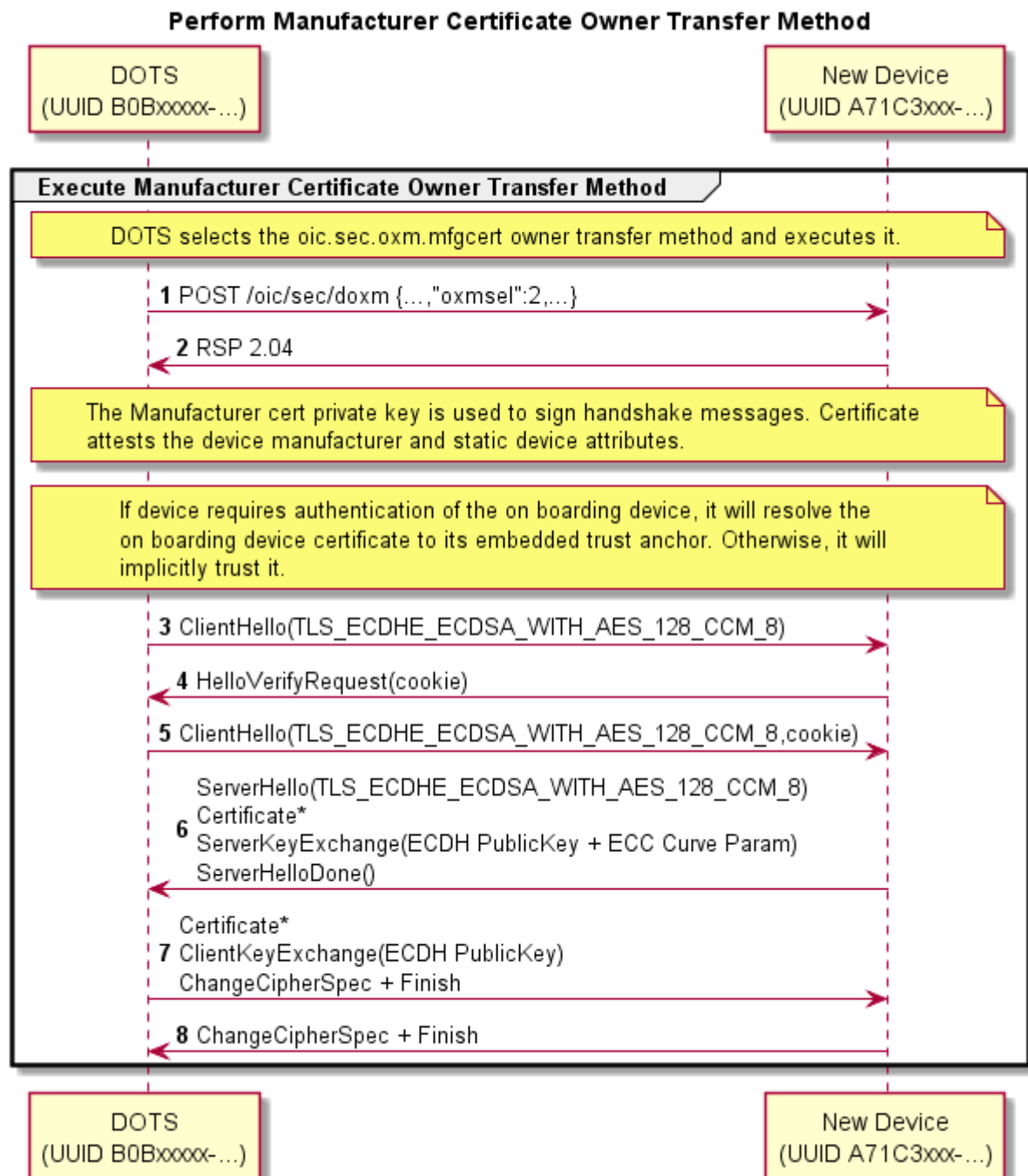


Table 4 – Manufacturer Certificate Based OTM Details

Step	Description
1, 2	The DOTS notifies the Device that it selected the "Manufacturer Certificate" method.
3 - 8	A DTLS session is established using the device's manufacturer certificate and optional DOTS certificate. The device's manufacturer certificate may contain data attesting to the Device hardening and security properties.

7.3.6.5 Security considerations

The manufacturer certificate private key is embedded in the Platform with a sufficient degree of assurance that the private key cannot be compromised.

The Platform manufacturer issues the manufacturer certificate and attests the private key protection mechanism.

7.3.7 Vendor specific OTMs

7.3.7.1 Vendor specific OTM general

The OCF anticipates situations where a vendor will need to implement an OTM that accommodates manufacturing or Device constraints. The Device OTM Resource is extensible for this purpose. Vendor-specific OTMs must adhere to a set of conventions that all OTMs follow.

- The OBT must determine which credential types are supported by the Device. This is accomplished by querying the Device's "/oic/sec/doxm" Resource to identify supported credential types.
- The OBT provisions the Device with OC(s).
- The OBT supplies the Device UUID and credentials for subsequent access to the OBT.
- The OBT will supply second carrier settings sufficient for accessing the owner's OCF Security Domain subsequent to ownership establishment.
- The OBT may perform additional provisioning steps but must not invalidate provisioning tasks to be performed by a security service.

7.3.7.2 Vendor-specific Owner Transfer Sequence Example

Vendor-specific OTM sequence example is shown in Figure 13 and steps described in Table 5.

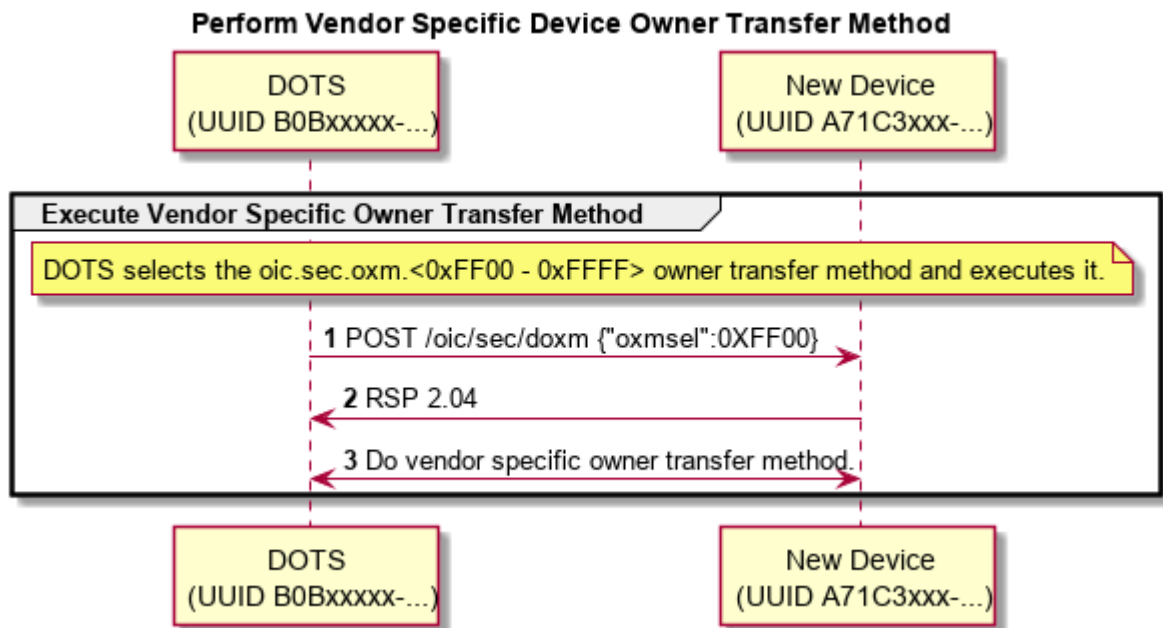


Figure 13 – Vendor-specific Owner Transfer sequence

Table 5 – Vendor-specific Owner Transfer details

Step	Description
1, 2	The DOTS selects a vendor-specific OTM.
3	The vendor-specific OTM is applied

7.3.7.3 Security considerations

The vendor is responsible for considering security threats and mitigation strategies.

7.3.8 Establishing Owner Credentials

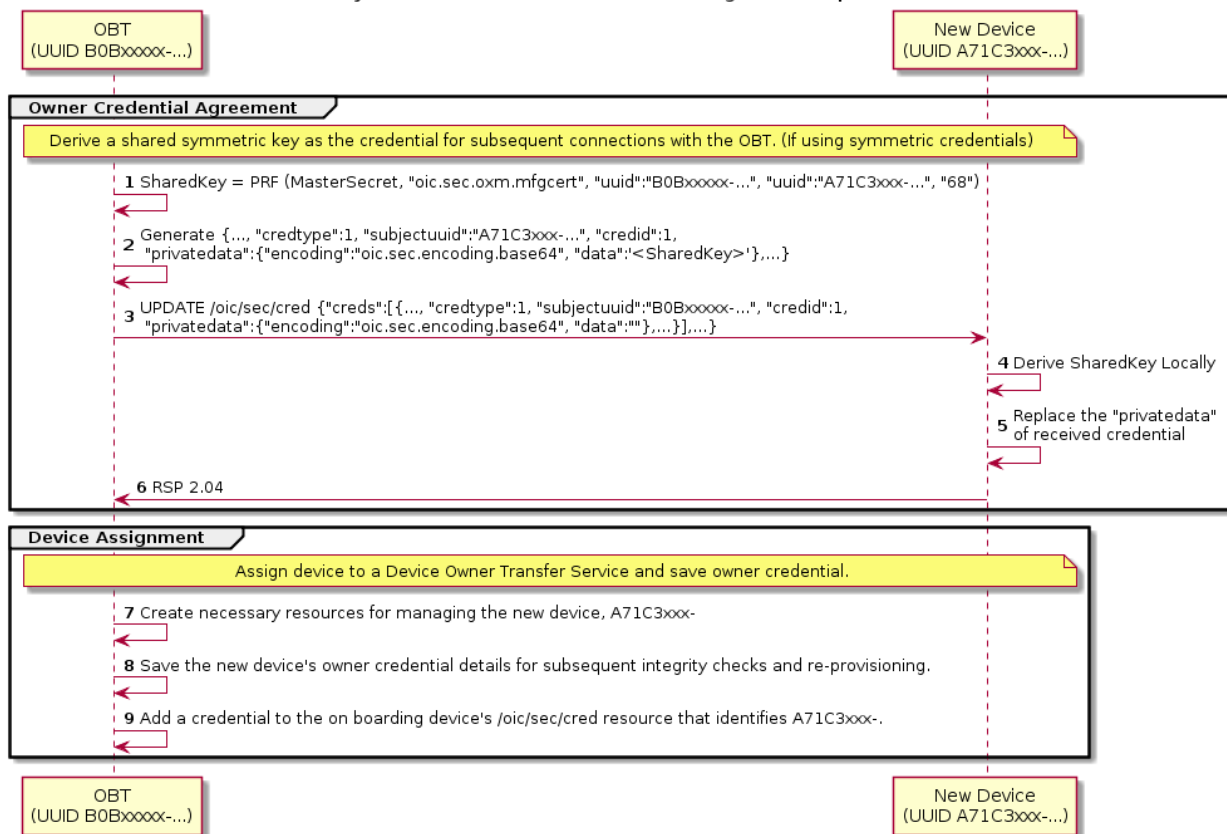
Once the OBT and the new Device have authenticated and established an encrypted connection using one of the defined OTM methods, the Owner Credential(s) can be provisioned.

The Owner Credential is provisioned as part of Ownership Transfer Method, and may be provisioned directly by CMS.

The steps for establishing Device's owner credentials (OC) as part of OTM are:

- 1) The OBT establishes the Device UUID and Device Owner Id.
- 2) The OBT then establishes Device's symmetric OC - See Figure 14 and Table 6.
- 3) Configure Device services.
- 4) Configure Device for peer to peer interaction.

Symmetric Owner Credential (OC) Assignment Sequence



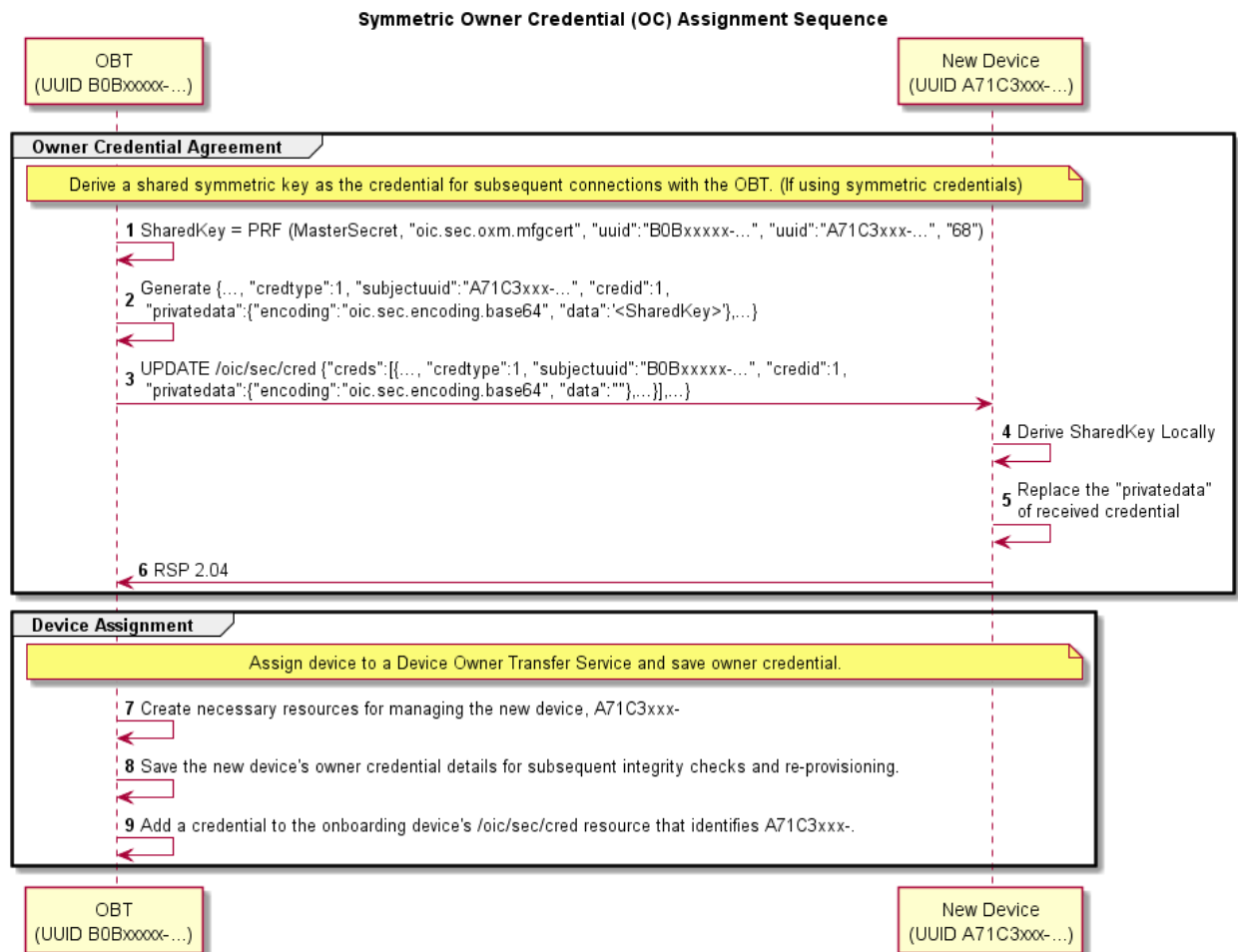


Figure 14 – Symmetric Owner Credential provisioning sequence

Table 6 – Symmetric Owner Credential assignment details

Step	Description
1, 2	The OBT uses a pseudo-random-function (PRF), the master secret resulting from the DTLS handshake, and other information to generate a symmetric key credential Resource Property - SharedKey.
3	The OBT creates a credential Resource Property set based on SharedKey and then sends the Resource Property set to the new Device with empty "privatedata" Property value.
4, 5	The new Device locally generates the SharedKey and updates it to the "privatedata" Property of the credential Resource Property set.
6	The new Device sends a success message.
7	The onboarding service creates a subjects Resource for the new device (e.g./A71C3xxx-...)
8	The onboarding service provisions its "/oic/svc/dots/subjects/A71C3xxx-/cred" Resource with the owner credential. Credential type is SYMMETRIC KEY.
9	(optional) The onboarding service provisions its own "/oic/sec/cred" Resource with the owner credential for new device. Credential type is SYMMETRIC KEY.

In particular when OBT establishes symmetric owner credentials as part of OTM sequence:

- The OBT generates a Shared Key using the SharedKey Credential Calculation method described in 7.3.2.
- The OBT sends an empty key to the new Device's `"/oic/sec/cred"` Resource, identified as a symmetric pair-wise key. The Subject UUID of the `"/oic/sec/cred"` entry shall match the Device UUID of the OBT.
- Upon receipt of the OBT's symmetric owner credential, the new Device shall independently generate the Shared Key using the SharedKey Credential Calculation method described in 7.3.2 and store it with the owner credential.
- The new Device shall use the Shared Key owner credential(s) stored via the `"/oic/sec/cred"` Resource to authenticate the owner during subsequent connections.

7.3.9 Security profile assignment

OCF Devices may have been evaluated according to an OCF Security Profile. Evaluation results could be accessed from a manufacturer's certificate, OCF web server or other public repository. The DOTS reviews evaluation results to determine which OCF Security Profiles the OCF Device is authorized to possess and configures the Device with the subset of evaluated security profiles best suited for the OCF Security Domain owner's intended segmentation strategy.

The OCF Device vendor shall set a manufacturer default value for the `"supportedprofiles"` Property of the `"/oic/sec/sp"` Resource to match those approved by OCF's testing and certification process. The `"currentprofile"` Property of the `"/oic/sec/sp"` Resource shall be set to one of the values contained in the `"supportedprofiles"`. The manufacturer default value shall be re-asserted when the Device transitions to RESET Device State.

The OCF Device shall only allow the `"/oic/sec/sp"` Resource to be updated when the Device is in one of the following Device States: RFOTM, RFPRO, SRESET and may not allow any update as directed by a Security Profile.

The DOTS may update the `"supportedprofiles"` Property of the `"/oic/sec/sp"` Resource with a subset of the OCF Security Profiles values the Device achieved as part of OCF Conformance testing. The DOTS may locate conformance results by inspecting manufacturer certificates supplied with the OCF Device by selecting the `"credusage"` Property of the `"/oic/sec/cred"` Resource having the value of `"oic.sec.cred.mfgcert"`. The DOTS may further locate conformance results by visiting a well-known OCF web site URI corresponding to the `ocfCPLAttributes` extension fields (clause 9.4.2.2.7). The DOTS may select a subset of Security Profiles (from those evaluated by OCF conformance testing) based on a local policy.

As part of onboarding (while the OTM session is active) the DOTS should configure ACE entries to allow DOTS access subsequent to onboarding.

The DOTS should update the `"currentprofile"` Property of the `"/oic/sec/sp"` Resource with the value that most correctly depicts the OCF Security Domain owner's intended Device deployment strategy.

The CMS may issue role credentials using the Security Profile value (e.g. the `"sp-blue-v0 OID"`) to indicate the OCF Security Domain owner's intention to segment the OCF Security Domain according to a Security Profile. The CMS retrieves the `supportedprofiles` Property of the `"/oic/sec/sp"` Resource to select role names corroborated with the Device's supported Security Profiles when issuing role credentials.

If the CMS issues role credentials based on a Security Profile, the AMS supplies access control entries that include the role designation(s).

7.4 Provisioning

7.4.1 Provisioning flows

7.4.1.1 Provisioning flows general

As part of onboarding a new Device a secure channel is formed between the new Device and the OBT. Subsequent to the Device ownership status being changed to "owned", there is an opportunity to begin provisioning. The OBT provisions the support services that should be subsequently used to complete Device provisioning and on-going Device management.

The Device employs a Client-directed provisioning strategy. The "/oic/sec/pstat" Resource identifies the provisioning strategy and current provisioning status. The provisioning service should determine which provisioning strategy is most appropriate for the OCF Security Domain. See 13.8 for additional detail.

7.4.1.2 Client-directed provisioning

Client-directed provisioning relies on a provisioning service that identifies Servers in need of provisioning then performs all necessary provisioning duties.

An example of Client-directed provisioning is shown in Figure 15 and steps described in Table 7.

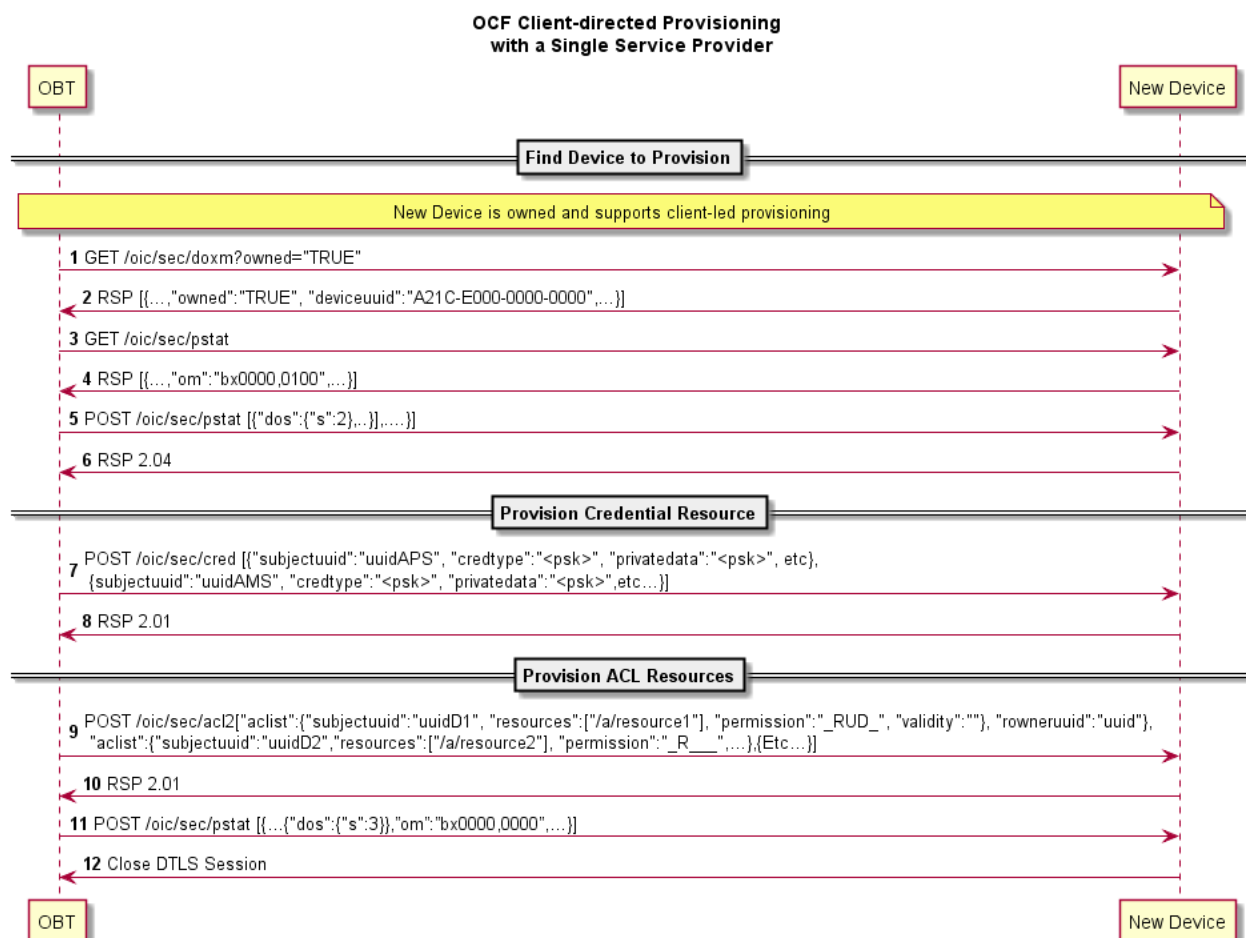


Figure 15 – Example of Client-directed provisioning

Table 7 – Steps describing Client -directed provisioning

Step	Description
1	Discover Devices that are owned and support Client-directed provisioning.
2	The "/oic/sec/doxm" Resource identifies the Device and it's owned status.
3	DOTS (on OBT) obtains the new Device's provisioning status found in "/oic/sec/pstat" Resource
4	The "pstat" Resource describes the types of provisioning modes supported and which is currently configured. A Device manufacturer should set a default current operational mode ("om"). If the "om" isn't configured for Client-directed provisioning, its "om" value can be changed.
5 – 6	Change Device state to Ready-for-Provisioning.
7 – 8	CMS (on OBT) instantiates the "/oic/sec/cred" Resource. It contains credentials for the provisioned services and other Devices
9 - 10	AMS (on OBT) instantiates "/oic/sec/acl2" Resource.
11	The new Device provisioning status mode is updated to reflect that ACLs have been configured. (Ready-for-Normal-Operation state)
12	The secure session is closed.

7.4.1.3 Server-directed provisioning [DEPRECATED]

This clause is intentionally left blank.

7.4.1.4 Server-directed provisioning involving multiple support services [DEPRECATED]

This clause is intentionally left blank.

8 Device Onboarding state definitions

8.1 Device Onboarding general

As explained in 5.3, the process of onboarding completes after the ownership of the Device has been transferred and the Device has been provisioned with relevant configuration/services as explained in 5.4. The Figure 16 shows the various states a Device can be in during the Device lifecycle. Device shall reject any requests to perform a state transition not shown on Figure 16.

The "/pstat.dos.s" Property is RW by the "/oic/sec/pstat" Resource owner (e.g. "doxs" service) so that the Resource owner can remotely update the Device state. When the Device is in RFNOP or RFPRO, ACLs can be used to allow remote control of Device state by other Devices. When the Device state is SRESET the Device OC may be the only indication of authorization to access the Device. The Device owner may perform low-level consistency checks and re-provisioning to get the Device suitable for a transition to RFPRO.