OCF "Essen" – Remove_normative_OBT_requirements_from_ OCF_Sec_Spec – Security WG CR 2919

Legal Disclaimer

1 Scope

2 Normative References

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

<Add/change the following definitions>

3.1.1
OCF Onboarding
initial establishment of ownership over a Device, and initial provisioning of the Device for normal operation

3.1.2
Out-of-Band Communication Channel
any mechanism for delivery of a secret from one party to another, not specified by OCF

3.2 Abbreviated terms

<Remote the following abbreviation>

4 Document Conventions and Organization

5 Security Overview

5.1 Preamble

5.2 Access Control

5.2.1 ACL Architecture

5.2.1.1 ACL Architecture General

5.2.1.2 Use of local ACLs

5.2.1.3 Use of AMS

AMS improves ACL policy management. However, they can become a central point of failure. Due to network latency overhead, ACL processing may be slower through an AMS.

AMS centralizes access control decisions, but Server Devices retain enforcement duties. The AMS is authenticated by referencing a credential issued to the device identifier contained in "/oic/sec/acl2.rowneruuid".

5.2.2 Access Control Scoping Levels

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 becomes the mechanism through which the Device can then be provisioned, at the end of which the Device becomes operational and is able to interact with other Devices in an OCF environment.

<No changes after this point in this clause>

5.3.2 Onboarding Steps

5.3.3 Establishing a Device Owner

The objective behind establishing Device ownership is to allow the legitimate user that owns/purchased the Device to assert itself as the owner and manager of the Device. This is done through the use of an 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 (see [OBTSpec]).

The DOTS uses one of the OTMs specified in 7.3 to securely establish Device ownership. The term owner transfer is used since it is assumed that even for a new Device, the ownership is transferred from the manufacturer/provider of the Device to the buyer/legitimate user of the new Device.

An OTM establishes a new owner (the operator of DOTS) that is authorized to manage the Device. Owner transfer establishes the following

<No changes after this point in this clause>

5.3.4 Provisioning for Normal Operation

5.3.5 Device Provisioning for OCF Cloud and Device Registration Overview

5.3.6 OCF Compliance Management System

5.4 Provisioning

5.4.1 Provisioning General

<No changes prior to this point in this clause>

<No changes after this point in this clause>

5.4.2 Provisioning other services

To be able to support the use of potentially different device management service hosts, each Device Secure Virtual Resource (SVR) has 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 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.

5.4.3 Provisioning Credentials for Normal Operation

<No changes prior to this point in this clause>

The CMS securely provisions credentials for Device-to-Device interactions using the CMS credential provisioned by the DOTS.

The following example describes how a Device updates a symmetric key credential involving a peer Device. The Device discovers the credential to be updated; for example, a secure connection attempt fails. The CMS returns an updated symmetric key credential. The CMS updates the corresponding symmetric key credential on the peer Device.

5.4.4 Role Assignment and Provisioning for Normal Operation

5.4.5 ACL 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.

5.5 Secure Resource Manager (SRM)

6 Security for the Discovery Process

7 Security Provisioning

7.1 Device Identity

7.2 Device Ownership

<No changes prior to this point in this clause>

1) The DOTS establishes a secure session with new device.

<No changes after this point in this clause>

7.3 Device Ownership Transfer Methods

7.3.1 OTM implementation requirements

<No changes prior to this point in this clause>

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 13 depicts new Device discovery sequence.

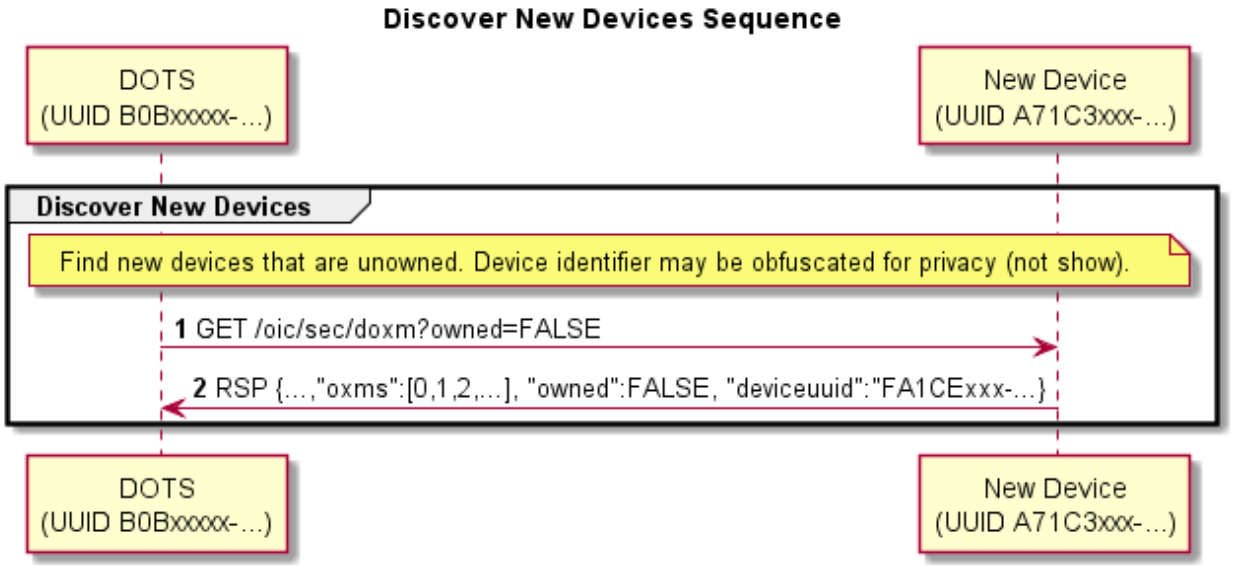


Figure 1 – Discover New Device Sequence

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 ID that may change subsequent to successful owner transfer. The device should supply a temporal ID to facilitate discovery as a guest device. Clause 7.3.9 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):

<No changes after this point in this clause>

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

<No changes prior to this point in this clause>

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

<Some text and/or figures not shown>

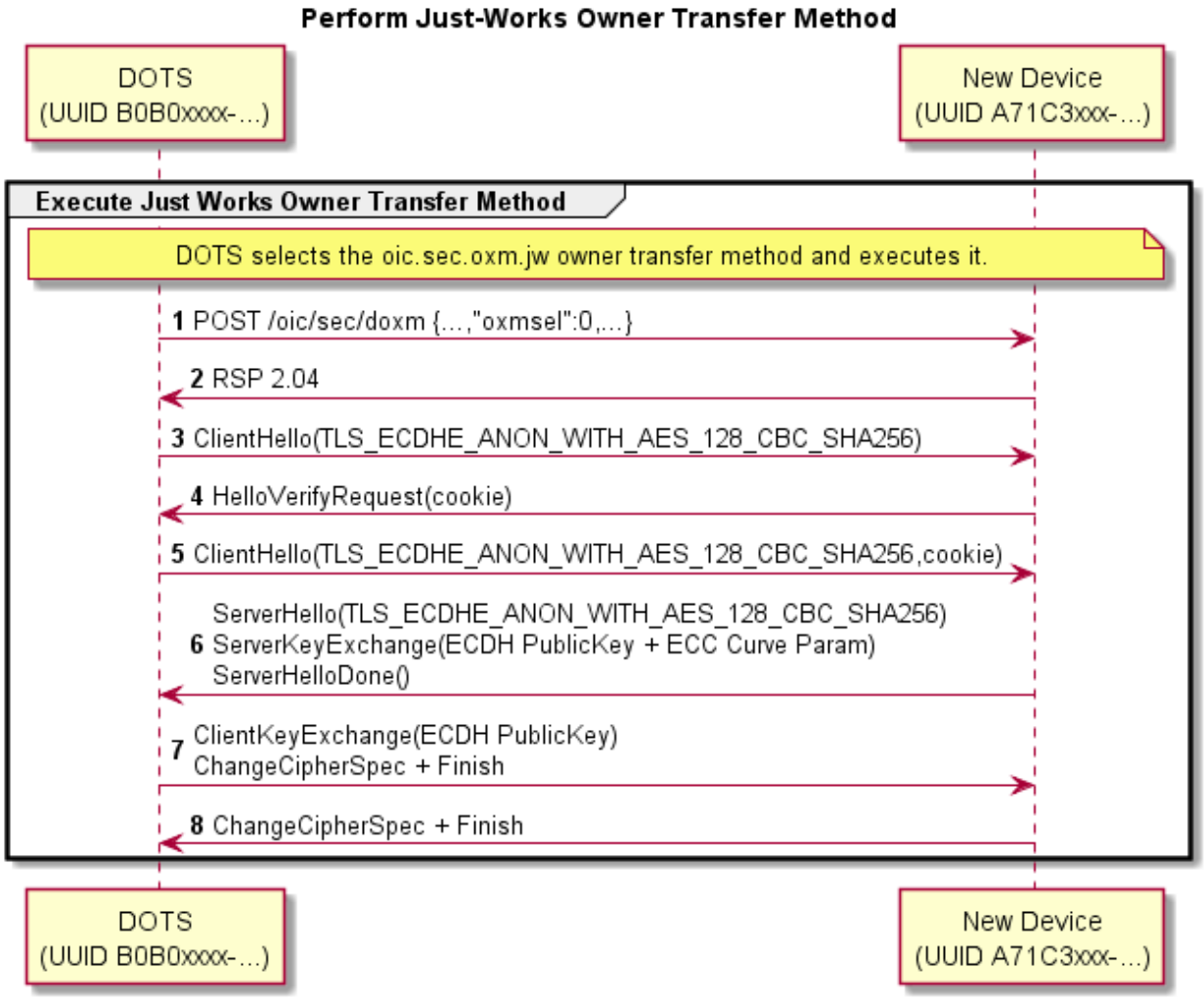


Figure 2 – A Just Works OTM

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.

<Some text and/or figures not shown>

The DOTS verifies the asserted Device ID does not conflict with a Device ID 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 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 someone authorized the transfer of ownership by having physical access to the new Device via the Out-of-Band CommunicationChannel.

7.3.5.2 Random PIN Owner Transfer Sequence

Random PIN-based OTM sequence is shown in Figure 15 and steps described in Table 3.

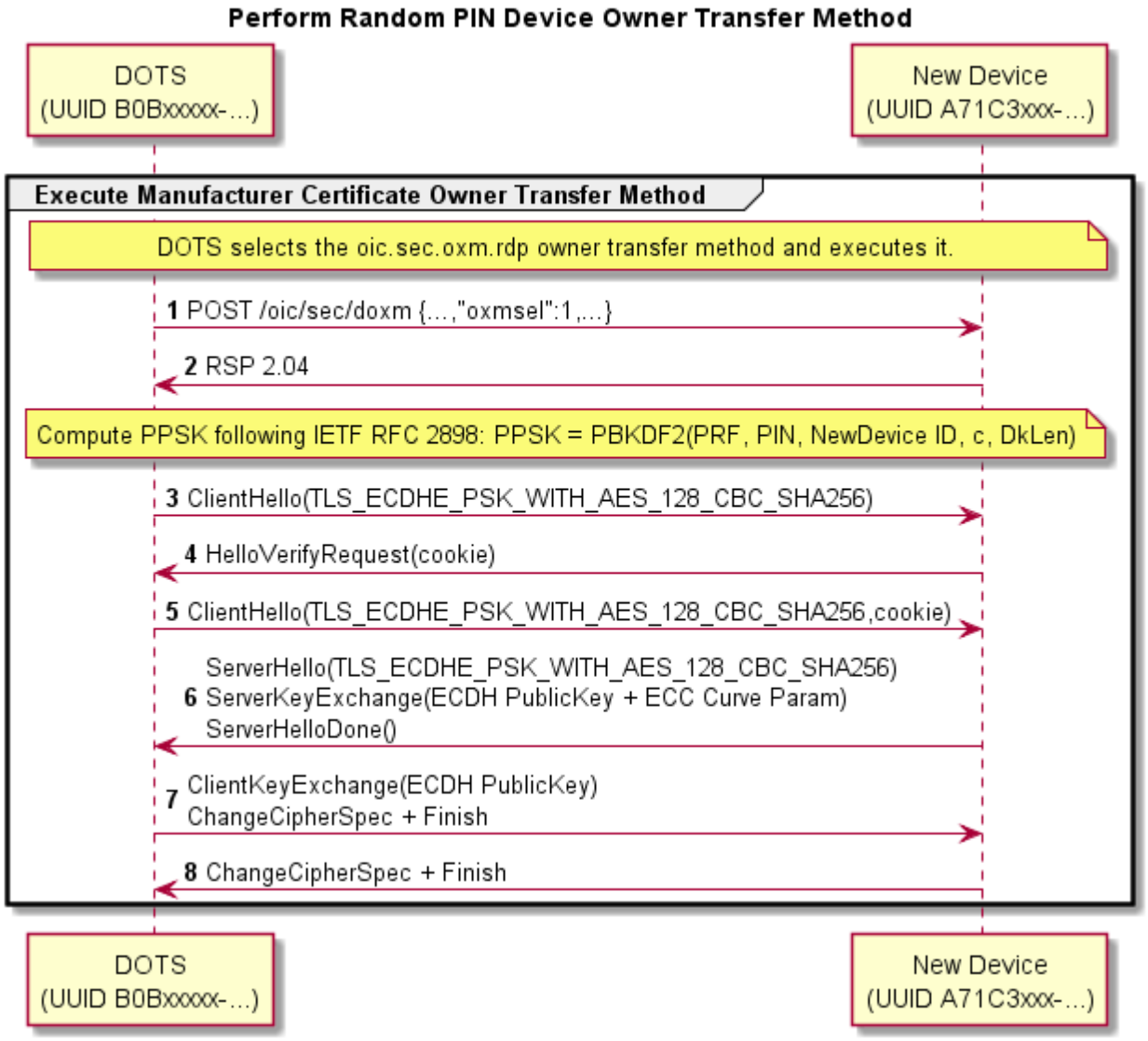


Figure 3 – Random PIN-based OTM

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

PPSK = PBKDF2(PRF, PIN, Device ID, 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 Communciation Channel.
- Device ID – UUID of the new device.

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

<No changes prior to this point in this clause>

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.

<Some text and/or figures not shown>

The Random PIN device OTM security depends on an assumption that a secure out-of-band method 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.

<Some text and/or figures not shown>

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) 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

7.3.6.3 Certificate Owner Transfer Sequence Security Considerations

In order for full, mutual authentication to occur between the device and the DOTS, both the device and DOTS must be able to trace back to a mutual Trust Anchor or Certificate Authority. This implies that OCF may need to obtain services from a Certificate Authority (e.g. Symantec, Verisign, etc.) to provide ultimate Trust Anchors from which all subsequent OCF Trust Anchors are derived.

The DOTS authenticates the device during onboarding. However, the device is not required to authenticate the DOTS due to potential resource constraints on the device.

In the case where the Device does NOT authenticate the DOTS software, there is the possibility of malicious DOTS software unwittingly deployed by users, or maliciously deployed by an adversary, which can compromise OCF Security Domain access credentials and/or personal information.

7.3.6.4 Manufacturer Certificate Based OTM Sequence

Manufacturer Certificate Based OTM sequence is shown in Figure 16 and steps described in Table 4.

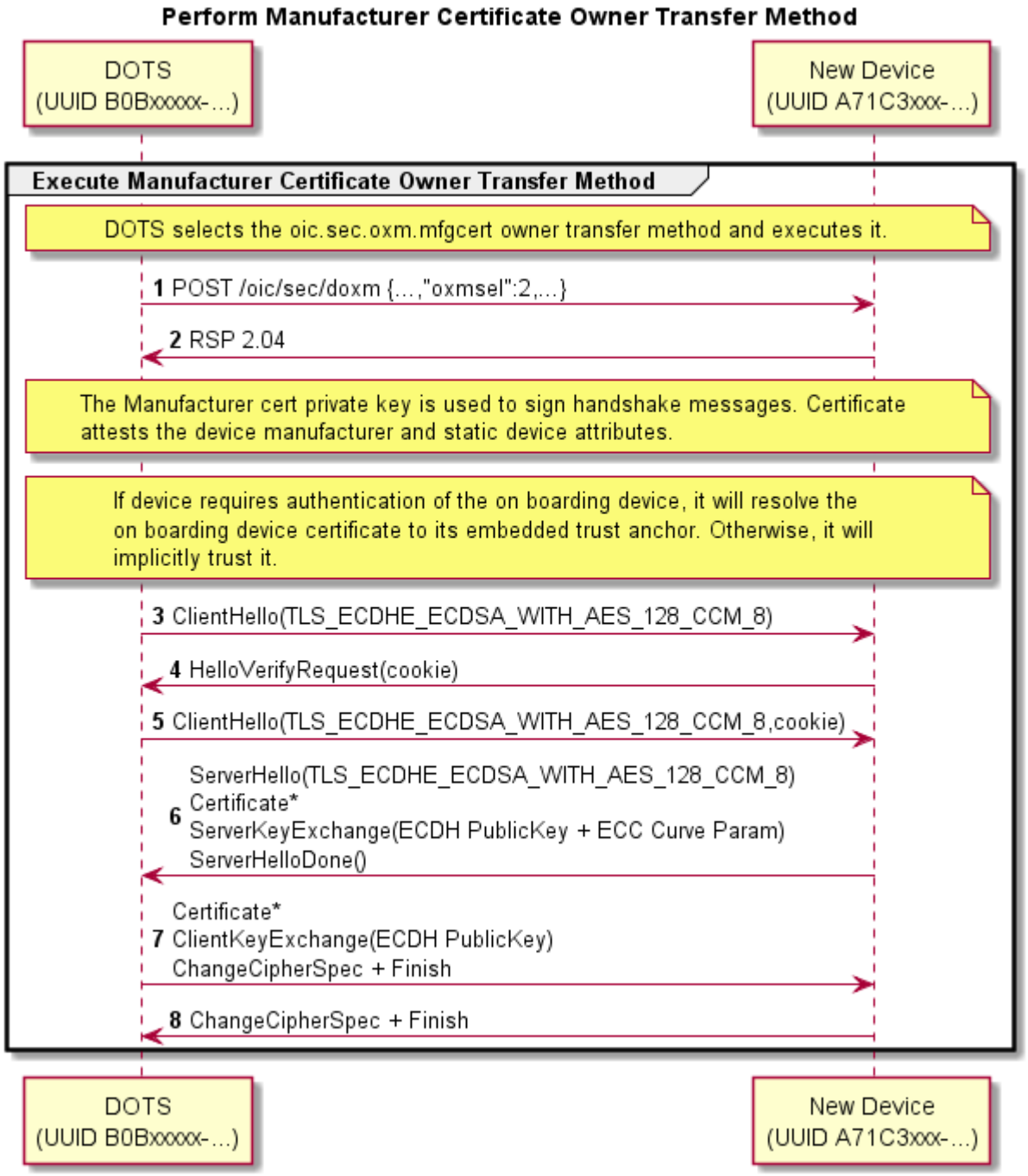


Figure 4 – Manufacturer Certificate Based OTM Sequence

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

7.3.7 Vendor Specific OTMs

7.3.8 Establishing Owner Credentials

<No changes prior to this point in this clause>

1) The OBT establishes the Device ID and Device owner uuid - See Figure 18 and Table 6.

<Some text and/or figures not shown>

In particular, if the OBT selects symmetric owner credentials:

– 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.

– 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.

<Some text and/or figures not shown>

If the OBT selects asymmetric owner credentials:

– The OBT adds its public key to the new Device's "/oic/sec/cred" Resource, identified as an Asymmetric Encryption Key.

– The OBT queries the "/oic/sec/cred" Resource from the new Device, supplying the new Device's UUID via the SubjectID query parameter. In response, the new Device shall return the public Asymmetric Encryption Key.

If the OBT selects certificate owner credentials:

– The OBT creates a certificate or certificate chain with the leaf certificate containing the public key returned by the new Device, signed by a mutually-trusted CA, and complying with the Certificate Credential Generation requirements defined in 7.3.3.

– The OBT adds the newly-created certificate chain to the "/oic/sec/cred" Resource, identified as an Asymmetric Signing Key with Certificate.

<No changes after this point in this clause>

7.3.9 Security considerations regarding selecting an Ownership Transfer Method - Moved to OCF Onboarding Tool document

7.3.10 Security Profile Assignment

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 24 and steps described in Table 12.

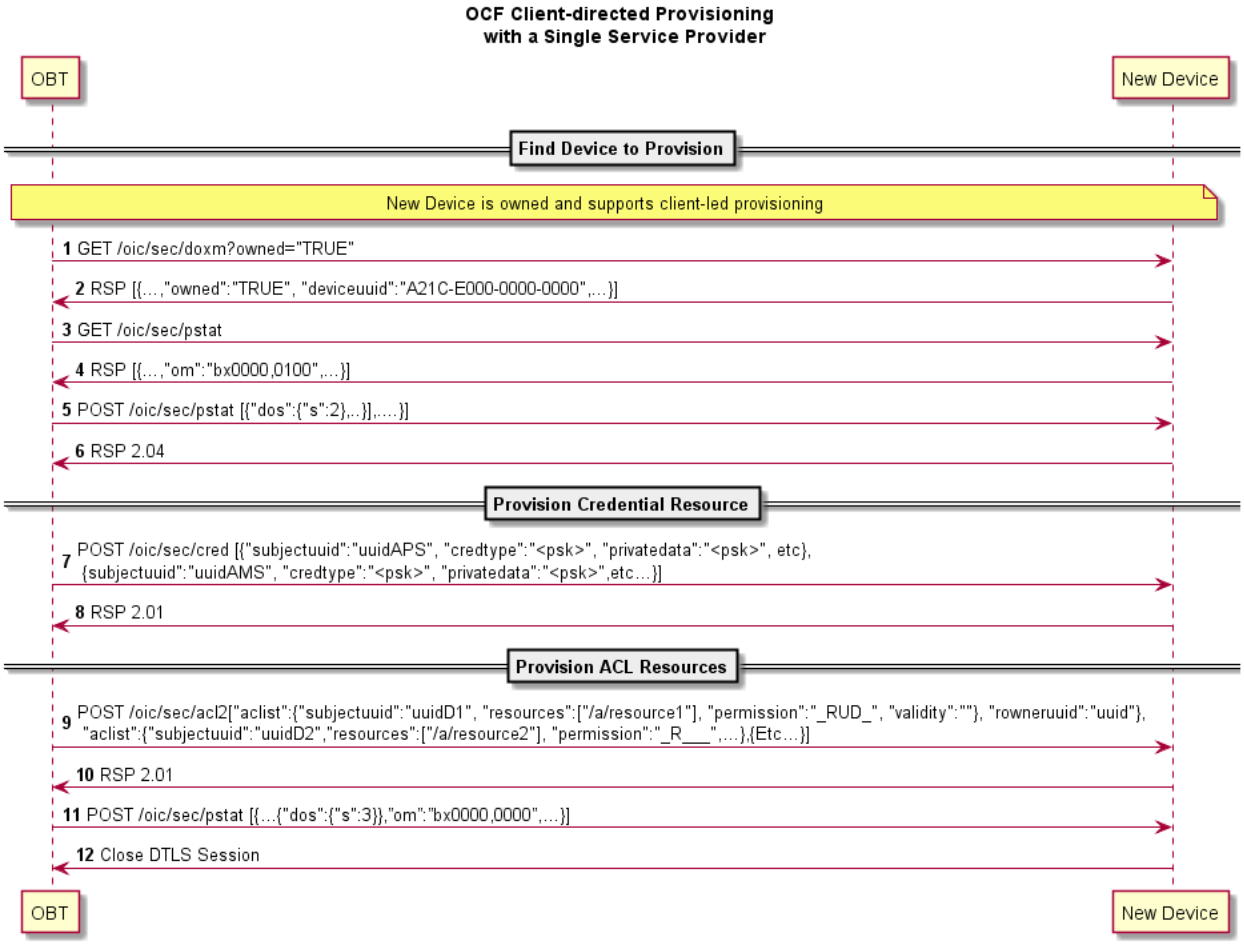


Figure 5 – Example of Client-directed provisioning

Table 5 – 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

7.4.1.4 Server-directed Provisioning Involving Multiple Support Services - Deprecated

8 Device Onboarding State Definitions

8.1 Device Onboarding General

8.2 Device Onboarding-Reset State Definition

8.3 Device Ready-for-OTM State Definition

8.4 Device Ready-for-Provisioning State Definition

8.5 Device Ready-for-Normal-Operation State Definition

8.6 Device Soft Reset State Definition

<No changes prior to this point in this clause>

If the DOTS credential cannot be found or is determined to be corrupted, the Device state transitions to RESET. The Device should remain in SRESET if the DOTS credential fails to validate the DOTS. This mitigates denial-of-service attacks that may be attempted by non-DOTS Devices.

When in SRESET, the following Resources and their specific Properties shall have the values as specified.

1) The "owned" Property of the "/oic/sec/doxm" Resource shall be TRUE.
2) The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
3) The "devowner" Property of the "/oic/sec/doxm" Resource shall be non-null, if this Property is implemented.
4) The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
5) The "deviceid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
6) The "sct" Property of the "/oic/sec/doxm" Resource shall retain its value.
7) The "oxmsel" Property of the "/oic/sec/doxm" Resource shall retains its value.
8) The "isop" Property of the "/oic/sec/pstat" Resource shall be FALSE.
9) The "/oic/sec/pstat.dos.s" Property shall be SRESET.
10) The "om" (operational modes) Property of the "/oic/sec/pstat" Resource shall be "client-directed mode".
11) The "sm" (supported operational modes) Property of "/oic/sec/pstat" Resource may be updated by the Device owner (aka DOTS).

12) The "rowneruuid" Property of "/oic/sec/pstat", "/oic/sec/doxm", "/oic/sec/acl2", and "/oic/sec/cred" Resources may be reset by the Device owner (aka DOTS) and re-provisioned.

9 Security Credential Management

9.1 Preamble

This clause provides an overview of the credential types in OCF, along with details of credential use, provisioning and ongoing management.

9.2 Credential Lifecycle

9.2.1 Credential Lifecycle General

OCF credential lifecycle has the following phases: (1) creation, (2) deletion, (3) refresh and (5) revocation.

9.2.2 Creation

The CMS can provision credentials to the credential Resource on the Device. The Device shall verify the CMS is authorized by matching the rowneruuid Property of the "/oic/sec/cred" resource to the DeviceID of the credential the CMS used to establish the secure connection.

<No changes after this point in this clause>

9.2.3 Deletion

The CMS can delete credentials from the credential Resource.

<No changes after this point in this clause>

9.2.4 Refresh

Credential refresh may be performed before it expires. The CMS performs credential refresh.

<Some text and/or figures not shown>

<No changes after this point in this clause>

9.2.5 Revocation

9.3 Credential Types

9.4 Certificate Based Key Management

9.4.1 Overview

<No changes prior to this point in this clause>

The DOTS assigns a CMS to a Device when it is newly onboarded.

9.4.2 X.509 Digital Certificate Profiles

9.4.3 Certificate Revocation List (CRL) Profile

9.4.4 Resource Model

9.4.5 Certificate Provisioning

The CMS (e.g. a hub or a smart phone) issues certificates for new Devices.

The CA in the CMS retrieves a Device's public key and proof of possession of the private key, generates a Device's certificate signed by this CA certificate, and then the CMS transfers them to the Device including its CA certificate chain. Optionally, the CMS can also transfer one or more role certificates, which shall have the format described in clause 9.4.2. The subjectPublicKey of each role certificate shall match the subjectPublicKey in the Device certificate.

In the sequence in Figure 29, the Certificate Signing Request (CSR) is defined by PKCS#10 in IETF RFC 2986, and is included here by reference.

The sequence flow of a certificate transfer for a Client-directed model is described in Figure 29.

1) <Some text and/or figures not shown>.
2) <Some text and/or figures not shown>.
3) The CMS transfers the issued certificate and CA chain to the designated Device using the same credid, to maintain the association with the private key.

<No changes after this point in this clause>

9.4.6 CRL Provisioning

The only pre-requirement of CRL issuing is that CMS (e.g. a hub or a smart phone) has the function to register revocation certificates, to sign CRL and to transfer it to Devices.

The CMS sends the CRL to the Device.

Any certificate revocation reasons listed below cause CRL update on each Device.

– change of issuer name
– change of association between Devices and CA
– certificate compromise
– suspected compromise of the corresponding private key

CRL may be updated and delivered to all accessible Devices in the OCF Security Domain. In some special cases, Devices may request CRL to a given CMS.

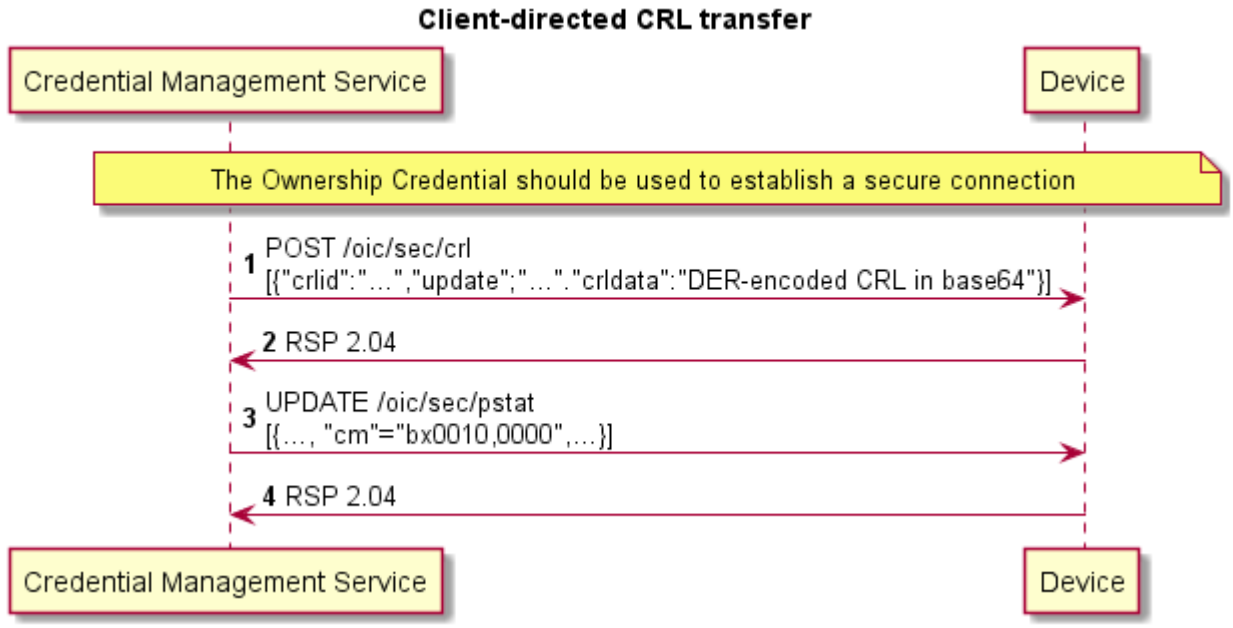
There are two options to update and deliver CRL;

– CMS pushes CRL to each Device
– each Device periodically requests to update CRL

The sequence flow of a CRL transfer for a Client-directed model is described in Figure 30.

1) The CMS may retrieve the CRL Resource Property.
2) If the Device requests the CMS to send CRL, it should transfer the latest CRL to the Device.

414



416 **Figure 6 – Client-directed CRL Transfer**

417
418

419 # 10 Device Authentication

420 # 11 Message Integrity and Confidentiality

421 # 12 Access Control

422 ## 12.1 ACL Generation and Management

423 This clause is intentionally left empty.

424 ## 12.2 ACL Evaluation and Enforcement

425 ### 12.2.1 ACL Evaluation and Enforcement General

426 ### 12.2.2 Host Reference Matching

427 ### 12.2.3 Resource Wildcard Matching

428 ### 12.2.4 Multiple Criteria Matching

429 ### 12.2.5 Subject Matching using Wildcards

430 ### 12.2.6 Subject Matching using Roles

431 ### 12.2.7 ACL Evaluation

432 #### 12.2.7.1 ACE2 matching algorithm

433 The OCF Server shall apply an ACE2 matching algorithm that matches in the following sequence:

1) The local "/oic/sec/acl2" Resource contributes its ACE2 entries for matching.

<No changes after this point in clause 12>

13 Security Resources

13.1 Security Resources General

OCF Security Resources are shown in Figure 34.

"/oic/sec/cred" Resource and Properties are shown in Figure 35.

"/oic/sec/acl2" Resource and Properties are shown in Figure 36.

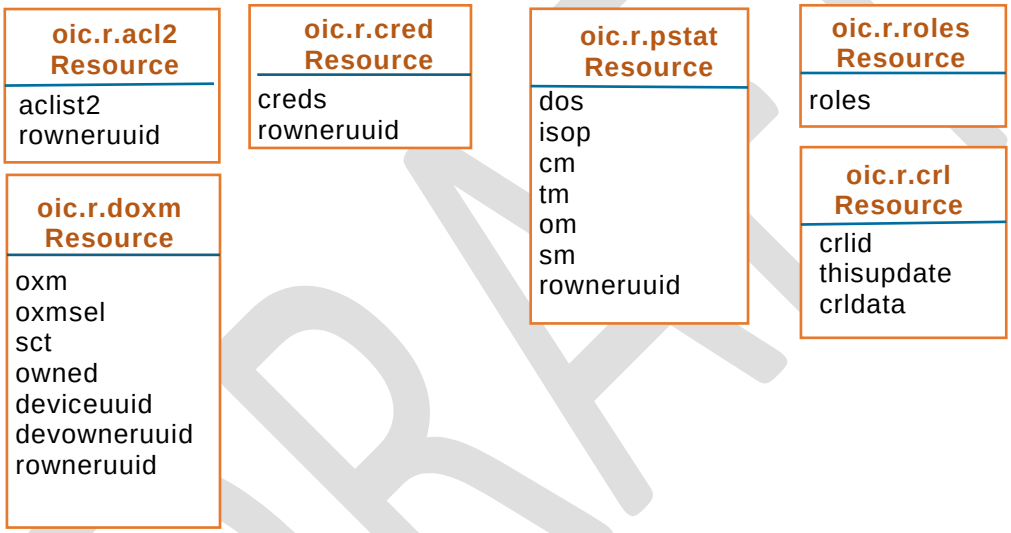


Figure 7 – OCF Security Resources

13.2 Device Owner Transfer Resource

13.2.1 Device Owner Transfer Resource General

<No changes prior to this point in this clause>.

<Some text and/or figures not shown>

<Some text and/or figures not shown>

<No changes after this point in this clause>

13.2.2 Persistent and Semi-Persistent Device Identifiers

13.2.3 Onboarding Considerations for Device Identifier

13.2.4 OCF defined OTMs

Table 27 defines the Properties of the "oic.sec.doxmtype".

Table 6 – Properties of the "oic.sec.doxmtype" Property

Value Type Name	Value Type URN (optional)	Enumeration Value (mandatory)	Description
OCFJustWorks	oic.sec.doxm.jw	0	The just-works method relies on anonymous Diffie-Hellman key agreement protocol to allow an DOTS to assert ownership of the new Device. The first DOTS to make the assertion is accepted as the Device owner. The just-works method results in a shared secret that is used to authenticate the Device to the DOTS and likewise authenticates the DOTS to the Device. The Device allows the DOTS to take ownership of the Device, after which a second attempt to take ownership by a different DOTS will fail[a].
OCFSharedPin	oic.sec.doxm.rdp	1	The new Device randomly generates a PIN that is communicated via an out-of-band channel to a DOTS. An in-band Diffie-Hellman key agreement protocol establishes that both endpoints possess the PIN. Possession of the PIN by the DOTS signals the new Device that device ownership can be asserted.
OCFMfgCert	oic.sec. doxm.mfgcert	2	The new Device is presumed to have been manufactured with an embedded asymmetric private key that is used to sign a Diffie-Hellman exchange at Device onboarding. The manufacturer certificate should contain Platform hardening information and other security assurances assertions.
OCF Reserved	<Reserved>	3	Reserved
OCFSelf	oic.sec.oxm.self	4	The manufacturer shall set the /doxm.oxmsel value to (4). The Server shall reset this value to (4) upon entering RESET Device state.
OCF Reserved	<Reserved>	5~0xFEFF	Reserved for OCF use
Vendor-defined Value Type Name	<Reserved>	0xFF00~0xFFFF	Reserved for vendor-specific OTM use
a The just-works method is subject to a man-in-the-middle attacker. Precautions should be taken to provide physical security when this method is used.			

459 **13.3 Credential Resource**

460 **13.3.1 Credential Resource General**

461 **13.3.2 Properties of the Credential Resource**

462 **13.3.2.1 Credential ID**

463 **13.3.2.2 Subject UUID**

464 **13.3.2.3 Role ID**

465 **13.3.2.4 Credential Type**

466 **13.3.2.5 Public Data**

467 **13.3.2.6 Private Data**

468 **13.3.2.7 Optional Data**

469 **13.3.2.8 Period**

470 **13.3.2.9 Credential Refresh Method Type Definition - Deprecated**

471 **13.3.2.10 Credential Usage**

472 **13.3.2.11 Resource Owner**

473 **13.3.3 The Resource Owner Property allows credential provisioning to occur soon after**
474 **Device onboarding before access to support services has been established. It**
475 **identifies the entity authorized to manage the "/oic/sec/cred" Resource in**
476 **response to Device recovery situations.Key Formatting**

477 **13.3.4 Credential Refresh Method Details - Deprecated**

478

479 **13.4 Certificate Revocation List**

480 **13.5 ACL Resources**

481 **13.5.1 ACL Resources General**

482 All Resource hosted by a Server are required to match an ACL policy. ACL policies can be
483 expressed using "/oic/sec/acl2". The subject (e.g. "deviceuuid" of the Client) requesting access to
484 a Resource shall be authenticated prior to applying the ACL check. Resources that are available
485 to multiple Clients can be matched using a wildcard subject. All Resources accessible via the
486 unsecured communication endpoint shall be matched using a wildcard subject.

487 **13.5.2 OCF Access Control List (ACL) BNF defines ACL structures.**

488 **13.5.3 ACL Resource**

489 <No changes prior to this point in this clause>.

490 Evaluation of local ACL Resource completes when all ACL Resource have been queried and no
491 entry can be found for the requested Resource for the requestor – e.g. "/oic/sec/acl2" does not
492 match the subject and the requested Resource.

493 <No changes after this point in this clause>

494 **13.6 Access Manager ACL Resource - Deprecated**

495

13.7 Signed ACL Resource - Deprecated

13.8 Provisioning Status Resource

The "/oic/sec/pstat" Resource maintains the Device provisioning status. Device provisioning should be Client-directed or Server-directed. Client-directed provisioning relies on a Client device to determine what, how and when Server Resources should be instantiated and updated. Server-directed provisioning relies on the Server to seek provisioning when conditions dictate.

<Some text and/or figures not shown>.

<Some text and/or figures not shown>

– The Device permits an authenticated and authorised Client to change the Device state of a Device by updating pstat.dos.s to the desired value. The allowed Device state transitions are defined in Figure 27.

– Prior to updating "pstat.dos.s", the Client configures the Device to meet entry conditions for the new Device state. The SVR definitions define the entity (Client or Server) expected to perform the specific SVR configuration change to meet the entry conditions. Once the Client has configured the aspects for which the Client is responsible, it can update "pstat.dos.s".

<Some text and/or figures not shown>

– The DOTS UPDATES the "devowneruuid" Property in the "/doxm" Resource to a non-nil UUID value. The DOTS (or other authorized client) can update it multiple times while in RFOTM. It is not updatable while in other device states except when the Device state returns to RFOTM through RESET.

– The DOTS can have additional provisioning tasks to perform while in RFOTM. When done, the DOTS UPDATES the "owned" Property in the "/doxm" Resource to "true".

<Some text and/or figures not shown>

– An authorized Client performs SVR consistency checks. The authorized Client can provision SVRs as needed to ensure they are available for continued provisioning in RFPRO or for normal functioning in RFNOP.

– The authorized Device owner can avoid entering RESET state and RFOTM by UPDATING "dos.s" Property of the "/pstat" Resource with RFPRO or RFNOP values

– ACLs on SVR are presumed to be invalid. Access authorization is granted according to Device owner privileges only.

<Some text and/or figures not shown>.

Table 60 defines the values of "oic.sec.pomtype".

530 **Table 7 – Value Definition of the "oic.sec.pomtype" Property**

Value	Operation Mode	Description
bx0000,0001 (1)	Server-directed utilizing multiple provisioning services	Provisioning related services are placed in different Devices. Hence, a provisioned Device should establish multiple DTLS sessions for each service. This condition exists when bit 0 is FALSE.
bx0000,0010 (2)	Server-directed utilizing a single provisioning service	All provisioning related services are in the same Device. Hence, instead of establishing multiple DTLS sessions with provisioning services, a provisioned Device establishes only one DTLS session with the Device. This condition exists when bit 0 is TRUE.
bx0000,0100 (4)	Client-directed provisioning	Device supports provisioning service control of this Device's provisioning operations. This condition exists when bit 1 is TRUE. When this bit is FALSE this Device controls provisioning steps.
bx0000,1000(8) – bx1000,0000(128)	<Reserved>	Reserved for later use
bx1111,11xx	<Reserved>	Reserved for later use

531

532 ### 13.9 Certificate Signing Request Resource

533 ### 13.10 Roles Resource

534 ### 13.11 Account Resource

535 <No changes prior to this point in this clause>.

536 Both initial and redirected-to OCF Clouds are expected to belong to the same Vendor; they are
537 assumed to have the same UUID and are assumed to have an Out-of-Band Communication
538 Channel established.

539 <No changes prior to this point after this clause>

540 ### 13.12 Account Session Resource

541 ### 13.13 Account Token Refresh Resource

542 ### 13.14 Security Virtual Resources (SVRs) and Access Policy

543 ### 13.15 SVRs, Discoverability and OCF Endpoints

544 ### 13.16 Additional Privacy Consideration for Core and SVRs Resources

545 #### 13.16.1 Additional Privacy Considerations for Core and SVR Resources General

546 <No changes prior to this point in this clause>.

547 During the OTM process the DOTS UPDATEing devowneruuid Property of the "/oic/sec/doxm"
548 Resource to a non-nil UUID value is the trigger for the Device to expose its persistent or semi-
549 persistent device identifier. Therefore, the Device shall supply deviceuuid Property of
550 "/oic/sec/doxm" Resource in response to RETRIEVE requests while the devowneruuid Property of
551 the "/oic/sec/doxm" Resource is a non-nil-UUID value.

552 The DOTS or AMS can also provision an ACL policy that restricts access to the "/oic/sec/doxm"
553 Resource such that only authenticated Clients are able to obtain the persistent or semi-persistent
554 device identifier via the deviceuuid Property value of the "/oic/sec/doxm" Resource.

555 <No changes in this clause after this point>

13.16.2 Privacy Protecting the Device Identifiers

<No changes in this clause prior to this point>

– The AMS can provision an ACL policy on the "/oic/sec/doxm" and "/oic/d" resources to further protect the "deviceuuid" and "di" Properties from being disclosed unnecessarily.

<No changes in this clause after this point>

13.16.3 Privacy Protecting the Protocol Independent Device Identifier

<No changes in this clause prior to this point>

– The AMS can provision an ACL policy on the "/oic/d" Resource to further protect the piid Property of "/oic/p" Resource from being disclosed unnecessarily.

13.16.4 Privacy Protecting the Platform Identifier

<No changes in this clause prior to this point>

– The AMS can provision an ACL policy on the "/oic/p" Resource to protect the pi Property from being disclosed unnecessarily.

13.17 Easy Setup Resource Device State

.

The "/example/EasySetupResURI" Resource should not be discoverable in RFOTM or SRESET state. After ownership transfer process is completed with the DOTS, and the Device enters in RFPRO Device state, the "/example/EasySetupResURI" may be Discoverable.

<Some text and/or figures not shown>

In RFPRO state, AMS is expected to configure ACL2 Resource on the Device with ACE2 for following Resources to be only configurable by the Mediator with permission to UPDATE or RETRIEVE access:

– "/example/EasySetupResURI"

– "/example/WifiConfResURI"

– "/example/DevConfResURI"

An ACE2 granting RETRIEVE or UPDATE access to the Easy Setup Resource

```
{
        "subject": { "uuid": "<insert-UUID-of-Mediator>" },
        "resources": [
            { "href": "/example/EasySetupResURI" },
            { "href": "/example/WiFiConfResURI" },
            { "href": "/example/DevConfResURI" },
        ],
        "permission": 6 // RETRIEVE (2) or UPDATE and RETRIEVE(6)
}
```

ACE2 may be re-configured after Easy Setup process. These ACE2s should be installed prior to the Mediator performing any RETRIEVE/UPDATE operations on these Resources.

In RFPRO or RFNOP, the Mediator should discover /EasySetupResURI Resources and UPDATE these Resources. The Mediator may UPDATE /EasySetupResURI resources in RFNOP Device state.

A Mediator shall be hosted on an OCF Device.

14 Security Hardening Guidelines/ Execution Environment Security

14.1 Preamble

14.2 Execution Environment Elements

14.2.1 Execution Environment Elements General

14.2.2 Secure Storage

14.2.2.1 Secure Storage General

14.2.2.2 Hardware Secure Storage

14.2.2.3 Software Storage

14.2.2.4 Additional Security Guidelines and Best Practices

<No changes in this clause prior to this point>

2)

<No changes in clause 14.2 after this point>

14.3 Secure Boot

14.4 Attestation

14.5 Software Update

14.6 Non-OCF Endpoint interoperability

14.7 Security Levels

14.8 Security Profiles

14.8.1 Security Profiles General

14.8.2 Identification of Security Profiles (Normative)

14.8.3 Security Profiles

14.8.3.1 Security Profiles General

14.8.3.2 Security Profile Unspecified (sp-unspecified-v0)

14.8.3.3 Security Profile Baseline v0 (sp-baseline-v0)

14.8.3.4 Security Profile Black (sp-black-v0)

14.8.3.5 Security Profile Blue v0 (sp-blue-v0)

14.8.3.5.1 Blue Profile General

14.8.3.5.2 Platforms and Devices for Security Profile Blue v0

14.8.3.5.3 Requirements for Certification at Security Profile Blue v0

<No changes prior to this point in this clause>

– The DOTS is expected to perform a lookup of the certification status of the OCF Device using the OCF CPL Attributes Extension values and verify that the sp-blue-v0 OID is listed in the extension's "securityprofiles" field.

OCF Blue profile defines the following OCF Device security functionality:

– <Some text and/or figures not shown>

– The DOTS is expected to check certificate revocation status for all certificates in manufacturer certificate path(s) if available. If a certificate is revoked, certificate validation fails and the connection is refused. The DOTS may disregard revocation status results if unavailable.

<No changes in clause 14 after this point>

15 Device Type Specific Requirements

15.1 Bridging Security

15.1.1 Universal Requirements for Bridging to another Ecosystem

15.1.2 Additional Security Requirements specific to Bridged Protocols

15.1.2.1 Additional Security Requirements specific to the AllJoyn Protocol

For AllJoyn translator, an authenticated and authorized Client shall be able to block the communication of all OCF Devices with all Bridged Devices that don't communicate securely with the Bridge, by using the Bridge Device's "oic.r.securemode" Resource specified in ISO/IEC 30118-3:2018

<No changes in clause 15 after this point>

Annex A
(informative)
Access Control Examples

Example OCF ACL Resource

Annex B
(Informative)
Execution Environment Security Profiles

Annex C
(normative)
Resource Type definitions

C.1 List of Resource Type definitions

Table C.1 contains the list of defined security resources in this document.

Table C.1 – Alphabetized list of security resources

Friendly Name (informative)	Resource Type (rt)	Clause
Access Control List	oic.r.acl	C.3
Access Control List 2	oic.r.acl2	C.4
Account	oic.r.account	C.2
Account Session	oic.r.session	C.13
Account Token Refresh	oic.r.tokenrefresh	C.15
Certificate Revocation	oic.r.crl	C.7
Certificate Signing Request	oic.r.crl	C.8
Credential	oic.r.cred	C.6
Device owner transfer method	oic.r.doxm	C.9
Device Provisioning Status	oic.r.pstat	C.10
~~Managed Access Control~~	~~oic.r.acl2~~	~~C.5~~
Roles	oic.r.pstat	C.11
Security Profile	oic.r.sp	C.14
~~Signed Access Control List~~	~~oic.r.sacl~~	~~C.12~~

<No changes in (non-autogenerated part of) this document after this point>

