OCF “Fargo” – Clarify usage of Owner Credential – Security WG CR 2868

START OF CHANGE

3.1.20 Owner Credential (OC)

a credential, provisioned to a Device, for the purposes of mutual authentication of the Device and OBT(3.1.18) 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.

END OF CHANGE

START OF CHANGE

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 10 depicts Onboarding Overview.

```
@startuml
autonumber
title Summary of Onboarding Process
participant "OBT\n(UUID B0Bxxxxx-...)" as OT
participant "CMS Device\n(UUID C85xxxxx-...)" as CM
participant "AMS Device\n(UUID A85xxxxx-...)" as AM
participant "New Device\n(UUID A71C3xxx-...)" as ND

group Discover New Devices
note over OT, ND
Discover new devices (not owned) and find a suitable owner transfer method.
end note

OT->ND: Discover unowned devices.
ND->OT: Return supported owner transfer methods.
end
break

group Execute Owner Transfer Method
OT->ND: Select the owner transfer method.
OT<->ND: Perform the owner transfer handshake.
end
break

group Establish Device Identity
OT<->ND: Establish device identifier and provision owner identity
```

```
end
break

group Establish Owner Credentials
OT->ND: Request the type of credentials supported by the new device.
OT<->ND: Establish symmetric owner credential.end
break


group Configure Device Services
note over OT, ND
Define device and delegate management services such as AMS, CMS and DOTS.
end note
OT->ND: Provision the DOTS service by setting the resource owner for /doxm and
/pstat
OT->ND: Provision the AMS service by setting the resource owner for /acl2
OT->ND: Provision the CMS service by setting the resource owner for /cred
OT->ND:   Provision the AMS credential.
OT->ND: Provision the CMS credential.
OT->ND: Set the device's owned Property to TRUE.
end
break

group Prepare for Peer Device Interactions
note over CM, ND
Provision the new device with peer credentials and access control policies.
end note
CM->ND: Change device state to ready-for-provisioning.
CM->ND: CMS provisions credentials to the new device and peer devices.
AM->ND: AMS provisions access control entries to the new device and peer devices.

note over AM, ND
Enable the device to operate normally.
end note
AM->ND: Change device state to ready-for-normal-operation.
end

@enduml
```

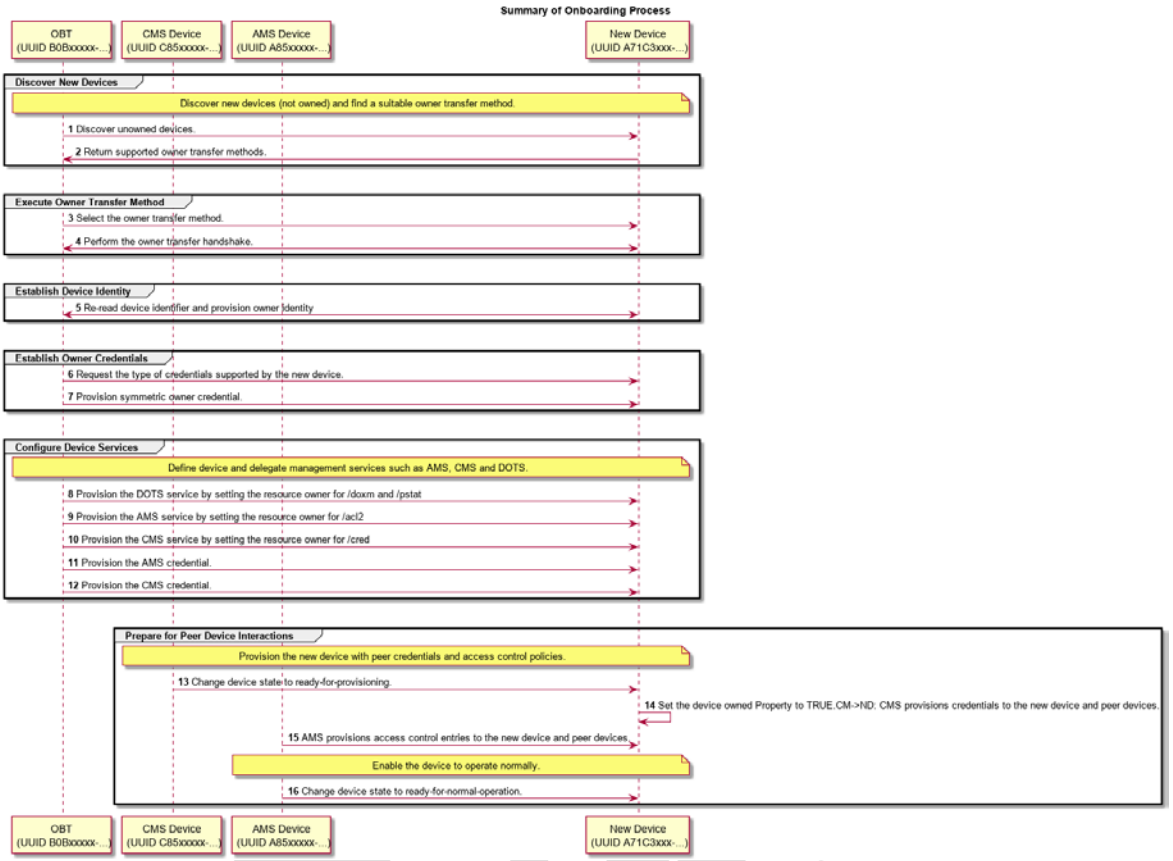

Figure 1 – Onboarding Overview

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 7.5.

Onboarding and provisioning implementations could utilize services defined outside this document, it is expected that in using other services, trust between the device being onboarded and the various tools is not transitive. This implies that the device being onboarded will individually authenticate the credentials of each and every tool used during the onboarding process; that the tools not share credentials or imply a trust relationship where one has not been established.

END OF CHANGE

START OF CHANGE

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 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 (see [OBTSpec]).

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. Owner transfer establishes 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.

– Preparing the Device for provisioning by providing credentials that may be needed.

END OF CHANGE

START OF CHANGE

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 CMSO.

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

1) The OBT establishes the Device ID and Device Owner Id
2) The OBT then establishes Device's symmetric OC - See Figure 20 and Table 8
3) Configure Device services.
4) Configure Device for peer to peer interaction

```
@startuml
autonumber
title Symmetric Owner Credential (OC) Assignment Sequence
participant "OBT\n(UUID B0Bxxxxx-...)" as OT
participant "New Device\n(UUID A71C3xxx-...)" as ND

group Owner Credential Agreement
note over OT, ND
Derive a shared symmetric key as the credential for subsequent connections with the
OBT. (If using symmetric credentials)
end note
OT->OT: SharedKey = PRF (MasterSecret, "oic.sec.oxm.mfgcert", "uuid":"B0Bxxxxx-
...", "uuid":"A71C3xxx-...", "68")
OT->OT: Generate {..., "credtype":1, "subjectuuid":"A71C3xxx-...", "credid":1,\n
"privatedata":{"encoding":"oic.sec.encoding.base64", "data":'<SharedKey>'},...}
```

```
OT->ND: UPDATE /oic/sec/cred {"creds":[{..., "credtype":1, "subjectuuid":"B0Bxxxxx-
...", "credid":1,\n "privatedata":{"encoding":"oic.sec.encoding.base64",
"data":""},...}],...}
ND->ND: Derive SharedKey Locally
ND->ND: Replace the "privatedata" \nof received credential
ND->OT: RSP 2.04
end

group Device Assignment
note over OT, ND
Assign device to a Device Owner Transfer Service and save owner credential.
end note
OT->OT: Create necessary resources for managing the new device, A71C3xxx-
OT->OT: Save the new device's owner credential details for subsequent integrity
checks and re-provisioning.
OT->OT:    Add a credential to the onboarding device's /oic/sec/cred resource that
identifies A71C3xxx-.
End

@enduml
```

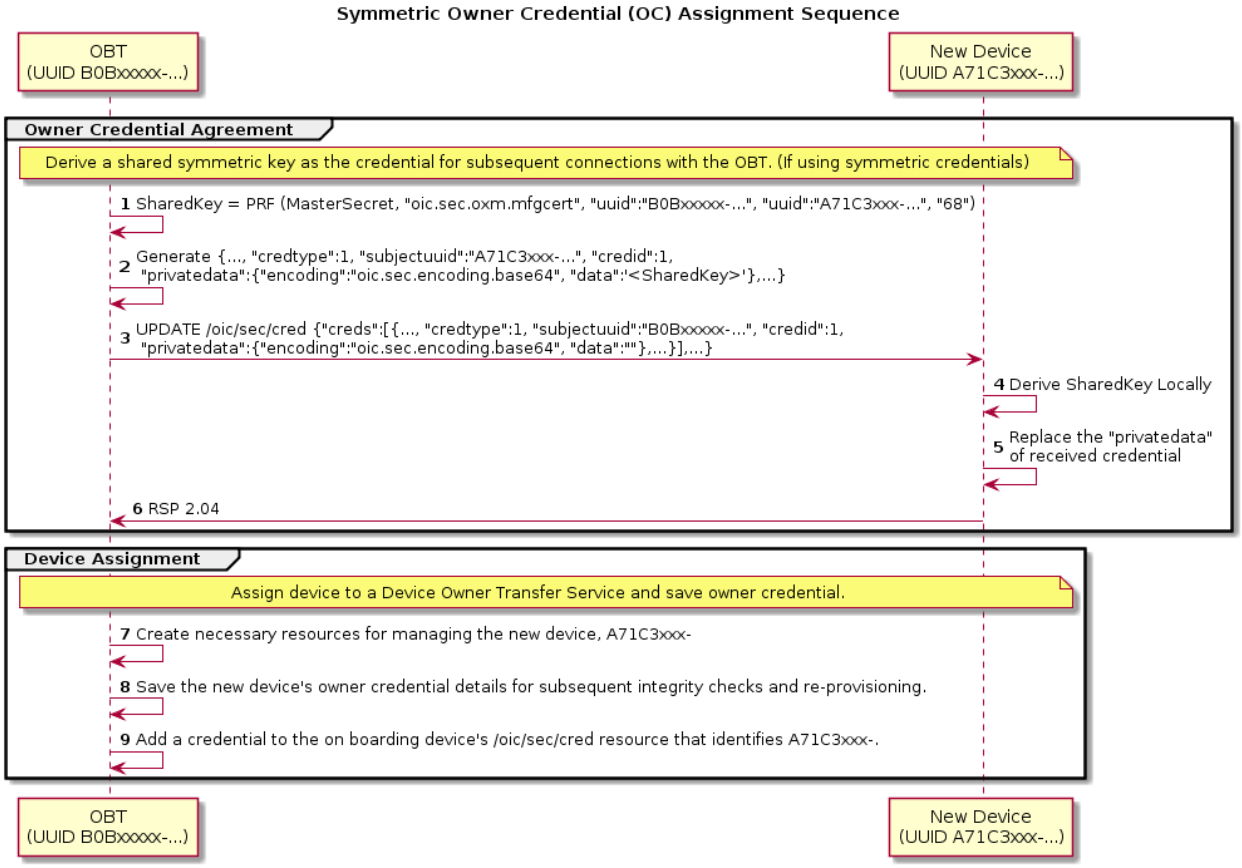

Figure 2 – Symmetric Owner Credential Provisioning Sequence

Table 1 – 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.

END OF CHANGE