OCF “Ipanema” – Clarify when OBT loses "admin" privileges during onboarding – Security WG CR 2335

Legal Disclaimer

****** Add term & def to clause 3.1 ******

1.1.1
Device Onboarding Connection (DOC)

special DTLS connection established for the purposes of onboarding the Device securely when a Device is in RFOTM state

NOTE: The Owner Transfer Method selected will determine the specifics of the DOC used.

****** End of Change ******

****** Add abbreviation to clause 3.2 ******

1.1.2
DOC
Device Onboarding Connection

****** End of Change ******

****** Changes to Clause 7.3.5.2 ******

7.3.5.2 Random PIN based Owner Transfer Sequence

Random PIN-based OTM sequence is shown in Figure 13 and steps described in Table 3.

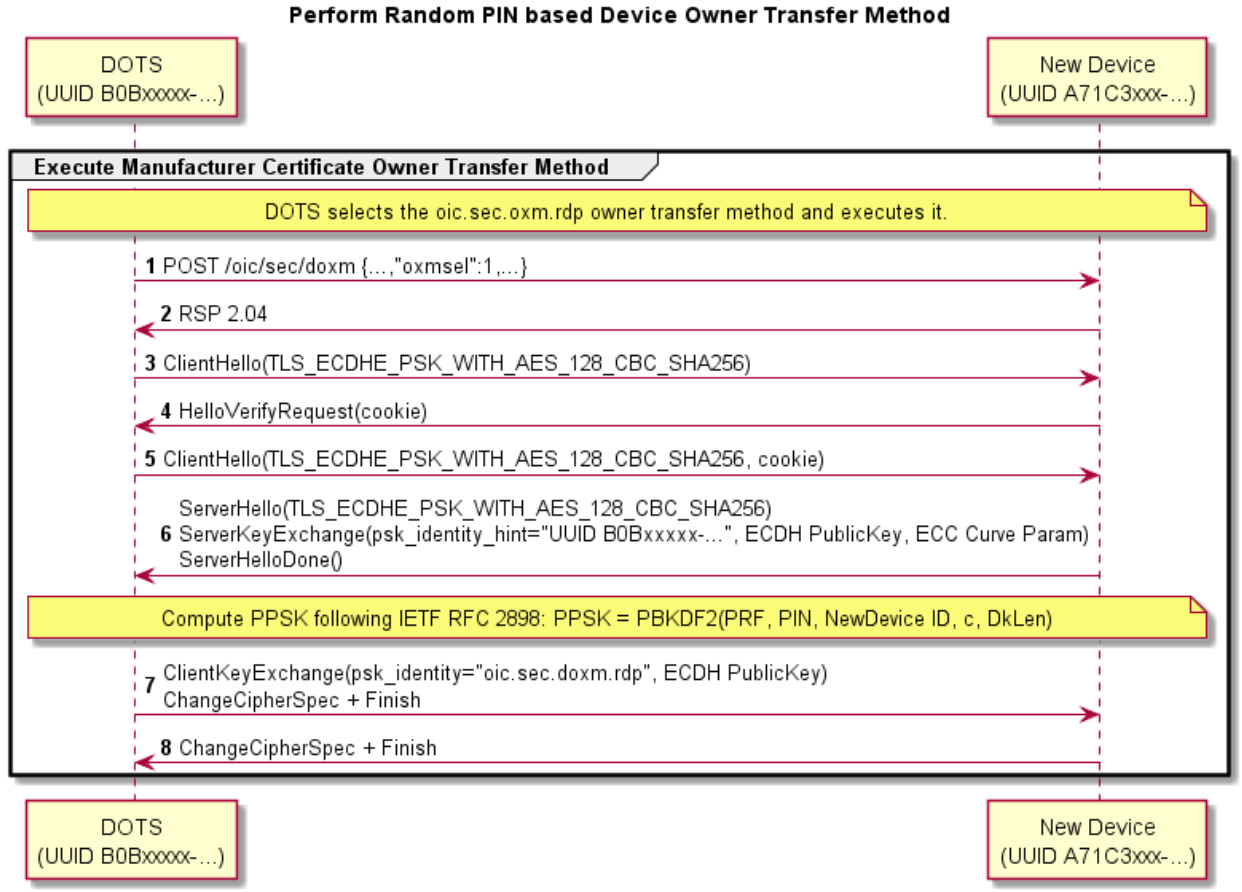

Figure 1 – Random PIN-based OTM

Table 1 – 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 following requirements apply to the DTLS handshake messages for this OTM:

– At Step 6:
  – The Server shall only use a DTLS ciphersuite supported by the Random PIN Based OTM (see clause 11.3.2.2),
  – The new Device shall set the "psk_identity_hint" field of the ServerKeyExchange message to the concatenation of

  - the string "oic.sec.doxm.rdp";
  - the colon character ':';
  - 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.

- At Step 7:
  - If the new Device determines that the "psk_identity" field of the ClientKeyExchange message does not match the string "oic.sec.doxm.rdp", then the new Device shall reject the DTLS Handshake.
  - 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 ciphersuites without confusion about which OTM should be applied.

<No further changes after this point in the present clause>

****** End of Changes ******

****** Changes to clause 7.6.2.1 ******

7.6.2.1 Manufacturer Certificate Based OTM Sequence

Manufacturer Certificate Based OTM sequence is shown in Figure 14 and steps described in Table 4.

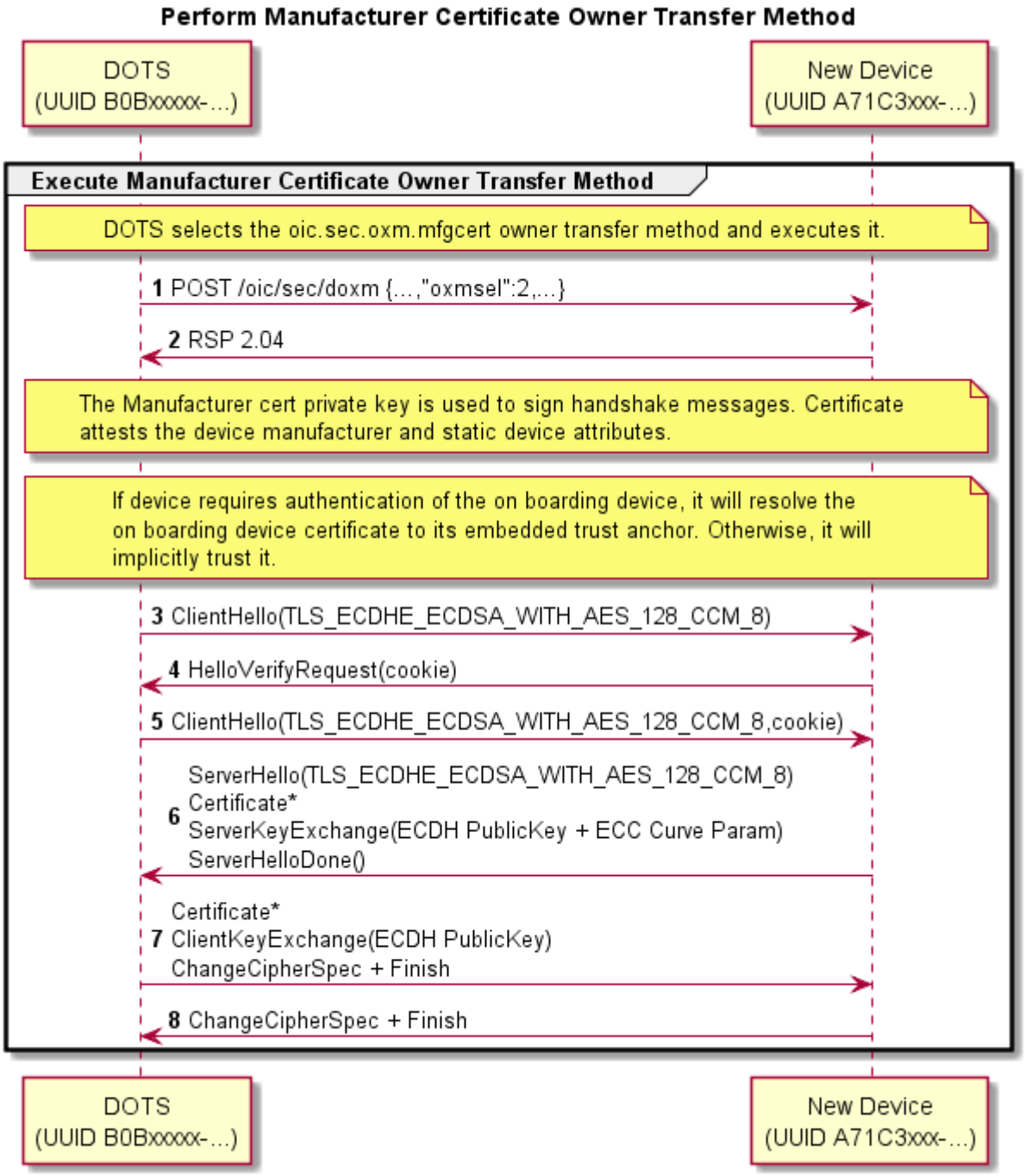

Figure 2 – Manufacturer Certificate Based OTM Sequence

Table 2 – 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. The device's manufacturer certificate may contain data attesting to the Device hardening and security properties.

If the Manufacturer Certificate Based OTM is selected at step 1, then the following requirements apply

– At step 6:
  – The new Device shall use a DTLS ciphersuite supported for use with the Manufacturer Certificate Based OTM (see clause 11.3.2.3),
  – The new Device shall not send a CertificateRequest message. Note: CertificateRequest message shall not be sent when establishing the DTLS connection for Device authentication using certificates (clause 10.4.1).

****** End of Changes ******

****** Changes to clause 8 ******

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 23 shows the various states a Device can be in during the Device lifecycle.

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.

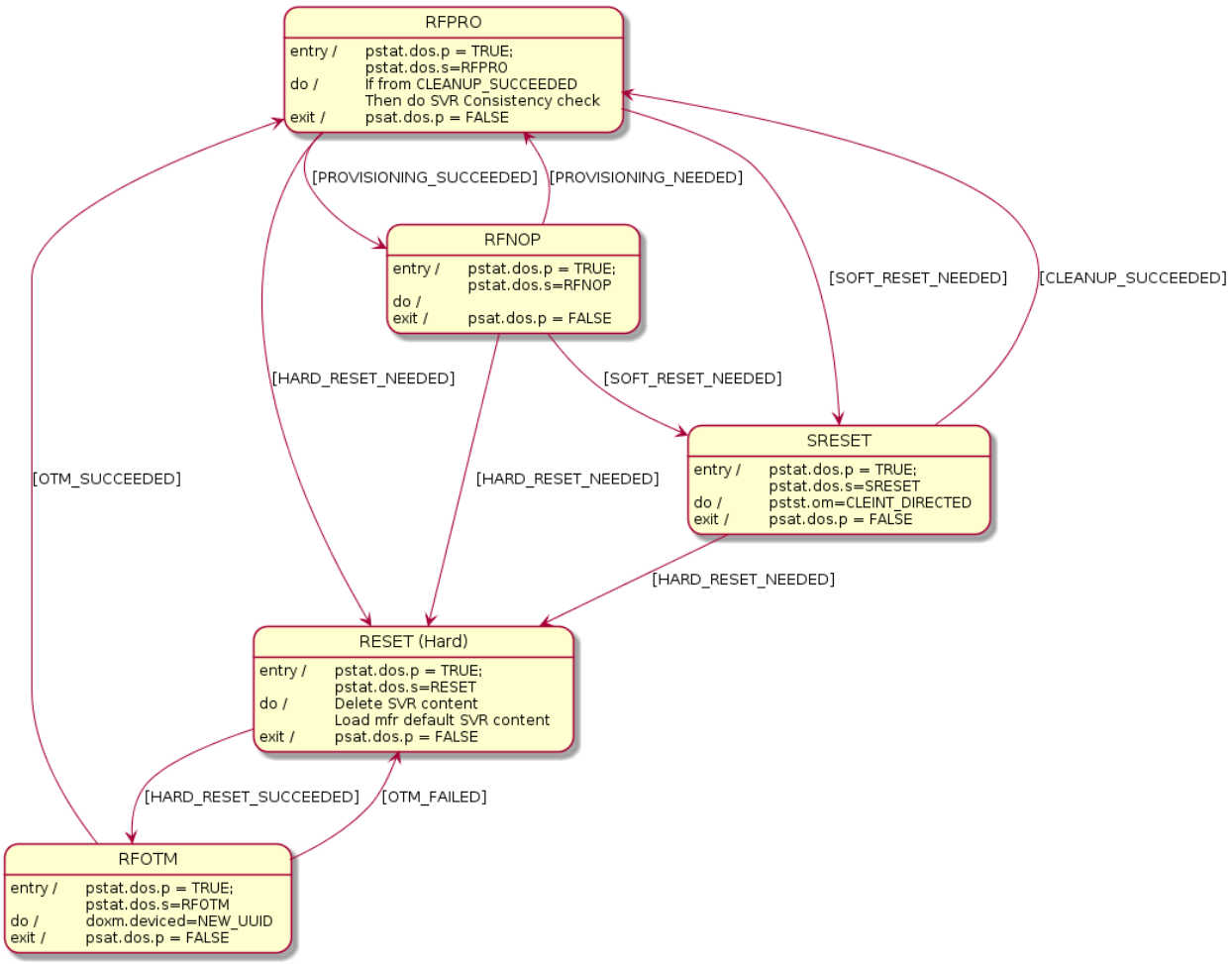

Figure 3 – Device state model

As shown in the diagram, at the conclusion of the provisioning step, the Device comes in the "Ready for Normal Operation" state where it has all it needs in order to start interoperating with other Devices. Clause 8.5 specifies the minimum mandatory configuration that a Device shall hold in order to be considered as "Ready for Normal Operation".

In the event of power loss or Device failure, the Device should remain in the same state that it was in prior to the power loss / failure

If a Device or resource owner OBSERVEs "/pstat.dos.s", then transitions to SRESET will give early warning notification of Devices that may require SVR consistency checking.

In order for onboarding to function, the Device shall have the following Resources installed:

1) "/oic/sec/doxm" Resource
2) "/oic/sec/pstat" Resource
3) "/oic/sec/cred" Resource

The values contained in these Resources are specified in the state definitions in 8.2, 8.3, 8.4, 8.5 and 8.6. Access policy for these and other SVRs are also described.

8.2 Device Onboarding-Reset State Definition

The /pstat.dos.s = RESET state is defined as a "hard" reset to manufacturer defaults. Hard reset also defines a state where the Device asset is ready to be transferred to another party.

The Platform manufacturer should provide a physical mechanism (e.g. button) that forces Platform reset. All Devices hosted on the same Platform transition their Device states to RESET when the Platform reset is asserted.

The following Resources and their specific properties shall have the value as specified:

1) The "owned" Property of the "/oic/sec/doxm" Resource shall transition to FALSE.
2) The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall be nil UUID.
3) The "devowner" Property of the "/oic/sec/doxm" Resource shall be nil UUID, if this Property is implemented.
4) The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall be set to the manufacturer default value.
5) The "deviceid" Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value, if this Property is implemented.
6) The "sct" Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value.
7) The "oxmsel" Property of the "/oic/sec/doxm" Resource shall be reset to the manufacturer's default value.
8) The "isop" Property of the "/oic/sec/pstat" Resource shall be FALSE.
9) The "dos" Property of the "/oic/sec/pstat" Resource shall be updated: dos.s shall equal "RESET" state and dos.p shall equal "FALSE".
10) The "om" (operational modes) Property of the "/oic/sec/pstat" Resource shall be set to the manufacturer default value.
11) The "sm" (supported operational modes) Property of the "/oic/sec/pstat" Resource shall be set to the manufacturer default value.
12) The "creds" Property of the "/oic/sec/cred" Resource shall be set to the manufacturer default value.
13) The "aclist2" Property of the "/oic/sec/acl2" Resource shall be set to the manufacturer default value.
14) The "rowneruuid" Property of "/oic/sec/pstat", "/oic/sec/doxm", "/oic/sec/acl2", and "/oic/sec/cred" Resources shall be nil UUID.
15) The "supportedprofiles" Property of the "/oic/sec/sp" Resource shall be set to the manufacturer default value.
16) The "currentprofile" Property of the "/oic/sec/sp" Resource shall be set to the manufacturer default value.
17) The Device shall not accept DTLS connection attempts nor TLS connection attempts nor any other requests, including discovery requests.
18) Any existing DTLS or TLS Connections shall be closed.

8.3 Device Ready-for-OTM State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for ownership transfer:

- The "owned" Property of the "/oic/sec/doxm" Resource shall be FALSE and will transition to TRUE.
- The "devowner" Property of the "/oic/sec/doxm" Resource shall be nil UUID, if this Property is implemented.
- The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall be nil UUID.
- The "deviceid" Property of the "/oic/sec/doxm" Resource may be nil UUID, if this Property is implemented. The value of the di Property in "/oic/d" is undefined.
- The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall be set to the manufacturer default value.
- The "isop" Property of the "/oic/sec/pstat" Resource shall be FALSE.
- The "dos" of the "/oic/sec/pstat" Resource shall be updated: "dos.s" shall equal "RFOTM" state and dos.p shall equal "FALSE".
- The "/oic/sec/cred" Resource shall contain credential(s) if required by the selected OTM.
- If there is no open Device Onboarding Connection, then
  - Anonymous Retrieve and Updates requests (those arriving over unauthenticated channel such as CoAP) for the “/oic/sec/doxm” Resource shall be granted.
  - If an anonymous request to Update the “/oic/sec/doxm” Resource attempts to update "oxmsel" to a value that is not indicated as supported by the Device in "oxms", then the Device shall reject the request with an appropriate error message (e.g. bad request).
  - All Retrieve requests to the “/oic/sec/pstat” Resource shall be granted.
  - All other requests, with the exception of Retrieve requests to the Discovery Resources ("/oic/res", "/oic/d" and "/oic/p"), shall be rejected with an appropriate error message (e.g. forbidden).
  - Prior to a successful anonymous Update of "oxmsel" in "/oic/sec/doxm", all attempts to establish new DTLS connections shall be rejected.
  - After a successful anonymous Update of "oxmsel" in "/oic/sec/doxm",
  - The Device shall allow establishing a Device Onboarding Connection (DOC) matching the "oxmsel" Property of the "/oic/sec/doxm" Resource (as specified in clause 7.3), and shall reject attempts to establish other DTLS connections.
- If there is an open DOC, then
  - All requests received over the DOC which target DCRs shall be granted, regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.
  - All unicast requests which are not received over the open Device DOC shall be rejected with an appropriate error message (e.g. forbidden), regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.
  - All attempts to establish new DTLS connections shall be rejected.
- If the DOC is closed in RFOTM, then the Device shall transition to RESET state.

8.4 Device Ready-for-Provisioning State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for provisioning:

- The "owned" Property of the "/oic/sec/doxm" Resource shall be TRUE.
- The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall not be nil UUID.

- The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall not be nil UUID and shall be set to the value that was determined during RFOTM processing. Also, the value of the "di" Property in "/oic/d" Resource shall be the same as the "deviceid" Property in the "/oic/sec/doxm" Resource.
- The "oxmsel" Property of the "/oic/sec/doxm" Resource shall have the value of the actual OTM used during ownership transfer.
- The "isop" Property of the "/oic/sec/pstat" Resource shall be FALSE.
- The "dos" of the "/oic/sec/pstat" Resource shall be updated: "dos.s" shall equal "RFPRO" state and "dos.p" shall equal "FALSE".
- The "rowneruuid" Property of every installed Resource shall be set to a valid Resource owner (i.e. an entity that is authorized to instantiate or update the given Resource). Failure to set a "rowneruuid" may result in an orphan Resource.
- The "/oic/sec/cred" Resource shall contain credentials for each entity referenced by "rowneruuid" and "devowneruuid" Properties.
- If there is an open DOC, then all requests received over the DOC which target a DCR shall be granted, regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.
- The Device shall allow establishing DTLS connections authenticated with locally issued credentials (clauses 10.2 and 10.4).and shall reject attempts to establish other DTLS connections.

8.5 Device Ready-for-Normal-Operation State Definition

The following Resources and their specific properties shall have the value as specified when the Device enters ready for normal operation:

- The "owned" Property of the "/oic/sec/doxm" Resource shall be TRUE.
- The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall not be nil UUID.
- The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall not be nil UUID and shall be set to the ID that was configured during OTM. Also the value of the "di" Property in "/oic/d" shall be the same as the deviceuuid.
- The "oxmsel" Property of the "/oic/sec/doxm" Resource shall have the value of the actual OTM used during ownership transfer.
- The "isop" Property of the "/oic/sec/pstat" Resource shall be set to TRUE by the Server once transition to RFNOP is otherwise complete.
- The "dos" of the "/oic/sec/pstat" Resource shall be updated: "dos.s" shall equal "RFNOP" state and dos.p shall equal "FALSE".
- The "rowneruuid" Property of every installed Resource shall be set to a valid resource owner (i.e. an entity that is authorized to instantiate or update the given Resource). Failure to set a "rowneruuid" results in an orphan Resource.
- The "/oic/sec/cred" Resource shall contain credentials for each service referenced by "rowneruuid" and "devowneruuid" Properties.
- If there is an open DOC, then requests received over the DOC shall have access decisions determined as follows:
  - A request which targets a DCR shall be granted, regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.
  - A request which targets an NCR shall be granted by matching an ACE as per normal request authorization, with "subject" matching the "anon-clear" connection type.

– The Device shall allow establishing DTLS connections authenticated with locally issued credentials and shall reject attempts to establish other DTLS connections.

8.6 Device Soft Reset State Definition

The soft reset state is defined (e.g. "/pstat.dos.s" = SRESET) where entrance into this state means the Device is not operational but remains owned by the current owner. The Device may exit SRESET by authenticating to a DOTS (e.g. "rt" = "oic.r.doxs") using the OC provided during original onboarding (but should not require use of an OTM /doxm.oxms).

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.

– The "owned" Property of the "/oic/sec/doxm" Resource shall be TRUE.
– The "devowneruuid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
– The "devowner" Property of the "/oic/sec/doxm" Resource shall be non-null, if this Property is implemented.
– The "deviceuuid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
– The "deviceid" Property of the "/oic/sec/doxm" Resource shall remain non-null.
– The "sct" Property of the "/oic/sec/doxm" Resource shall retain its value.
– The "oxmsel" Property of the "/oic/sec/doxm" Resource shall retains its value.
– The "isop" Property of the "/oic/sec/pstat" Resource shall be FALSE.
– The "/oic/sec/pstat.dos.s" Property shall be SRESET.
– The "om" (operational modes) Property of the "/oic/sec/pstat" Resource shall be "client-directed mode".
– The "sm" (supported operational modes) Property of "/oic/sec/pstat" Resource may be updated by the Device owner (aka DOTS).
– 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.
– If there is an open DOC, then all requests received over the DOC which target a DCR shall be granted, regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.
– The Device shall allow establishing DTLS connections authenticated with locally issued credentials and shall reject attempts to establish other DTLS connections.

****** End of Change ******