OCF 2.0 – Deprecate DOS-like bits of pstat.cm and pstat.tm - Security WG CR 2547

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HEREWITH INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2018 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

Make the following changes:

7.4.1.1 Client-directed Provisioning

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

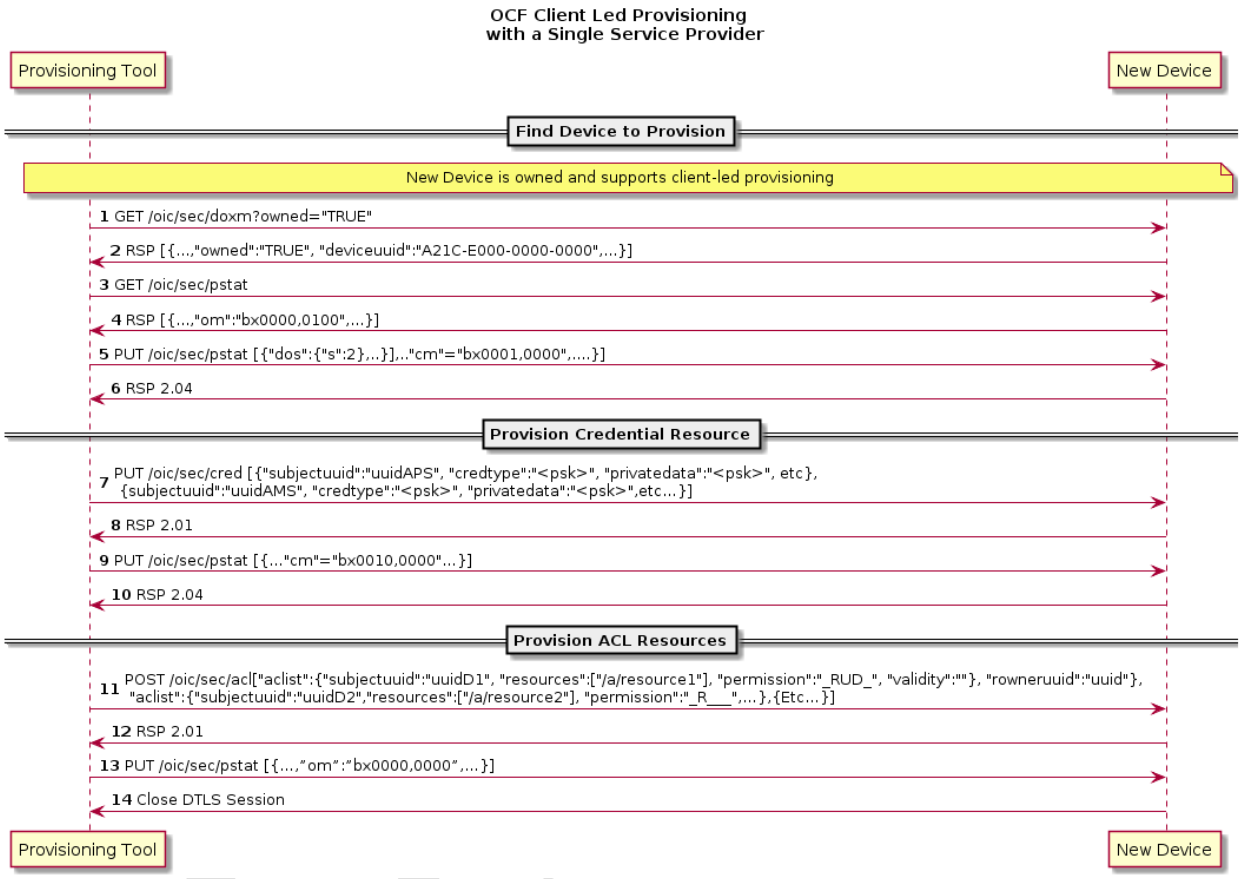

Figure 1 – Example of Client-directed provisioning

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	Provisioning Tool (PT) 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	PT instantiates the /oic/sec/cred Resource. It contains credentials for the provisioned services and other Devices
9 - 10	PT instantiates /oic/sec/acl Resources.
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.

Table 1 – Steps describing Client -directed provisioning

7.4.1.2 Server-directed Provisioning

Server-directed provisioning relies on the Server (i.e. New Device) for directing much of the provisioning work. As part of the onboarding process the support services used by the Server to seek additional provisioning are provisioned. The New Device uses a self-directed, state-driven approach to analyze current provisioning state, and tries to drive toward target state. This example assumes a single support service is used to provision the new Device.

DRAFT

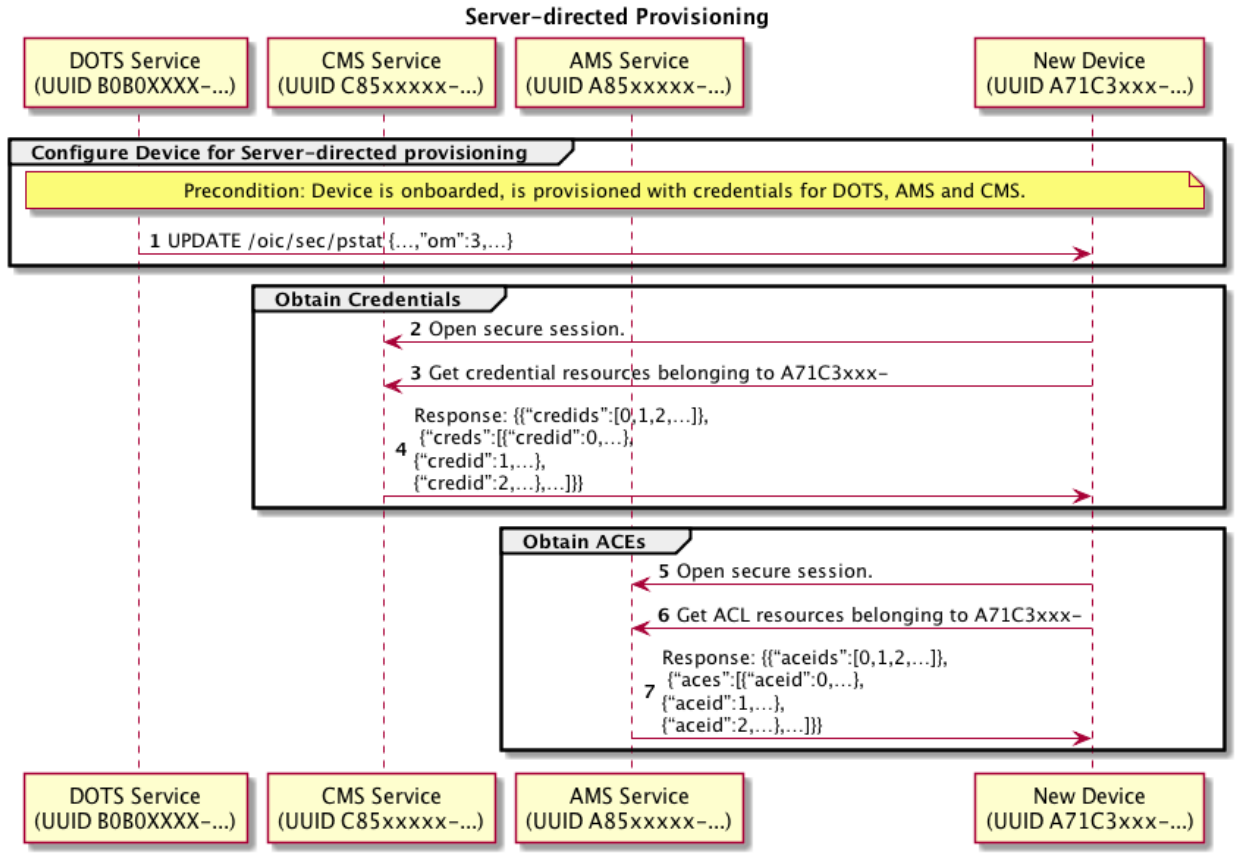

Figure 2 – Example of Server-directed provisioning using a single provisioning service

Step	Description
1	The new Device verifies it is owned.
2	The new Device verifies it is in self-provisioning mode.
3	The new Device verifies its target provisioning state is fully provisioned.
4	The new Device verifies its current provisioning state requires provisioning.
5	The new Device initiates a secure session with the provisioning tool using the /oic/sec/doxm. DevOwner value to open a TLS connection using SharedKey.
8 – 9	The new Devices gets the /oic/sec/cred Resources. It contains credentials for the provisioned services and other Devices.
11 – 12	The new Device gets the /oic/sec/acl Resources.
14	The secure session is closed.

Table 2 – Steps for Server-directed provisioning using a single provisioning service

7.4.1.3 Server-directed Provisioning Involving Multiple Support Services

A Server-directed provisioning flow, involving multiple support services distributes the provisioning work across multiple support services. Employing multiple support services is an effective way to distribute provisioning workload or to deploy specialized support. The following example demonstrates using a provisioning tool to configure two support services, a CMS and an AMS.

DRAFT

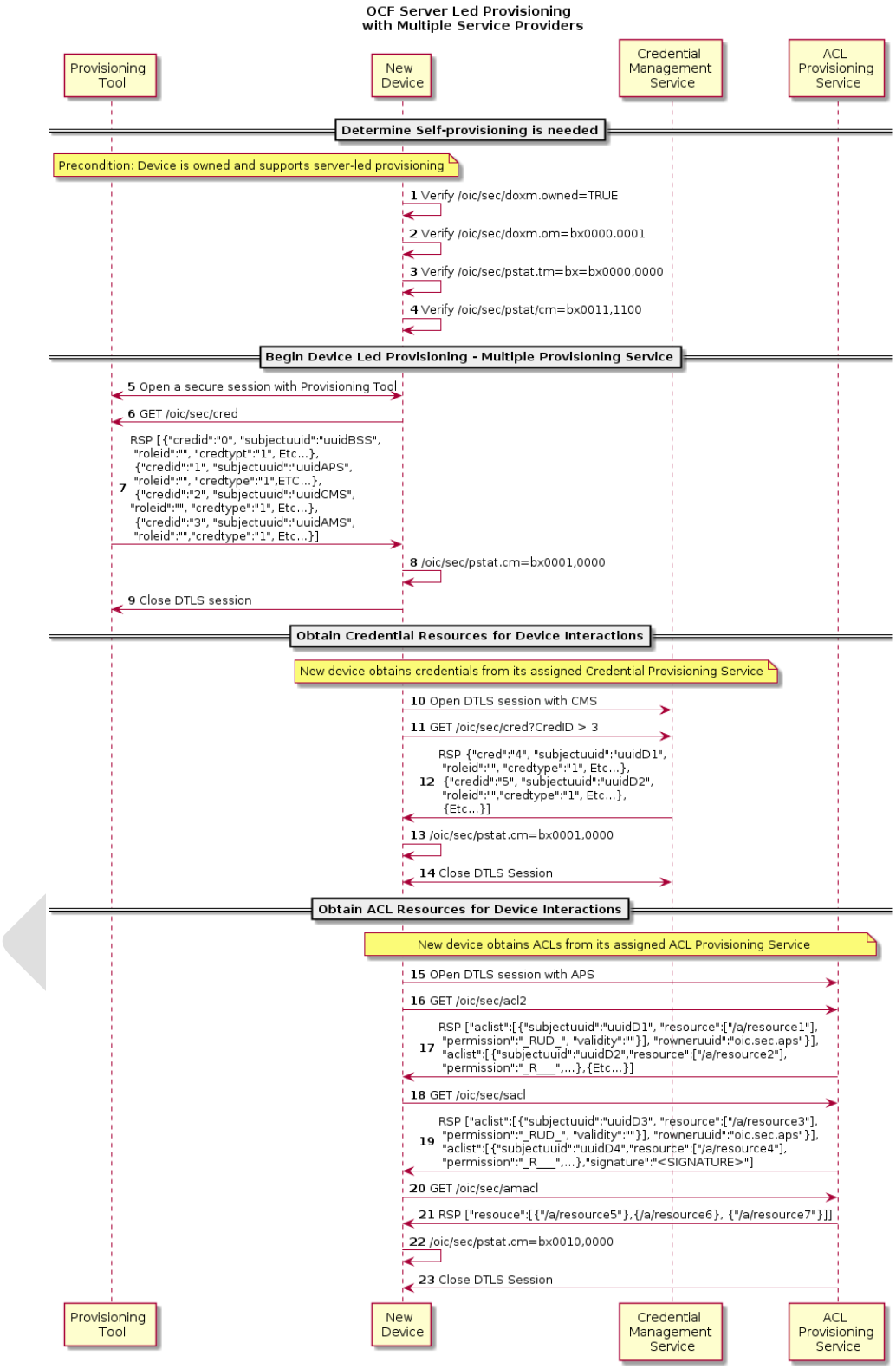

Figure 3 – Example of Server-directed provisioning involving multiple support services

Step	Description
1	The new Device verifies it is owned.
2	The new Device verifies it is in self-provisioning mode.
3	The new Device initiates a secure session with the provisioning tool using the /oic/sec/doxm. DevOwner value to open a TLS connection using SharedKey.
4-5	The new Device gets credentials Resource for the provisioned services and other Devices
6	The new Device closes the DTLS session with the provisioning tool.
7	The new Device finds the CMS from the /oic/sec/cred Resource, rowneruuid Property and opens a DTLS connection. The new device finds the credential to use from the /oic/sec/cred Resource.
8-9	The new Device requests additional credentials that are needed for interaction with other devices.
10	The DTLS connection is closed.
11	The new Device finds the ACL provisioning and management service from the /oic/sec/acl2 Resource, rowneruuid Property and opens a DTLS connection. The new device finds the ACL to use from the /oic/sec/acl2 Resource.
12-13	The new Device gets ACL Resources that it will use to enforce access to local Resources.
14-15	The new Device should get SACL Resources immediately or in response to a subsequent Device Resource request.
16-17	The new Device should also get a list of Resources that should consult an Access Manager for making the access control decision.
18	The DTLS connection is closed.

Table 3 – Steps for Server-directed provisioning involving multiple support services

8 Device Onboarding State Definitions

As explained in Section 5.2, 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 Section 5.3. The diagram below 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.

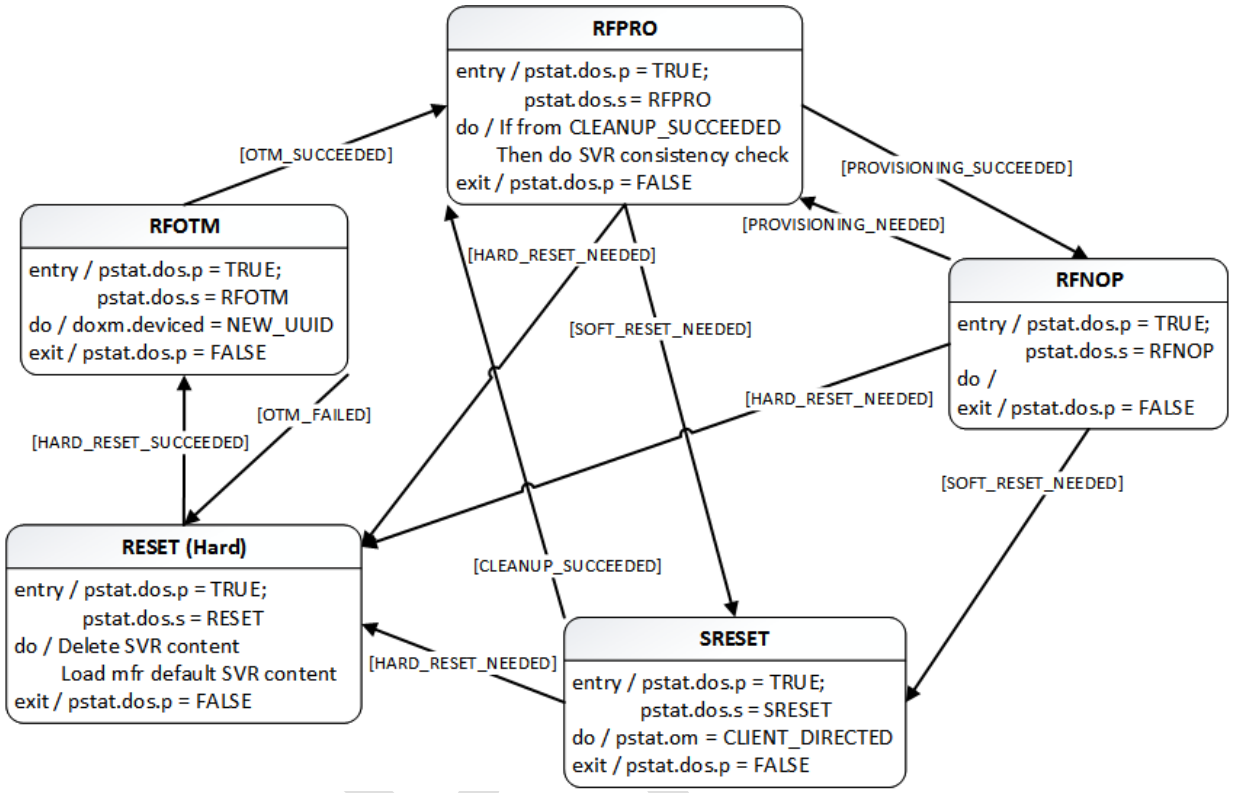

Figure 4 – Device state model

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. Section 8.1 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

/oic/sec/pstat Resource

/oic/sec/cred Resource

The values contained in these Resources are specified in the state definitions below.

8.1 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 nil-UUID 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 rowneruuid Property of /oic/sec/pstat, /oic/sec/doxm, /oic/sec/acl, /oic/sec/amacl, /oic/sec/sacl, and /oic/sec/cred Resources shall be nil UUID.

8.2 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:

1) The owned Property of the /oic/sec/doxm Resource shall be FALSE and will transition to TRUE.

2) The devowner Property of the /oic/sec/doxm Resource shall be nil UUID, if this Property is implemented.

3) The devowneruuid Property of the /oic/sec/doxm Resource shall be nil UUID.

4) 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.

5) The deviceuuid Property of the /oic/sec/doxm Resource may be nil UUID. The value of the di Property in /oic/d is undefined.

6) The isop Property of the /oic/sec/pstat Resource shall be FALSE.

7) The dos of the /oic/sec/pstat Resource shall be updated: dos.s shall equal "RFOTM" state and dos.p shall equal "FALSE".

8) The /oic/sec/cred Resource shall contain credential(s) if required by the selected OTM

8.3 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:

1) The owned Property of the /oic/sec/doxm Resource shall be TRUE.

2) The devowneruuid Property of the /oic/sec/doxm Resource shall not be nil UUID.

3) 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.

4) The oxmsel Property of the /oic/sec/doxm Resource shall have the value of the actual OTM used during ownership transfer.

5) The isop Property of the /oic/sec/pstat Resource shall be FALSE.

6) The dos of the /oic/sec/pstat Resource shall be updated: dos.s shall equal "RFPRO" state and dos.p shall equal "FALSE".

7) 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.

8) The /oic/sec/cred Resource shall contain credentials for each entity referenced by an rowneruuid, amsuuid, devowneruuid.

8.4 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:

1) The owned Property of the /oic/sec/doxm Resource shall be TRUE.

2) The devowneruuid Property of the /oic/sec/doxm Resource shall not be nil UUID.

3) 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.

4) The oxmsel Property of the /oic/sec/doxm Resource shall have the value of the actual OTM used during ownership transfer.

5) The isop Property of the /oic/sec/pstat Resource shall be set to TRUE by the Server once transition to RFNOP is otherwise complete.

6) The dos of the /oic/sec/pstat Resource shall be updated: dos.s shall equal "RFNOP" state and dos.p shall equal "FALSE".

7) 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.

8) The /oic/sec/cred Resource shall contain credentials for each service referenced by a rowneruuid, amsuuid, devowneruuid.

8.5 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).

The DOTS should perform a consistency check of the SVR and if necessary, re-provision them sufficiently to allow the Device to transition to RFPRO.

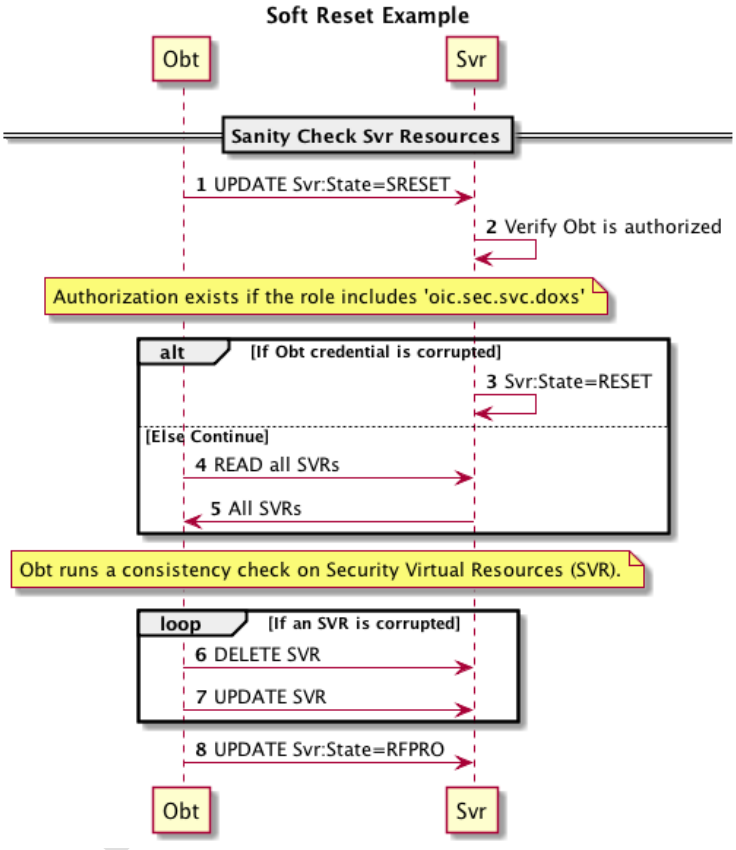

Figure 5 – OBT Sanity Check Sequence in SRESET

The DOTS should perform a sanity check of SVRs before final transition to RFPRO Device state. 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 DOXS 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 deviceuuidProperty 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 DOXS).
12) The rowneruuid Property of /oic/sec/pstat, /oic/sec/doxm, /oic/sec/acl, /oic/sec/acl2, /oic/sec/amacl, /oic/sec/sacl, and /oic/sec/cred Resources may be reset by the Device owner (aka DOXS) and re-provisioned.

13.7 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. Server-directed provisioning depends on configuration of the rowneruuid Property of the /oic/sec/doxm, /oic/sec/cred and /oic/sec/acl2 Resources to identify the device ID of the trusted DOXS, CMS and AMS services respectively. Furthermore,

the /oic/sec/cred Resource should be provisioned at ownership transfer with credentials necessary to open a secure connection with appropriate support service.

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	Interfaces	Description	Related Functional Interaction
/oic/sec/pstat	Provisioning Status	oic.r.pstat	baseline	Resource for managing Device provisioning status	Configuration

Table 4 – Definition of the oic.r.pstat Resource

DRAFT

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Device Onboarding State	dos	oic.sec.dostype	-	Yes	RW		Device Onboarding State
Is Device Operational	isop	Boolean	T|F	Yes	R	RESET	**Server shall set to FALSE**
					R	RFOTM	Server shall set to FALSE
					R	RFPRO	Server shall set to FALSE
					R	RFNOP	Server shall set to TRUE
					R	SRESET	Server shall set to FALSE
Current Mode	cm	oic.sec.dpmtype	bitmask	Yes	R	RESET	
					R	RFOTM	
					R	RFPRO	
					R	RFNOP	
					R	SRESET	
Target Mode	tm	oic.sec.dpmtype	bitmask	Yes	R	RESET	
					RW	RFOTM	
					RW	RFPRO	
					RW	RFNOP	
					RW	SRESET	
Operational Mode	om	oic.sec.pomtype	bitmask	Yes	R	RESET	Server shall set to manufacturer default.
					RW	RFOTM	Set by DOXS after successful OTM
					RW	RFPRO	Set by CMS, AMS, DOXS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOXS after successful authentication
					RW	SRESET	Set by DOXS.
Supported Mode	sm	oic.sec.pomtype	bitmask	Yes	R	All states	Supported provisioning services operation modes
Device UUID	deviceuuid	String	uuid	Yes	RW	All states	[DEPRECATED] A uuid that identifies the Device to which the status applies
Resource Owner ID	rowneruuid	String	uuid	Yes	R	RESET	Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000")

DRAFT

					RW	RFOTM	The DOXS should configure the rowneruuid Property when a successful owner transfer session is established.
					R	RFPRO	n/a
					R	RFNOP	n/a
					RW	SRESET	The DOXS (referenced via devowneruuid Property of /oic/sec/doxm Resource) should verify and if needed, update the resource owner Property when a mutually authenticated secure session is established. If the rowneruuid does not refer to a valid DOXS the Server shall transition to RESET Device state.

Table 5 – Properties of the oic.r.pstat Resource

The provisioning status Resource /oic/sec/pstat is used to enable Devices to perform self-directed provisioning. Devices are aware of their current configuration status and a target configuration objective. When there is a difference between current and target status, the Device should consult the rowneruuid Property of /oic/sec/cred Resource to discover whether any suitable provisioning services exist. The Device should request provisioning if configured to do so. The om Property of /oic/sec/pstat Resource will specify expected Device behaviour under these circumstances.

Self-directed provisioning enables Devices to function with greater autonomy to minimize dependence on a central provisioning authority that should be a single point of failure in the network.

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Device Onboarding State	s	UINT16	enum (0=RESET, 1=RFOTM, 2=RFPRO, 3=RFNOP, 4=SRESET	Y	R	RESET	The Device is in a hard reset state.
					RW	RFOTM	Set by DOXS after successful OTM to RFPRO.
					RW	RFPRO	Set by CMS, AMS, DOXS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOXS after successful authentication
					RW	SRESET	Set by CMS, AMS, DOXS after successful authentication
Pending state	p	Boolean	T | F	Y	R	All States	TRUE (1) – 's' state is pending until all necessary changes to Device resources are complete FALSE (0) – 's' state changes are complete

Table 6 – Properties of the /oic/sec/dostype Property

In all Device states:

An authenticated and authorised Client may 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 may update pstat.dos.s. The Server then makes any changes for which the Server is responsible, including updating required SVR values, and set pstat.dos.s to the new value.

The pstat.dos.p Property is read-only by all Clients.

The Server sets pstat.dos.p to TRUE before beginning the process of updating pstat.dos.s, and sets it back to FALSE when the pstat.dos.s change is completed.

Any requests to update pstat.dos.s while pstat.dos.p is TRUE are denied.

When Device state is RESET:

All SVR content is removed and reset to manufacturer default values.

The default manufacturer Device state is RESET.

DRAFT

NCRs are reset to manufacturer default values.

NCRs are inaccessible.

After successfully processing RESET the SRM transitions to RFOTM by setting s Property of /oic/sec/dostype Resource to RFOTM.

When Device state is RFOTM:

NCRs are inaccessible.

Before OTM is successful, the deviceuuid Property of /oic/sec/doxm Resource shall be set to a temporary non-repeated value as defined in sections 13.1 and 13.15.

Before OTM is successful, the s Property of /oic/sec/dostype Resource is read-only by unauthenticated requestors

After the OTM is successful, the s Property of /oic/sec/dostype Resource is read-write by authorized requestors.

The negotiated Device OC is used to create an authenticated session over which the DOXS directs the Device state to transition to RFPRO.

If an authenticated session cannot be established the ownership transfer session should be disconnected and SRM sets back the Device state to RESET state.

Ownership transfer session, especially Random PIN OTM, should not exceed 60 seconds, the SRM asserts the OTM failed, should be disconnected, and transitions to RESET (/pstat.dos.s=RESET).

The DOXS UPDATES the devowneruuid Property in the /doxm Resource to a non-nil UUID value. The DOXS (or other authorized client) may 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 DOXS may have additional provisioning tasks to perform while in RFOTM. When done, the DOXS UPDATES the "owned" Property in the /doxm Resource to “true”.

When Device state is RFPRO:

The s Property of /oic/sec/dostype Resource is read-only by unauthorized requestors and read-write by authorized requestors.

NCRs are inaccessible, except for Easy Setup Resources, if supported.

DRAFT

The OCF Server may re-create NCRs.

An authorized Client may provision SVRs as needed for normal functioning in RFNOP.

An authorized Client may perform consistency checks on SVRs to determine which shall be re-provisioned.

Failure to successfully provision SVRs may trigger a state change to RESET. For example, if the Device has already transitioned from SRESET but consistency checks continue to fail.

The authorized Client sets the /pstat.dos.s=RFNOP.

When Device state is RFNOP:

The /pstat.dos.s Property is read-only by unauthorized requestors and read-write by authorized requestors.

NCRs, SVRs and core Resources are accessible following normal access processing.

An authorized may transition to RFPRO. Only the Device owner may transition to SRESET or RESET.

When Device state is SRESET:

NCRs are inaccessible. The integrity of NCRs may be suspect but the SRM doesn't attempt to access or reference them.

SVR integrity is not guaranteed, but access to some SVR Properties is necessary. These include devowneruuid Property of the /oic/sec/doxm Resource, "creds":[{...,{"subjectuuid":<devowneruuid>},...}] Property of the /oic/sec/cred Resource and s Property of the /oic/sec/dostype Resource of /oic/sec/pstat Resource.

The certificates that identify and authorize the Device owner are sufficient to re-create minimalist /cred and /doxm resources enabling Device owner control of SRESET. If the SRM can't establish these Resources, then it will transition to RESET state.

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

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

DRAFT

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

The SRM asserts a Client-directed operational mode (e.g. /pstat.om=CLIENT_DIRECTED).

The *provisioning mode* type is a 16-bit mask enumerating the various Device provisioning modes. "{ProvisioningMode}" should be used in this document to refer to an instance of a provisioning mode without selecting any particular value.

Type Name	Type URN	Description
Device Provisioning Mode	urn:oic.sec.dpmtype	Device provisioning mode is a 16-bit bitmask describing various provisioning modes

Table 7 – Definition of the oic.sec.dpmtype Property

Value	Device Mode	Description
bx0000,0001 (1)	Deprecated	
bx0000,0010 (2)	Deprecated	
bx0000,0100 (4)	Deprecated	
bx0000,1000 (8)	Deprecated	
bx0001,0000 (16)	Deprecated	
bx0010,0000 (32)	Deprecated	
bx0100,0000 (64)	Initiate Software Version Validation	Software version validation requested/pending (1) Software version validation complete (0)
bx1000,0000 (128)	Initiate Secure Software Update	Secure software update requested/pending (1) Secure software update complete (0)

Table 8 – Value Definition of the oic.sec.dpmtype Property (Low-Byte)

DRAFT