OCF 2.0.3 – NCRs shall only be accessible in RFNOP – Security WG CR 2712

Legal Disclaimer

Clause 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. 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 DOTS, 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.

Table 1 – Definition of the oic.r.pstat Resource

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 2 – Properties of the oic.r.pstat Resource

Property Title	Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
Device Onboarding State	dos	oic.sec.dostype	N/A	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	Server shall set to 0000,0001
					R	RFOTM	Server sets it to xxxx,xx10
					R	RFPRO	Server sets it to xxxx,xx00
					R	RFNOP	Server sets it to xxxx,xx00
					R	SRESET	Server shall set to XXXX,XX01
Target Mode	tm	oic.sec.dpmtype	bitmask	Yes	R	RESET	Server shall set to 0000,0010
					RW	RFOTM	Set by DOTS after successful OTM
					RW	RFPRO	Set by CMS, AMS, DOTS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOTS after successful authentication
					RW	SRESET	Set by DOTS as needed to recover from failures. Server shall set to XXXX,XX00 upon entry into SRESET.
Operational Mode	om	oic.sec.pomtype	bitmask	Yes	R	RESET	Server shall set to manufacturer default.
					RW	RFOTM	Set by DOTS after successful OTM
					RW	RFPRO	Set by CMS, AMS, DOTS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOTS after successful authentication
					RW	SRESET	Set by DOTS.
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")
					RW	RFOTM	The DOTS should configure the rowneruuid Property when a successful owner transfer session is established.

					R	RFPRO	n/a
					R	RFNOP	n/a
					RW	SRESET	The DOTS (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 DOTS the Server shall transition to RESET Device state.

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.

Table 3 – Properties of the /oic/sec/dostype Property

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 DOTS after successful OTM to RFPRO.
					RW	RFPRO	Set by CMS, AMS, DOTS after successful authentication
					RW	RFNOP	Set by CMS, AMS, DOTS after successful authentication
					RW	SRESET	Set by CMS, AMS, DOTS 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

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.**
- **NCRs are reset to manufacturer default values.**
- **NCRs shall not be accessible.**
- **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 shall not be accessible.**
- **Before OTM is successful, the deviceuuid Property of /oic/sec/doxm Resource shall be set to a temporary non-repeated value as defined in clauses 13.2 and 13.16.**
- **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 DOTS 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 DOTS UPDATES the devowneruuid Property in the /doxm Resource to a non-nil UUID value. The DOTSDOXS (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 DOTS may have additional provisioning tasks to perform while in RFOTM. When done, the DOTSDOXS 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 shall not be accessible, except for Easy Setup Resources, if supported.**
- **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 shall not be accessible. 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**
- **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.

Table 4 – Definition of the oic.sec.dpmtype Property

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

Value	Device Mode	Description
bx0000,0001 (1)	Reset	Device reset mode enabling manufacturer reset operations
bx0000,0010 (2)	Take Owner	Device pairing mode enabling owner transfer operations
bx0000,0100 (4)	Not Applicable	N/A
bx0000,1000 (8)	Security Management Services	Service provisioning mode enabling instantiation of Device security services and related credentials
bx0001,0000 (16)	Provision Credentials	Credential provisioning mode enabling instantiation of pairwise Device credentials using a management service of type urn:oic.sec.cms
bx0010,0000 (32)	Provision ACLs	ACL provisioning mode enabling instantiation of Device ACLs using a management service of type urn:oic.sec. ams
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 6 – Value Definition of the oic.sec.dpmtype Property (High-Byte)

Value	Device Mode	Description
bx0000,0000 – bx1111,1111	<Reserved>	Reserved for later use

The *provisioning operation mode* type is a 8-bit mask enumerating the various provisioning operation modes.

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

Type Name	Type URN	Description
Device Provisioning OperationMode	urn:oic.sec.pomtype	Device provisioning operation mode is a 8-bit bitmask describing various provisioning operation modes

Table 8 – 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