OCF 1.0 Security CR - CR32

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.

Objectives

a) Remote authenticated control of device state change.

b) Removal of device from normal operation (but not removal of device ownership).

c) Removal of device from operation and enablement of device for new ownership.

Section 8 Changes

Note: Changes Section 8 of the OCFv1.0 Security Specification. Replaces Figure on line 1400.

The /pstat.dos.s property is RW by the /pstat resource owner (e.g. 'doxs' or 'bss' 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 owner credential 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.

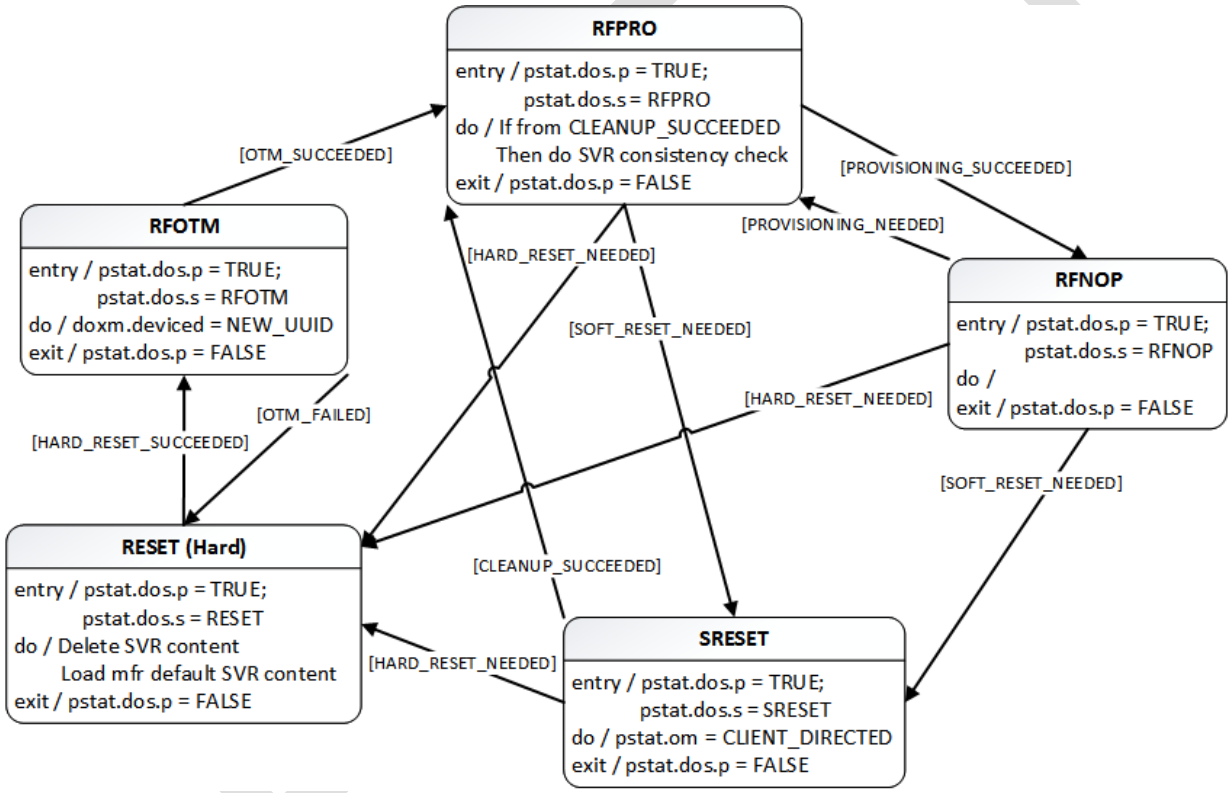

Figure <TBD> – Device state model

The device should resume to the same state that it was in at the time of 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.

Note: Changes Section 8.1 defining RESET state.

Clarify 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.

Item 9: the words ”, if this property is implemented*” shall be stricken.*

Note: Updates Section 8.2.

Item 7: the words ”, if this property is implemented*” shall be stricken.*

Note: Updates Section 8.3.

Item 6: the words ”, if this property is implemented*” shall be stricken.*

Note: Updates Section 8.4.

Item 6: the words ”, if this property is implemented*” shall be stricken.*

Note: Adds Section 8.5 defining SRESET state.

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 an onboarding tool (e.g. “rt” = “oic.r.doxs”) using the ownership credential provided during original onboarding (but should not require use of an owner transfer method /doxm.oxms).

The onboarding tool must perform a consistency check of the security virtual resources (SVR) and if necessary, re-provision them sufficiently to allow the device to transition to RFPRO.

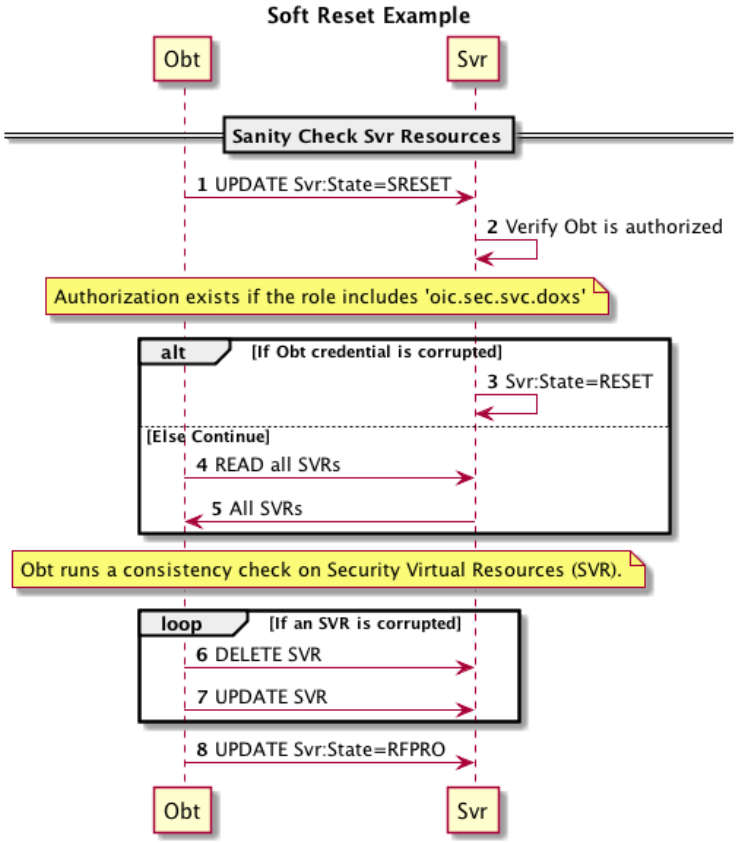

Figure 1 - OBT Sanity Check Sequence in SRESET

The OBT performs a sanity check of security virtual resources before final transition to RFPRO device state. If the device's OBT credential cannot be found or is determined to be corrupted, the device state transitions to RESET. The device remains in SRESET if the OBT credential fails to validate the OBT. This mitigates denial-of-service attacks that may be attempted by non-OBT 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 current provisioning mode property - “cm” of the /oic/sec/pstat resource shall be “00000001”.

11. The target provisioning mode property - “tm” of the /oic/sec/pstat resource shall be “00XXXX00”.

12. The operational modes property - “om” of the /oic/sec/pstat resource shall be ‘client-directed mode’.

13. The supported operational modes property (/pstat.sm) may be updated by the device owner (aka DOXS).

14. 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.

15. The “rowner” property of /oic/sec/pstat, /oic/sec/doxm, /oic/sec/acl, /oic/sec/amacl, /oic/sec/sacl, /oic/sec/cred and /oic/sec/svc resources may be reset and re-provisioned.

Section 13 Changes

13.6 /oic/sec/pstat

Note: Changes Section 13.6 of the OCFv1.0 Security Specification.

Property Name	Value Type	Value Rule	Mandatory	Access Mode	Device State	Description
dos.s	UINT16	enum (0=RESET, 1=RFOTM, 2=RFPRO, 3=RFNOP, 4=SRESET	Y	RW	RESET	The device is in a hard reset state.
				RW	RFOTM	The device is in a Ready-For-Owner-Transfer-Method state.
				RW	RFPRO	The device is in a Ready-For-PROvisioning state.
				RW	RFNOP	The device is in a Ready-For-Normal-Operation state.
				RW	SRESET	The device is in a Soft-Reset state. State transitions can be effected remotely by writing to /pstat.dos.s when the caller is authenticated and authorized to update the dos.s property.
dos.p	boolean	T|F	Y	R	-	TRUE (1) – ‘s’ state is pending until all necessary changes to device resources are complete FALSE (0) – ‘s’ state changes are complete.

Table 38 - The /pstat.dos property

In all states:

- The /pstat.dos.p property is read-only by all requestors.
- An authenticated client can effect a device state change by updating pstat.dos.s=<device_state>. Doing so instructs the server to automatically perform all the changes required to transition to the designated device state. There may be multiple steps, hence the dos.p value is set to TRUE as the first step and remains TRUE until all steps are complete. The final step sets dos.p to FALSE. The dos.s value is set to the designated

device state at the same time the dos.p value is set to FALSE. A client may observe /pstat.dos to be notified when a device state change is completed.

- The client is authenticated to write to /pstat.dos.s if it possesses an appropriate role (e.g. DOXS, CMS, AMS).
- Write requests to /pstat.dos.s where the requestor tries to transition to a state that isn't reachable will result in a DEVICE_STATE_NOT_PERMITTED error.
- Write requests to /pstat.dos.s when /pstat.dos.p is TRUE will result in a DEVICE_STATE_NOT_READY error.
- /pstat.dos.p must be set to TRUE on entrance.
- /pstat.dos.p property must be set to FALSE on exit.

When device state is RESET:

- All SVR content is removed and reset to manufacturer default values.
- The default manufacturer device state is RESET.
- Vertical resources are reset to manufacturer default values.
- Vertical resources are inaccessible.
- If client subscribers OBSERVE dos.p=FALSE, the notification is sent prior to the point where access control and credential resources (needed to deliver the message) are dismantled.
- After successfully processing RESET the SRM transitions to RFOTM by setting /pstat.dos.s to RFOTM.

When device state is RFOTM:

- Vertical resources are inaccessible.
- Before OTM is successful, the /doxm.deviceid must be set to a randomized UUID value.
- Before OTM is successful, the /pstat.dos.s property is read-only by unauthenticated requestors
- After the OTM is successful, the /pstat.dos.s property is read-write by authorized requestors.
- The negotiated device owner credential is used to create an authenticated session over which the onboarding tool directs the device state to transition to RFPRO.
- If an authenticated session cannot be established when the OTM completes after <tbd=60> seconds, the SRM asserts the OTM failed and transitions to RESET (/pstat.dos.s=RESET). (Note: The transfer of ownership is considered complete when /doxm.owned is set to TRUE. The device state may continue in RFOTM to complete initial provisioning.)

When device state is RFPRO:

- The /pstat.dos.s property is read-only by unauthorized requestors and read-write by authorized requestors.
- Vertical resources are inaccessible.
- The OCF Server may re-create vertical resources.
- An authorized client (e.g. “oic.sec.svc.doxs”, “oic.sec.svc.ams”, “oic.sec.svc.cms”) 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.
- Vertical resources, SVRs and core resources are accessible following normal access processing.
- An authorized client (e.g. “oic.sec.svc.doxs”, “oic.sec.svc.ams”, “oic.sec.svc.cms”) may transition to RFPRO. Only the device owner (e.g. “oic.sec.svc.doxs”) may transition to SRESET or RESET.

When device state is SRESET:

- Vertical resources are inaccessible. The integrity of vertical resources 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 /doxm.devowner, /cred[<devowner>] and /pstat.dos.
- 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 (e.g. “oic.sec.svc.doxs”) 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 writing RFPRO or RFNOP to /pstat.dos.s.
- ACLs on secure virtual resources (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).