# OCF 1.0 Security CR - CR22

## Legal Disclaimer

## 1. Device State Profiles

Device state may affect the property access policy. Consequently, subsequent to transitioning into or out of a device state it is possible that property access behavior may change as part of device state transition.

The property Access Mode specifies the least restricted property access across all device states. Exceptional behavior is described from the perspective of the stated access mode.

Privacy may be affected by the property's access policy; hence privacy considerations are described for each property where a privacy threat exists.

### 1.1. Security and Core Resource Property behavior conditional on Device State

| Resource Type | Property title | Property name | Value type | Access Mode | | Behavior |
|---|---|---|---|---|---|---|
| | | | | RESET | | |
| | | | | RFOTM | | |
| | | | | RFPRO | | |
| | | | | RFNOP | | |
| | | | | SRESET | | |
| oic.wk.p | Platform ID | pi | oic.types-schema.uuid | All States | R | Server shall construct a temporary random UUID. *(does not override the persistent pi)* Server sets to its persistent value after secure owner transfer session is established. |
| Oic.wk.p | Protocol Independent Identifier | piid | Oic.types-schema.uuid | RESET, SRESET RFPRO, RFNOP | R | Server should construct a temporary random UUID when entering RESET state. |
| | | | | RFOTM | RW | DOXS may set the persistent value after secure owner transfer |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | session is established; otherwise Server sets value. |
| oic.wk.d | Device Identifier | di | oic.types-schema.uuid | All states | R | /d.di shall mirror the value contained in /doxm.deviceuuid in all device states. |

Refer to Section 13.8 for additional detail related to /doxm.deviceuuid, /d.di, /d.piid and /p.pi property behavior.

Table X - Device state specific access mode behaviour for core resources.

| Resource Type | Property title | Property name | Value type | Access Mode | | Behavior |
|---|---|---|---|---|---|---|
| | | | | RESET | | |
| | | | | RFOTM | | |
| | | | | RFPRO | | |
| | | | | RFNOP | | |
| | | | | SRESET | | |
| oic.r.doxm | Device ID | deviceuuid | oic.sec.didtype | RESET | R | Server shall construct a temporary random UUID that differs for each transition to RESET. |
| | | | | RFOTM | RW | DOXS shall update to a value it has selected after secure owner transfer session is established. If update fails with error PROPERTY_NOT_FOUND the DOXS shall either accept the Server provided value or update /doxm.owned=FALSE and terminate the |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | session. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | R | n/a |
| ~~oic.r.doxm~~ | ~~Owner transfer methods~~ | ~~oxms~~ | ~~Array of oic.sec.oxmtype~~ | ~~**RESET**~~ | ~~R~~ | ~~Server shall set to manufacturer default.~~ |
| | | | | ~~**RFOTM**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFPRO**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFNOP**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**SRESET**~~ | ~~R~~ | ~~n/a~~ |
| oic.r.doxm | Selected owner transfer method | oxmsel | oic.sec.doxmtype | **RESET** | R | Server shall set to (4) “oic.sec.oxm.self” |
| | | | | **RFOTM** | RW | DOXS shall set to it’s selected DOXS and both parties execute the DOXS. After secure owner transfer session is established DOXS shall update the oxmsel again making it permanent. If the DOXS fails the Server shall transition device state to RESET. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | R | n/a |
| ~~oic.r.doxm~~ | ~~Supported credential~~ | ~~sct~~ | ~~oic.sec.credtype~~ | ~~**RESET**~~ | ~~R~~ | ~~Server shall set to manufacturer default.~~ |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ~~types~~ | | | ~~**RFOTM**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFPRO**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFNOP**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**SRESET**~~ | ~~R~~ | ~~n/a~~ |
| oic.r.doxm | Device ownership status | owned | Boolean | **RESET** | R | Server shall set to FALSE. |
| | | | | **RFOTM** | RW | DOXS shall set to TRUE after secure owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | R | n/a |
| oic.r.doxm | Device owner | devowneruuid | uuid | **RESET** | R | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000" ) |
| | | | | **RFOTM** | RW | DOXS shall set value after secure owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | R | n/a |
| oic.r.doxm | Resource owner | rowneruuid | uuid | **RESET** | R | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000" ) |
| | | | | **RFOTM** | RW | The DOXS should configure the rowneruuid property when a successful owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) 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. |
| oic.r.pstat | Provisioning device state | dos.s | Integer | **RESET** | R | |
| | | | | **RFOTM** | RW | Set by DOXS after successful OTM to RFPRO. |
| | | | | **RFPRO** | RW | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **RFNOP** | RW | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **SRESET** | RW | Set by CMS, AMS, DOXS after successful authentication |
| oic.r.pstat | Is device operational | isop | Boolean | **RESET** | R | Server shall set to FALSE |
| | | | | **RFOTM** | R | Server shall set to FALSE |
| | | | | **RFPRO** | R | Server shall set to FALSE |
| | | | | **RFNOP** | R | Server shall set to TRUE |
| | | | | **SRESET** | R | Server shall set to FALSE |

| | | | | | | |
|---|---|---|---|---|---|---|
| oic.r.pstat | Current provisioning status | cm | oic.sec.dpmtype.bitmask | **RESET** | R | Server shall set to 0000,0001 |
| | | | | **RFOTM** | R | Should be set by DOXS after successful OTM to 00xx,xx10. |
| | | | | **RFPRO** | R | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **RFNOP** | R | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **SRESET** | R | Server shall set to 0000,0001 |
| oic.r.pstat | Target provisioning mode | tm | oic.sec.dpmtype.bitmask | **RESET** | R | Server shall set to 0000,0010 |
| | | | | **RFOTM** | RW | Set by DOXS after successful OTM |
| | | | | **RFPRO** | RW | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **RFNOP** | RW | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **SRESET** | RW | Set by DOXS as needed to recover from failures. Server shall set to XXXX,XX00 upon entry into SRESET. |
| oic.r.pstat | Operational mode | om | oic.sec.pomtype.bitmask | **RESET** | R | Server shall set to manufacturer default. |
| | | | | **RFOTM** | RW | Set by DOXS after successful OTM |
| | | | | **RFPRO** | RW | Set by CMS, AMS, DOXS after successful authentication |
| | | | | **RFNOP** | RW | Set by CMS, AMS, DOXS after successful authentication |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **SRESET** | RW | Set by DOXS. |
| ~~oic.r.pstat~~ | ~~Supported operational modes~~ | ~~sm~~ | ~~oic.sec.pomtype.bitmask~~ | ~~**RESET**~~ | ~~R~~ | ~~Server shall set to manufacturer default~~ |
| | | | | ~~**RFOTM**~~ | ~~R~~ | ~~Set by DOXS after successful OTM~~ |
| | | | | ~~**RFPRO**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFNOP**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**SRESET**~~ | ~~R~~ | ~~n/a~~ |
| ~~oic.r.pstat~~ | ~~Target device ID~~ | ~~deviceuuid~~ | ~~oic.sec.didtype, uuid~~ | ~~**RESET**~~ | ~~R~~ | ~~Server shall set to NULL.~~ |
| | | | | ~~**RFOTM**~~ | ~~RW~~ | ~~Set by DOXS after successful OTM~~ |
| | | | | ~~**RFPRO**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**RFNOP**~~ | ~~R~~ | ~~n/a~~ |
| | | | | ~~**SRESET**~~ | ~~R~~ | ~~n/a~~ |
| oic.r.pstat | Resource owner | rowneruuid | uuid | **RESET** | R | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000" ) |
| | | | | **RFOTM** | RW | The DOXS should configure the /pstat.rowneruuid property when a successful owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) 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. |
| oic.r.cred | List of Credentials | creds | array of oic.r.cred | **RESET** | R | Server shall set to manufacturer defaults. |
| | | | | **RFOTM** | RW | Set by DOXS after successful OTM |
| | | | | **RFPRO** | RW | Set by the CMS (referenced via the /cred.rowneruuid property) after successful authentication. Access to vertical resources is prohibited. |
| | | | | **RFNOP** | R | Access to vertical resources is permitted after a matching ACE is found. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) should evaluate the integrity of and may update creds entries when a secure session is established and the Server and DOXS are authenticated. |
| oic.r.cred | Private credential data | creds.privatedata | oic.sec.privdatatype | **RESET** | - | Server shall set to manufacturer default |
| | | | | **RFOTM** | W | Set by DOXS after successful OTM |
| | | | | **RFPRO** | W | Set by authenticated DOXS or CMS |
| | | | | **RFNOP** | - | Not writable during normal operation. |
| | | | | **SRESET** | W | DOXS may modify to enable transition to RFPRO. |
| oic.r.cred | Resource owner | rowneruuid | uuid | **RESET** | R | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000" ) |
| | | | | **RFOTM** | RW | The DOXS should configure the /cred.owneruuid property when a successful owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) 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. |
| oic.r.acl, oic.r.acl2, oic.r.sacl, oic.r.amacl | List of Access Control Entries (ACE) | aclist, aces, aclist, resources | array of oic.sec.ace, array of oic.sec.ace2, array of oic.sec.ace2, array of oic.sec.ace2.resource-ref | **RESET** | R | Server shall set to manufacturer defaults. |
| | | | | **RFOTM** | RW | Set by DOXS after successful OTM |
| | | | | **RFPRO** | RW | The AMS (referenced via rowneruuid property) shall update the aclist entries after mutually authenticated secure session is established. Access to vertical resources is prohibited. |
| | | | | **RFNOP** | R | Access to vertical resources is permitted after a matching ACE is found. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) should evaluate the integrity of and may update aclist entries when a secure session is established and the Server and DOXS are authenticated. |
| oic.r.acl, oic.r.acl2 | Resource owner | rowneruuid | uuid | **RESET** | R | Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000" ) |
| | | | | **RFOTM** | RW | The DOXS should configure the /acl.rowneruuid and /acl2.rowneruuid property when a successful owner transfer session is established. |
| | | | | **RFPRO** | R | n/a |
| | | | | **RFNOP** | R | n/a |
| | | | | **SRESET** | RW | The DOXS (referenced via /doxm.devowneruuid property) 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. |

| | | | | | | |
|---|---|---|---|---|---|---|
| oic.r.svc | Resource owner | rowneruuid | oic.sec.svctype | RESET | R | Server shall set to NULL. |
| | | | | RFOTM | RW | The DOXS should configure the rowneruuid property when a successful owner transfer session is established. |
| | | | | RFPRO | R | n/a |
| | | | | RFNOP | R | n/a |
| | | | | SRESET | RW | The DOXS (referenced via /doxm.devowneruuid property) 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 X - Device state specific access mode behavior for security resources.

Note: This table is distributed across the various affected tables in section 15.

This applies to Section 8.4 item 5 “The ‘isop’ property of the /oic/sec/pstat resource shall be TRUE.”

Becomes:

“The ‘isop’ property of the /oic/sec/pstat resource remains FALSE.”

This applies to Table 13 at Line 2102.
A new row shall be added with Value Type Name as “OICSelf”; Value Type URN as “oic.sec.oxm.self”; Enumeration Value as (4); Description as “The manufacturer shall set the /doxm.oxmsel value to (4). The Server shall reset this value to (4) upon entering RESET device state.

This applies to Section 13.1 at line 2100.

The device vendor shall determine that the device identifier /doxm.deviceuuid is persistent (not updatable) or that it is non-persistent (updatable by the owner transfer service – a.k.a DOXS).

If /doxm.deviceuuid is persistent, the request to update shall fail with the error PROPERTY_NOT_FOUND.

If it is non-persistent, the request to update shall succeed and the value supplied by DOXS shall be remembered until the device is RESET. If the update fails for any other reason and device state has not transitioned to RESET, the value of /doxm.deviceuuid shall be the nil UUID (e.g. "00000000-0000-0000-0000-000000000000" ).

Regardless of whether the device has a persistent or non-persistent deviceuuid, a temporal random non-repeating UUID is found each time the device enters RESET. The temporal deviceuuid is used while the device state is in the RESET state and while in the RFOTM device state until the DOXS establishes a secure OTM connection.

[1] IETF RFC 6973, *Privacy Considerations for Internet Protocols,* July 2013, https://www.rfc-editor.org/info/rfc6973