OCF "Fargo" – Deprecate persistent or fake Device UUID – Security WG CR 2979/3104

Legal Disclaimer

START OF CHANGE IN CLAUSE 7.1.1

7.1.1 General Device Identity

Each Device, which is a logical device, is identified with a Device ID.

Devices shall be identified by a Device ID value that is established as part of device onboarding. The "/oic/sec/doxm" Resource specifies the Device ID format (e.g. "urn:uuid"). Device IDs shall be unique within the scope of operation of the corresponding OCF Security Domain, and should be universally unique. The DOTS shall ensure Device ID of the new Device is unique within the scope of the owner's OCF Security Domain. The DOTS shall verify the chosen new device identifier does not conflict with Device IDs previously introduced into the OCF Security Domain.

Devices maintain an association of Device ID and cryptographic credential using a "/oic/sec/cred" Resource. Devices regard the "/oic/sec/cred" Resource as authoritative when verifying authentication credentials of a peer device.

A Device maintains its Device ID in the "/oic/sec/doxm" Resource. It maintains a list of credentials, both its own and other Device credentials, in the "/oic/sec/cred" Resource. The device ID can be used to distinguish between a device's own credential, and credentials for other devices. Furthermore, the "/oic/sec/cred" Resource may contain multiple credentials for the device.

When using manufacturer certificates, the certificate should bind the ID to the stored secret in the device as described later in this clause.

A physical Device, referred to as a Platform in OCF documents, may host multiple Devices. The Platform is identified by a Platform ID. The Platform ID shall be globally unique and inserted in the device in an integrity protected manner (e.g. inside secure storage or signed and verified).

An OCF Platform may have a secure execution environment, which shall be used to secure unique identifiers and secrets. If a Platform hosts multiple devices, some mechanism is needed to provide each Device with the appropriate and separate security.

END OF CHANGE

START OF CHANGE IN CLAUSE 13.2

13.2 Device Owner Transfer Resource

13.2.1 Device Owner Transfer Resource General

The "/oic/sec/doxm" Resource contains the set of supported Device OTMs.

Resource discovery processing respects the CRUDN constraints supplied as part of the security Resource definitions contained in this document.

"/oic/sec/doxm" Resource is defined in Table 20.

Table 1 – Definition of the "/oic/sec/doxm" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/doxm	Device OTMs	oic.r.doxm	oic.if.baseline	Resource for supporting Device owner transfer	Configuration

Table 21 defines the Properties of the "/oic/sec/doxm" Resource.

Table 2 – Properties of the "/oic/sec/doxm" Resource

Property Title	Property Name	Value Type	Value Rule	Mandatory	Device State	Access Mode	Description
OTM	oxms	oic.sec.doxmtype	array	Yes		R	Value identifying the owner-transfer-method and the organization that defined the method.
OTM Selection	oxmsel	oic.sec.doxmtype	UINT16	Yes	RESET	R	Server shall set to (4) "oic.sec.oxm.self"
					RFOTM	RW	DOTS shall set to its selected DOTS and both parties execute the DOTS. After secure owner transfer session is established DOTS shall update the oxmsel again making it permanent. If the DOTS fails the Server shall transition device state to RESET.
					RFPRO	R	n/a
					RFNOP	R	n/a
					SRESET	R	n/a
Supported Credential Types	sct	oic.sec.credtype	bitmask	Yes		R	Identifies the types of credentials the Device supports. The Server sets this value at framework initialization after determining security capabilities.
Device Ownership Status	owned	Boolean	T|F	Yes	RESET	R	Server shall set to FALSE.
					RFOTM	RW	DOTS shall set to TRUE after secure owner transfer session is established.
					RFPRO	R	n/a
					RFNOP	R	TRUE
					SRESET	R	TRUE
Device UUID	deviceuuid	String	oic.sec.didtype	Yes	RESET	R	No stipulation
					RFOTM	RW	DOTS updates to a value it has selected after secure owner transfer session is established.
					RFPRO	R	n/a
					RFNOP	R	n/a
					SRESET	R	n/a
Device Owner Id	devowneruuid	String	uuid	Yes	RESET	R	Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000")
					RFOTM	RW	DOTS shall set value after secure owner transfer session is established.

					RFPRO	R	n/a
					RFNOP	R	n/a
					SRESET	R	n/a
Resource Owner Id	rowneruuid	String	uuid	Yes	RESET	R	Server shall set to the nil uuid value (e.g. "00000000-0000-0000-0000-000000000000")
					RFOTM	RW	The DOTS shall configure the rowneruuid Property when a successful owner transfer session is established.
					RFPRO	R	n/a
					RFNOP	R	n/a
					SRESET	RW	The DOTS (referenced via 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 DOTS device identifier the Server shall transition to RESET Device state.

Table 22 defines the Properties of the "oic.sec.didtype".

Table 3 – Properties of the "oic.sec.didtype" type

Property Title	Property Name	Value Type	Value Rule	Mandatory	Device State	Access Mode	Description
Device ID	uuid	String	uuid	Yes	RW	-	A uuid value

The oxms Property contains a list of OTM where the entries appear in the order of preference. This Property contains the higher priority methods appearing before the lower priority methods. The DOTS queries this list at the time of onboarding and selects the most appropriate method.

OTMs consist of two parts, a URI identifying the vendor or organization and the specific method.

```
<DoxmType> ::= <NSS>
<NSS> ::= <Identifier> | {{<NID>"."} <NameSpaceQualifier> "."} <Method>
<NID> :: = <Vendor-or-Organization>
<Identifier> ::= INTEGER
<NameSpaceQualifier> ::= String
<Method> ::= String
<Vendor-Organization> ::= String
```

When an OTM successfully completes, the "owned" Property is set to "1" (TRUE). Consequently, subsequent attempts to take ownership of the Device will fail.

There are four device identifiers

1) "deviceuuid" Property of "/oic/sec/doxm" - random DOTS-provisioned value unique for a given security domain, used as a device identity for access control, mapped internally to a device-owned credential
2) "di" Property of "/oic/d" - mirroring the value of "deviceuuid" Property of "/oic/sec/doxm"
3) "piid" Property of "/oic/d" - defined in [CoreSpec].
4) "pi" Property of "/oic/p"- defined in [CoreSpec].

END OF CHANGE

START OF CHANGE IN CLAUSE 13.8

13.8 Provisioning Status Resource

…

When Device state is RFOTM:

– NCRs are inaccessible.
– Before OTM is successful, the "s" Property of "/oic/sec/dostype" Resource is read-only by unauthenticated requestors

END OF CHANGE

START OF CHANGE IN CLAUSE 13.16

13.16 Additional Privacy Consideration for Core Resources

Unique immutable identifiers are a privacy consideration due to their potential for being used as a tracking mechanism. These include the following Resources and Properties:

– "/oic/d" Resource containing the "piid" Property.
– "/oic/p" Resource containing the "pi" Property.

These identifiers are unique values that are visible at various times throughout the Device lifecycle by anonymous requestors. This implies any Client Device, including those with malicious intent, are able to reliably obtain identifiers useful for building a log of activity correlated with a specific Platform and Device.

The "di" Property in the "/oic/d" Resource shall mirror that of the deviceuuid Property of the "/oic/sec/doxm" Resource. The DOTS should provision an ACL policy that restricts access to the "/oic/d" resource such that only authenticated Clients are able to obtain the "di" Property of "/oic/d" Resource. See clause 13.1 for deviceuuid Property lifecycle requirements.

Servers should expose a temporary, non-repeated, piid Property of "/oic/d" Resource Value upon entering RESET Device state. Servers shall expose a persistent value via the "piid" Property of "/oic/d" Property when the DOTS sets "devowneruuid" Property to a non-nil-UUID value. The DOTS should provision an ACL policy on the "/oic/d" Resource such that only authenticated Clients are able to obtain the "piid" Property of "/oic/d" Resource.

Servers should expose a temporary, non-repeated, "pi" Property value upon entering RESET Device state. Servers shall expose a persistent value via the "pi" Property of the "/oic/p" Resource when the DOTS sets "devowneruuid" Property to a non-nil-UUID value. The DOTS should provision an ACL policy on the "/oic/p" Resource such that only authenticated Clients are able to obtain the "pi" Property.

Table 55 depicts Core Resource Properties Access Modes given various Device States.

Table 4 – Core Resource Properties Access Modes given various Device States

Resource Type	Property title	Property name	Value type	Access Mode		Behaviour
oic.wk.p	Platform Identifier	pi	oic.types-schema.uuid	All States	R	Server exposes a temporary random UUID when in RESET state.
oic.wk.d	Permanent Immutable Identifier	piid	oic.types-schema.uuid	All States	R	Server exposes a temporary random UUID when in RESET state.
oic.wk.d	Device Identifier	di	oic.types-schema.uuid	All states	R	/d di mirrors the value contained in "/doxm" deviceuuid in all device states.

END OF CHANGE