

OCF “Ipanema” – DOXM support for multicast and query using "owned" is not documented nor in schemas – Security WG CR 2640

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 © 2020 Open Connectivity Foundation, Inc. All rights reserved.

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

DRAFT

***** **Changes to clause 7.3.1** *****

7.3.1 OTM implementation requirements

This document provides specifications for several methods for ownership transfer. Implementation of each individual ownership transfer method is considered optional. However, each device shall implement at least one of the ownership transfer methods not including vendor specific methods.

All OTMs included in this document are considered optional. Each vendor is required to choose and implement at least one of the OTMs specified in this document. The OCF, does however, anticipate vendor-specific approaches will exist. Should the vendor wish to have interoperability between a vendor-specific OTM and OBTs from other vendors, the vendor must work directly with OBT vendors to ensure interoperability. Notwithstanding, standardization of OTMs is the preferred approach. In such cases, a set of guidelines is provided in 7.3.7 to help vendors in designing vendor-specific OTMs.

The "/oic/sec/doxm" Resource is extensible to accommodate vendor-defined owner transfer methods (OTM). The DOTS determines which OTM is most appropriate to onboard the new Device. All OTMs shall represent the onboarding capabilities of the Device using the "oxms" Property of the "/oic/sec/doxm" Resource. The DOTS determines the Device's supported credential types using the Supported Credential Types "sct" Property of the "/oic/sec/doxm" Resource. The DOTS and CMS provision credentials according to the credential types supported.

Figure 9 depicts new Device discovery sequence.

```
@startuml
title Token sequence
autonumber
skinparam BoxPadding 20

participant "DOTS\n(UUID B0Bxxxxx-...)" as DOTS
participant "DOTS\n(UUID A71C3xxx-...)" as NewD

group Discover New Devices.
    note over DOTS, NewD
        Find new devices that are unowned (that is, in RFOTM state)
    end note
    DOTS->>NewD: Unsecured RETRIEVE "oic/sec/doxm" (optionally multicast)
    NewD->>DOTS: RSP {...,"oxms":{0,1,2,...}, "owned":FALSE, "deviceuuid":<manufacturer
default> ...}
end

@enduml
```

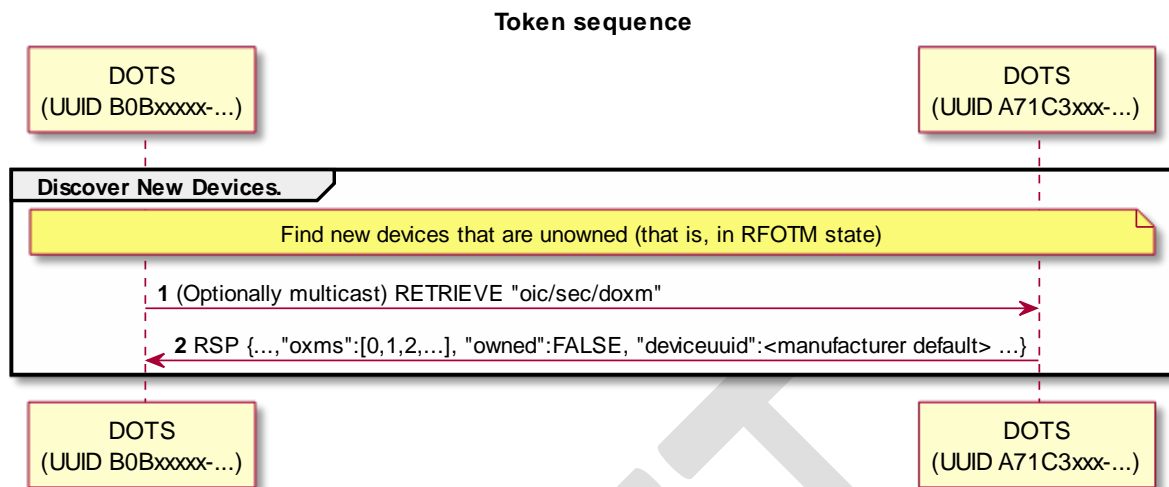


Figure 1 – Discover New Device Sequence

Table 1 – Discover New Device Details

Step	Description
1	The OBT queries to see if the new device is not yet owned.
2	The new device returns the "/oic/sec/doxm" Resource containing ownership status and supported OTMs. It also contains a temporal device ID that may change subsequent to successful owner transfer. The device should supply a temporal ID to facilitate discovery as a guest device. Clause 7.3.9 provides security considerations regarding selecting an OTM.

A Device shall support selective use of unsecured multicast to receive RETRIEVE requests to the Device "/oic/sec/doxm" Resource, as shown in Figure 9. Clause 10.4 of the **Core Framework** provides the generic details for using CoAP multicast requests in OCF. Multicast retrieval of the "/oic/sec/doxm" Resource supports filtering using the "owned" query parameter. When a multicast RETRIEVE request omits the "owned" query parameter or includes the "owned" query parameter set to "false", then the Device shall respond only if the Device is in RFOTM and there is no open Device Onboarding Connection. Otherwise the request shall be ignored by the Device, regardless of ACE configuration.

Vendor-specific device OTMs shall adhere to the "/oic/sec/doxm" Resource Specification for OCs that results from vendor-specific device OTM. Vendor-specific OTMs should include provisions for establishing trust in the new Device by the OBT an optionally establishing trust in the OBT by the new Device.

***** **End of Change** *****

***** **Append to end of clause 13.2.1** *****

See 13.16 for additional details related to privacy sensitive considerations.

The "/oic/sec/doxm" Resource supports CoAP multicast requests in certain cases. For details see clause 7.3.1.

***** End of Change *****

DRAFT