TTC仕様書
Technical Specification

TS-M2M-0024v3.2.2

oneM2M 技術仕様書
OCF とのインタワーク

oneM2M Technical Specification
oneM2M and OCF Interworking

2019 年 06 月 28 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Telecommunication
Technology
Committee

TS-M2M-0024v3.2.2

oneM2M 技術仕様書－OCF とのインタワーク [oneM2M Technical Specification - oneM2M and OCF Interworking]

＜参考＞ [Remarks]

１．英文記述の適用レベル [Application level of English description]

適用レベル [Application level]：E2

本標準の本文、付属資料および付録の文章および図に英文記述を含んでいる。

[English description is included in the text and figures of main body, annexes and appendices.]

２．国際勧告等の関連 [Relationship with international recommendations and standards]

本標準は、oneM2M で承認された Technical Specification 0024V3.2.2 に準拠している。

[This standard is standardized based on the Technical Specification 0024 (V3.2.2) approved by oneM2M.]

３．上記国際勧告等に対する追加項目等 [Departures from international recommendations]

原標準に対する変更項目 [Changes to original standard]

原標準が参照する標準のうち、TTC 標準に置き換える項目。

[Standards referred to in the original standard, which are replaced by TTC standards.]

原標準が参照する標準のうち、それらに準拠した TTC 標準等が制定されている場合は自動的に最新版 TTC 標準等に置き換え参照するものとする。

[Standards referred to in the original standard should be replaced by derived TTC standards.]

４．工業所有権 [IPR]

本標準に関わる「工業所有権等の実施の権利に係る確認書」の提出状況は、ＴＴＣホームページによる。

[Status of “Confirmation of IPR Licensing Condition” submitted is provided in the TTC web site.]

５．作成専門委員会 [Working Group]

oneM2M 専門委員会 [oneM2M Working Group]

ONEM2M
TECHNICAL SPECIFICATION

Document Number	TS-0024-V3.2.2
Document Name:	OCF Interworking
Date:	2019-04-18
Abstract:	This document specifies details on interworking between oneM2M-specified entities and OCF-specified clients and/or servers.

Template Version: 08 September 2015 (Dot not modify)

This Specification is provided for future development work within oneM2M only. The Partners accept no liability for any use of this Specification.

The present document has not been subject to any approval process by the oneM2M Partners Type 1. Published oneM2M specifications and reports for implementation should be obtained via the oneM2M Partners' Publications Offices.

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

Copyright Notification

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. NO oneM2M PARTNER TYPE 1 SHALL BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY THAT PARTNER FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL oneM2M BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. oneM2M EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Contents

1 Scope

The present document specifies the detailed methods for oneM2M and OCF interworking using the architecture identified in oneM2M TS-0033 [5] and annex F of oneM2M TS-0001 [2] for the following scenario:

- Interworking with full mapping of the semantics of the non-oneM2M data model to Mca, see scenario number 1 listed in clause F.2 of oneM2M TS-0001 [2]. This is also in line with the interworking concepts specified in oneM2M TS-0033 [5].

This interworking scenario allows for interworking between OCF devices and oneM2M entities purely based on the common understanding of aligned information models - such as the models defined in oneM2M TS-0023 [6]. There is no limitation regarding the direction of exposure of services: Services provided by OCF devices (OCF servers) can be exposed to oneM2M entities or vice versa. The oneM2M entities do not need to be aware of any details of the OCF protocols or interfaces.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[1] oneM2M TS-0011: "Common Terminology".

[2] oneM2M TS-0001: "Functional Architecture".

[3] Void.

[4] oneM2M TS-0003: "Security solutions".

[5] oneM2M TS-0033: "Interworking Framework".

[6] oneM2M TS-0023: "Home Appliances Information Model and Mapping".

[7] OCF-Core-Specification-V2.0.0.

NOTE: Available at https://openconnectivity.org/specs/OCF_Core_Specification_v2.0.0.pdf.

[8] OCF Device-Specification-V2.0.0.

NOTE: Available at https://openconnectivity.org/specs/OCF_Device_Specification_v2.0.0.pdf.

[9] OCF Security-Specification-V2.0.0.

NOTE: Available at https://openconnectivity.org/specs/OCF_Security_Specification_v2.0.0.pdf.

[10] OCF Bridging-Specification-V1.3.0.

NOTE: Available at https://openconnectivity.org/specs/OCF_Bridging_Specification_v1.3.0.pdf.

[11] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in oneM2M TS-0011 [1], oneM2M TS-0001 [2] and oneM2M TS-0033 [5] apply:

OCF Client: logical entity that accesses a Resource on an OCF Server

OCF Device: logical entity that assumes one or more roles (e.g. OCF Client, OCF Server)

OCF Framework: set of related functionalities and interactions defined in the OCF Core Specification [7], which enable interoperability across a wide range of networked devices, including the Internet of Things

OCF-IPE: IPE providing interworking functions for OCF-oneM2M interworking

OCF Physical Entity: aspect of the physical world that is exposed through an OCF Device

NOTE: An example of an OCF Physical Entity is a LED.

OCF Platform: physical device containing one or more Devices

OCF Resource: represents an OCF Entity modelled and exposed by the OCF Framework

OCF Server: OCF Device with the role of providing access to OCF Resource state information and facilitating remote interaction with those resources

OCF Functions: services or Device information provided by one or more OCF Servers by exposing access to OCF Resources via OCF-specified interfaces

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in oneM2M TS-0011 [1], oneM2M TS-0001 [2] and oneM2M TS-0033 [5].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACP	Access Control Policy
AE	Application Entity
AE-ID	Application Entity IDentifier
CBOR	Concise Binary Object Representation
CMDH	Communication Management and Delivery Handling
CSE	Common Services Entity
IPE	Interworking Proxy Entity
JSON	JavaScript Object Notation
OIC	Open Interconnect Consortium
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 Introduction to OCF interworking

OCF specifies an architecture enabling resource-based interactions among OCF Devices, see OCF-Core-Specification-V1.0.0 [7]. OCF Devices can expose aspects of the physical world like a lightbulb and/or logical entities like an application. The OCF Devices in the OCF architecture can provide services - in that case they play the role of an OCF Server - and/or consume services - in that case they play the role of an OCF Client.

The present document specifies details of the interworking with OCF Devices on the information model layer, see oneM2M TS-0033 [5], and the implications on how to represent and execute external OCF functions with means of resource instances in the oneM2M system and vice versa.

Service provided and/or consumed on either side (OCF versus oneM2M) are represented by resources hosted by service providers (OCF Servers or oneM2M CSEs) and accessible to service consumers (OCF Clients or oneM2M AEs/CSEs). In order to support seamless interworking across boundaries of OCF & oneM2M deployments, OCF and oneM2M have aligned several information models for such services so that they became technology agnostic. Definitions of such information models are contained in the following specifications:

- oneM2M TS-0023 [6].
- OCF Device-Specification-V1.3.0 [8].

In the remainder of the present document it is assumed that mutual exposure of services between oneM2M and OCF deployments is restricted to services represented by resource types defined in these specifications.

In line with oneM2M TS-0033 [5], the present document specifies two major directions of mutual OCF/oneM2M interworking:

- Expose OCF Functions provided by OCF Servers to oneM2M entities by using one or more OCF-IPE(s) which are acting as OCF Client(s). For this direction - OCF services exposed to oneM2M - the OCF-IPE(s) are creating and managing the oneM2M resources representing exposed services provided by OCF Servers and provide the required procedures to allow consumption of OCF services on the oneM2M side. Details on this exposure direction are specified in clause 6.1 of the present document.
- Expose services provided by oneM2M entities by using one or more OCF-IPE(s) which are acting as OCF Server(s). For this direction - oneM2M services provided to OCF - the OCF-IPE(s) are interacting with already created oneM2M resource representations that are offering the native oneM2M services and provide the required procedures to allow consumption of the oneM2M services on the OCF side. Details on this exposure direction are specified in clause 6.1 of the present document.

While it is possible that a single OCF-IPE can simultaneously support exposure of OCF Functions to oneM2M and exposure of oneM2M services to OCF, it is not mandated to implement OCF-IPEs in that way. It is also possible to instantiate separate OCF-IPEs for the different exposure directions. This is an implementation choice. In case that exposure in one direction needs to be correlated with a different Service Subscription Profile than for the other direction, separate OCF-IPEs are required. Details on the representation of OCF Functions by oneM2M Resources are defined in clause 7 of the present document.

6 OCF interworking architecture

6.1 Exposure of OCF Functions to the oneM2M System

6.1.1 Summary of Interworking Architecture for exposure of OCF Functions

An OCF-IPE exposing OCF Functions to the oneM2M System is responsible for the creation of oneM2M Resources representing the exposed OCF Functions on its own Registrar CSE. A single OCF-IPE may expose OCF Functions provided by one or more OCF Servers to the oneM2M System. A high-level summary of the relationship of OCF Servers providing OCF Functions to be exposed to oneM2M, one or more OCF-IPE(s) and sets of oneM2M Resources representing the exposed OCF Functions is depicted in figure 6.1.1-1.

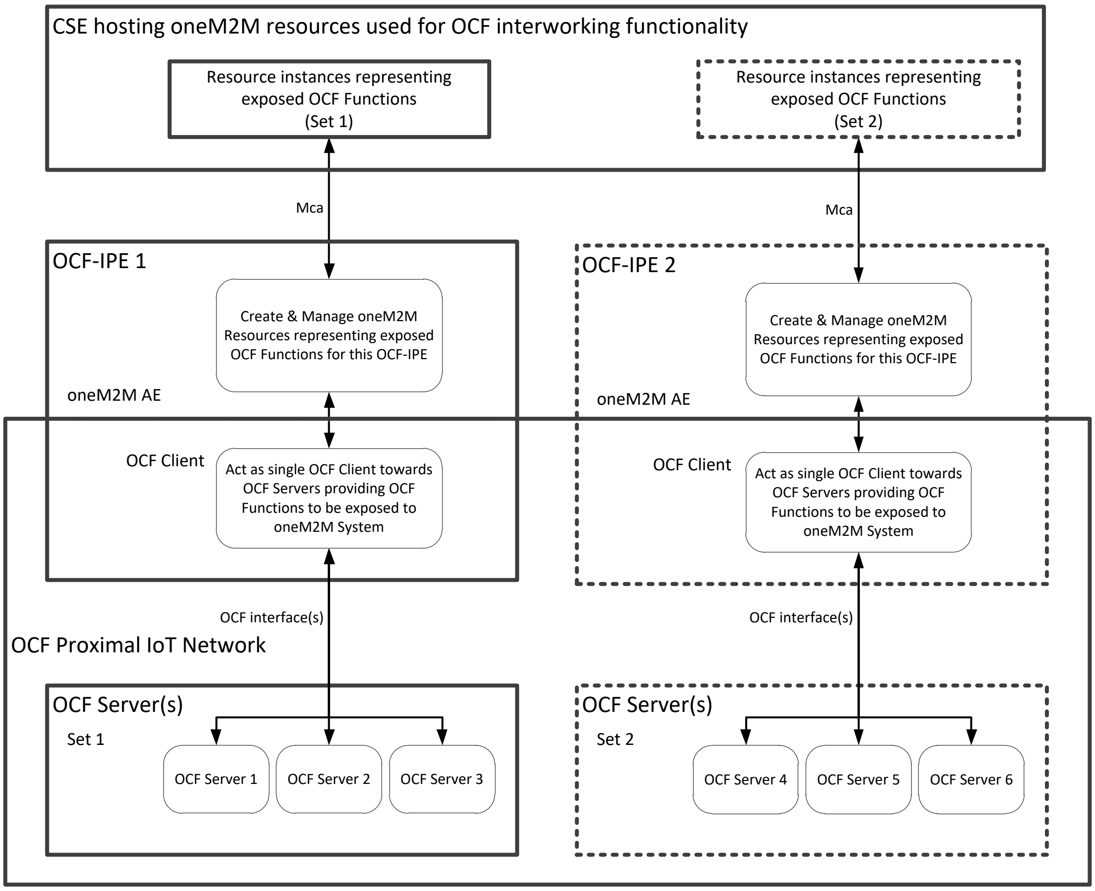

CSE hosting oneM2M resources used for OCF interworking functionality
Resource instances representing exposed OCF Functions (Set 1)
Resource instances representing exposed OCF Functions (Set 2)
Mca
Mca
OCF-IPE 1
OCF-IPE 2
Create & Manage oneM2M Resources representing exposed OCF Functions for this OCF-IPE
Create & Manage oneM2M Resources representing exposed OCF Functions for this OCF-IPE
oneM2M AE
oneM2M AE
OCF Client
OCF Client
Act as single OCF Client towards OCF Servers providing OCF Functions to be exposed to oneM2M System
Act as single OCF Client towards OCF Servers providing OCF Functions to be exposed to oneM2M System
OCF interface(s)
OCF interface(s)
OCF Proximal IoT Network
OCF Server(s)
Set 1
OCF Server 1
OCF Server 2
OCF Server 3
OCF Server(s)
Set 2
OCF Server 4
OCF Server 5
OCF Server 6

Figure 6.1.1-1: Summary of Interworking Architecture for Exposure OCF → oneM2M

More than one OCF-IPE may be instantiated for exposure of multiple non-overlapping sets of OCF Functions to the oneM2M System. In particular, if OCF Functions provided by different sets of OCF Servers shall be exposed to the oneM2M System and there is a deployment requirement to differentiate sets of OCF Functions provided by different OCF Servers - e.g. for the purpose of correlating them with different Service Subscription Profiles - then instantiating more than one OCF-IPE is required. Further details on the implications using more than one OCF-IPE for exposure of OCF Functions to the oneM2M System are defined in clause 7.1.

A specific instance of an OCF-IPE exposing OCF Functions to the oneM2M System shall play the role of a single OCF Client on the OCF side. If there is a deployment requirement to differentiate multiple OCF Clients who act as interworking proxies for exposing a common set of OCF Functions to the oneM2M System - for instance due to the need to assign different access control properties to them on the OCF side - then the OCF-IPE exposing those OCF Functions would need to play the role of multiple OCF Clients. However, mapping rules between the identifiers of Originators on the oneM2M side who attempt to consume the exposed OCF Functions and OCF Client identifiers to use for triggering the execution of the exposed OCF Functions on the OCF side are not specified in the present document. Therefore, it is assumed that each OCF-IPE is only playing the role of a single OCF Client on the OCF side. This restriction implies that all requests originating from oneM2M entities which are successfully modifying the corresponding oneM2M Resources and then get translated by a specific OCF-IPE to the corresponding interactions with OCF Servers are treated on the OCF side as coming from one single OCF Client and, therefore, will be handled by OCF Servers with the same access control properties, irrespective of the identifier of the Originator on the oneM2M side. However, by means of setting appropriate Access Control Privileges on the oneM2M side, it is certainly possible to define which entities on the oneM2M side will get which mode of access to the exposed OCF services. Support of multiple OCF Clients for a single OCF-IPE is for further study and might be subject of future releases of the present document.

After creation of oneM2M Resources representing exposed OCF Functions by a specific OCF-IPE, this particular OCF-IPE is also responsible for monitoring relevant parts of these created resources in order to detect any operations that need to be translated into an execution of corresponding OCF Functions. In case such an operation on the previously created oneM2M Resources gets detected, the corresponding Function on the OCF side shall be executed by the OCF-IPE.

State changes within the OCF Functions exposed by a specific OCF-IPE to the oneM2M System that are impacting the state of the corresponding oneM2M Resources which were previously created by that specific OCF-IPE need to be monitored on the OCF side and shall be translated by that specific OCF-IPE into corresponding state changes of the associated oneM2M Resources.

6.1.2 OCF-IPE Responsibilities to support exposure of OCF Functions to the oneM2M System

When exposing OCF Functions to the oneM2M System, an OCF-IPE shall be responsible to support the following procedures:

1) Determination of OCF Functions to be exposed to the oneM2M System
The OCF-IPE needs to determine which OCF Functions need to be exposed to the oneM2M System. This determination can be done in different ways (e.g. through provisioning, discovery, on-demand signalling, or combinations thereof). Further details of this procedure are defined in clause 8.1.1.

2) Creation/Deletion of oneM2M Resource representing exposed OCF Functions
The OCF-IPE needs to perform creation/deletion of resource instances representing OCF Functions according to the - possibly dynamically changing - need to expose them to the oneM2M System using resource types that are have been aligned between oneM2M and OCF in order to become technology independent. Further details on this procedure are defined in clause 8.1.2 Resource types that meet the requirement to be technology agnostic between OCF and oneM2M are defined in:

    - OCF Device-Specification [8] and oneM2M TS-0023 [6].

3) Mirroring state of exposed OCF Functions in oneM2M Resources
An OCF-IPE exposing OCF Functions provided by OCF Servers is responsible to modify the resource instances it has created in order to represent the exposed OCF Functions according to any state changes occurring in the corresponding OCF Servers. This implies that such an OCF-IPE shall monitor the state of the associated OCF Servers and upon detection of OCF Server state changes relevant for the exposed OCF Functions the OCF-IPE shall modify the previously created oneM2M Resources accordingly. Further details on this procedure are defined in clause 8.1.3.

4) Detection of requests to execute OCF Functions and invocation thereof
The OFC-IPE is responsible for monitoring relevant changes in the resource instances it has previously created for the purpose of representing the exposed OCF Functions. Upon detection of any valid operation meant to trigger the execution of the exposed OCF Functions, the OCF-IPE is responsible for the invocation of the corresponding OCF Functions via its own OCF Client. Further details of this procedure are defined in clause 8.1.4.

The set of responsibilities of the OCF-IPE when exposing OCF Functions to the oneM2M system is summarized in figure 6.1.2-1. The dashed boxes describe optional/alternative means to determine the set of exposed OCF Functions. Note that, in this figure one OCF-IPE is responsible for all interworking procedures to support exposure of OCF Functions to oneM2M. More than one OCF-IPE may be used to expose different sets of OCF Functions to oneM2M. Details on how to map exposed OCF Function into oneM2M Resources are defined in clause 7.

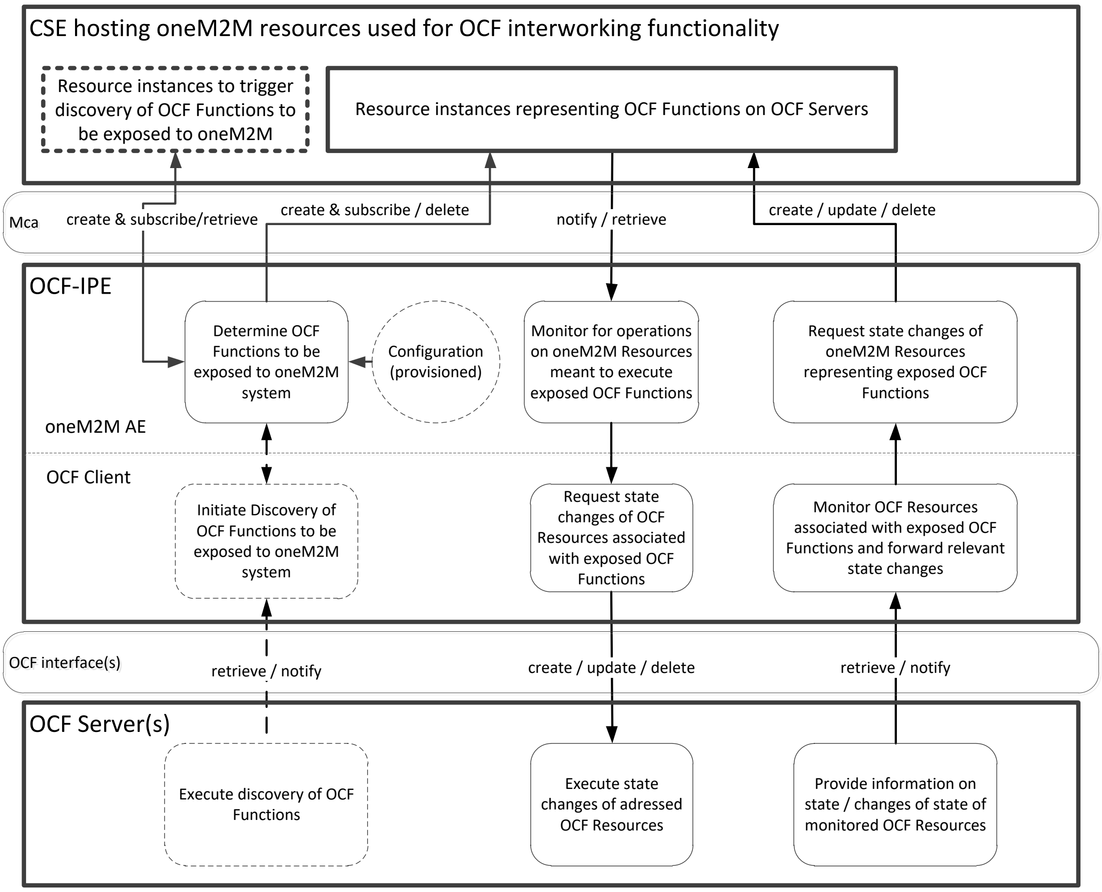

CSE hosting oneM2M resources used for OCF interworking functionality
Resource instances to trigger discovery of OCF Functions to be exposed to oneM2M
Resource instances representing OCF Functions on OCF Servers
Mca
create & subscribe/retrieve
create & subscribe / delete
notify / retrieve
create / update / delete
OCF-IPE
Determine OCF Functions to be exposed to oneM2M system
Configuration (provisioned)
Monitor for operations on oneM2M Resources meant to execute exposed OCF Functions
Request state changes of oneM2M Resources representing exposed OCF Functions
oneM2M AE
OCF Client
Initiate Discovery of OCF Functions to be exposed to oneM2M system
Request state changes of OCF Resources associated with exposed OCF Functions
Monitor OCF Resources associated with exposed OCF Functions and forward relevant state changes
OCF interface(s)
retrieve / notify
create / update / delete
retrieve / notify
OCF Server(s)
Execute discovery of OCF Functions
Execute state changes of adressed OCF Resources
Provide information on state / changes of state of monitored OCF Resources

Figure 6.1.2-1: Exposure of OCF Functions to the oneM2M System

6.2 Exposure of native oneM2M services to an OCF Proximal IoT Network

6.2.1 Summary of Interworking Architecture for exposure of native oneM2M services

An OCF-IPE exposing oneM2M services to an OCF Proximal IoT Network is responsible for the creation of OCF Server instances in the OCF Proximal IoT Network representing the exposed oneM2M services. A single OCF-IPE may expose one or more oneM2M services to the OCF Proximal IoT Network. A high-level summary of the relationship of oneM2M Resources providing the services to be exposed to the OCF Proximal IoT Network, one or more OCF-IPE(s) and sets of OCF Servers representing the exposed oneM2M services is depicted in figure 6.2.1-1.

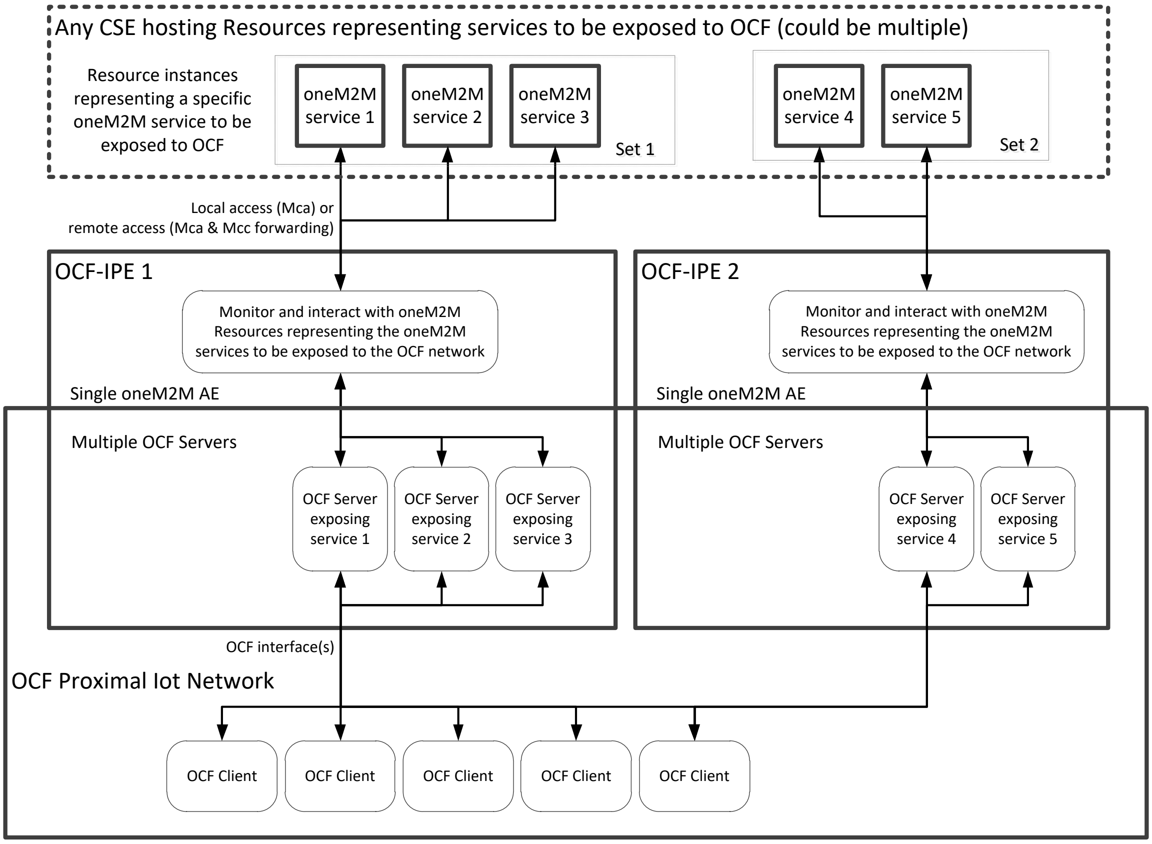

Any CSE hosting Resources representing services to be exposed to OCF (could be multiple)
Resource instances representing a specific oneM2M service to be exposed to OCF
oneM2M service 1
oneM2M service 2
oneM2M service 3
Set 1
oneM2M service 4
oneM2M service 5
Set 2
Local access (Mca) or remote access (Mca & Mcc forwarding)
OCF-IPE 1
Monitor and interact with oneM2M Resources representing the oneM2M services to be exposed to the OCF network
Single oneM2M AE
Multiple OCF Servers
OCF Server exposing service 1
OCF Server exposing service 2
OCF Server exposing service 3
OCF-IPE 2
Monitor and interact with oneM2M Resources representing the oneM2M services to be exposed to the OCF network
Single oneM2M AE
Multiple OCF Servers
OCF Server exposing service 4
OCF Server exposing service 5
OCF interface(s)
OCF Proximal Iot Network
OCF Client
OCF Client
OCF Client
OCF Client
OCF Client

Figure 6.2.1-1: Summary of Interworking Architecture for Exposure oneM2M → OCF

More than one OCF-IPE may be instantiated for exposure of multiple non-overlapping sets of oneM2M services to the OCF Proximal IoT Network. In particular, if there is a deployment requirement to differentiate the exposure of different sets of oneM2M services - e.g. for the purpose of correlating them with different Service Subscription Profiles - then instantiating more than one OCF-IPE is required. Further details on the implications using more than one OCF-IPE for exposure of oneM2M services to the OCF Proximal IoT Network are defined in clause 7.1.

A specific oneM2M service shall only be exposed to a given OCF Proximal IoT Network by at most one instance of an OCF-IPE connected to that OCF Proximal IoT Network. If there is a deployment requirement to differentiate multiple AE instances who act as interworking proxies on behalf of OCF Clients for exposing a common set of oneM2M services to the OCF Proximal IoT Network - for instance due to the need to assign different access control privileges to them on the oneM2M side - then the exposure of that common set of oneM2M services would require multiple instances of OCF-IPEs with a shared set of OCF Servers exposing the same set of oneM2M services to a given OCF Proximal IoT Network. However, mapping rules between the identifiers of OCF Clients who attempt to consume the exposed oneM2M services and the respective OCF-IPE AE-IDs to use for triggering the execution of the exposed oneM2M services are not specified in the present document. Therefore, it is assumed that each exposed oneM2M service is only interacting with one OCF-IPE for a given OCF Proximal IoT Network. This restriction implies that all requests originating from OCF Clients received by any of the OCF Servers instantiated by a given OCF-IPE which are meant to be translated by the OCF-IPE to the corresponding operations on oneM2M Resources representing the exposed oneM2M services are treated on the oneM2M side as coming from one single oneM2M AE and, therefore, will be handled by oneM2M CSEs with the same access control privileges, irrespective of the identifier of the requesting OCF Client. However, by means of setting appropriate access control properties on the OCF side - i.e. access control governing the acceptance or requests at the OCF Servers instantiated by the OCF-IPE - it is certainly possible to define which OCF Client will get which mode of access to the exposed oneM2M services. Therefore, access control can be imposed on OCF Client basis if the appropriate access control properties are provisioned properly into the OCF Servers instantiated by the OCF-IPE. Support of multiple OCF-IPEs exposing the same set of oneM2M services is for further study and might be subject of future releases of the present document.

After creation of OCF Server instances representing the exposed oneM2M services by a specific OCF-IPE, this particular OCF-IPE is also responsible for monitoring incoming OCF Client requests reaching these created OCF Servers in order to detect any requests that need to be translated into a corresponding operation on oneM2M Resources representing the exposed oneM2M services. In case such an request directed to the previously created OCF Servers gets detected, the corresponding operation(s) on the oneM2M side shall be executed by the OCF-IPE.

State changes within the oneM2M Resources representing the oneM2M services exposed to the OCF Proximal IoT Network by a specific OCF-IPE that are impacting the state of the corresponding resources on any of the OCF Servers that were previously created by that specific OCF-IPE need to be detected on the oneM2M side and shall be translated by that specific OCF-IPE into corresponding state changes of the associated resources in the OCF Servers.

6.2.2 OCF-IPE Responsibilities to support exposure of oneM2M services to an OCF Proximal IoT Network

When exposing oneM2M services to an OCF Proximal IoT Network, an OCF-IPE shall be responsible to support the following procedures:

1) Determination of oneM2M services to be exposed to the OCF Proximal IoT Network.
The OCF-IPE needs to determine which oneM2M services need to be exposed to the OCF Proximal IoT Network. This determination can be done in different ways (e.g. through provisioning, discovery, on-demand signalling, or combinations thereof). Further details of this procedure are defined in clause 8.2.1.

2) Instantiation/removal of OCF Servers representing exposed oneM2M services.
The OCF-IPE needs to perform instantiation/removal of OCF Server instances representing oneM2M services according to the - possibly dynamically changing - need to expose them to the OCF Proximal IoT Network using OCF Servers hosting OCF resource types that are have been aligned between oneM2M and OCF in order to become technology independent. Further details on this procedure are defined in clause 8.2.2. OCF resource types and equivalent oneM2M resource types that meet the requirement to be technology agnostic between OCF and oneM2M are defined in:

   - oneM2M TS-0023 [6] and OCF Device-Specification-V1.3.0 [8].

3) Mirroring state of oneM2M Resources representing exposed oneM2M services in OCF resources hosted on OCF Servers.
An OCF-IPE exposing oneM2M services to an OCF Proximal IoT Network is responsible to modify the resource instances in the OCF Servers it has instantiated in order to represent the exposed oneM2M services according to any state changes occurring in the corresponding oneM2M Resources. This implies that such an OCF-IPE shall monitor the state of the associated oneM2M Resources and upon detection of oneM2M Resource state changes relevant for the exposed oneM2M services, the OCF-IPE shall modify the corresponding resource state of OCF resources hosted in the previously instantiated OCF Servers accordingly. Further details on this procedure are defined in clause 8.2.3.

4) Detection of requests to consume exposed oneM2M services and execution thereof.
The OFC-IPE is responsible for monitoring relevant changes in the resources hosted by the OCF Servers the OCF-IPE has previously instantiated for the purpose of representing the exposed oneM2M services. Upon detection of any valid operation on the OCF side meant to trigger the consumption of the associated exposed oneM2M services, the OCF-IPE is responsible for the requesting the corresponding oneM2M operation on the oneM2M Resources representing the exposed oneM2M service to be consumed. Further details of this procedure are defined in clause 8.2.4.

The set of responsibilities of the OCF-IPE when exposing oneM2M services to an OCF Proximal IoT Network is summarized in figure 6.2.2-1. The dashed boxes describe optional/alternative means to determine the set of exposed oneM2M services. Note that, in this figure one OCF-IPE is responsible for all interworking procedures to support exposure of oneM2M services to an OCF Proximal IoT Network. More than one OCF-IPE may be used to expose different sets of oneM2M services to the same OCF Proximal IoT Network. Details on how to map exposed oneM2M services into OCF resources are defined in clause 7.

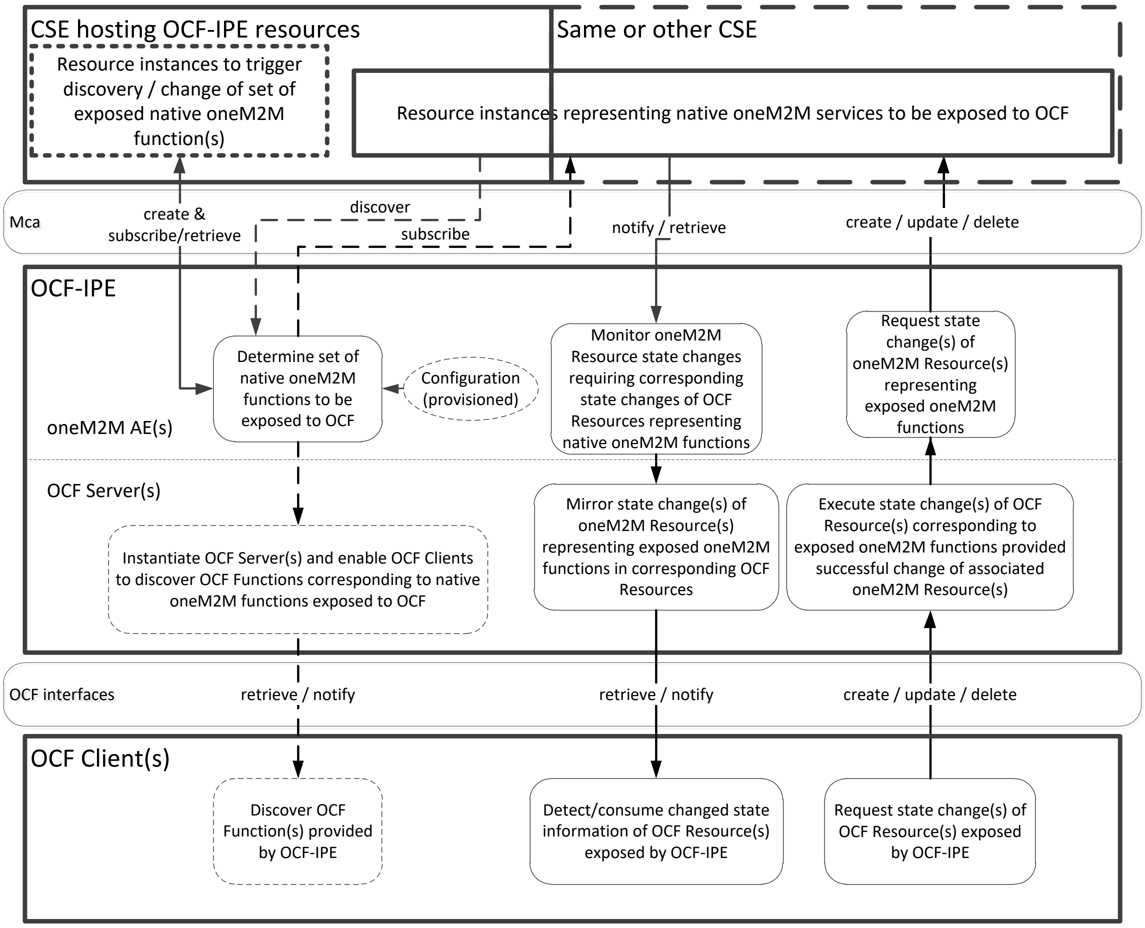

CSE hosting OCF-IPE resources
Same or other CSE
Resource instances to trigger discovery / change of set of exposed native oneM2M function(s)
Resource instances representing native oneM2M services to be exposed to OCF
Mca
create & subscribe/retrieve
discover
subscribe
notify / retrieve
create / update / delete
OCF-IPE
oneM2M AE(s)
Determine set of native oneM2M functions to be exposed to OCF
Configuration (provisioned)
Monitor oneM2M Resource state changes requiring corresponding state changes of OCF Resources representing native oneM2M functions
Request state change(s) of oneM2M Resource(s) representing exposed oneM2M functions
OCF Server(s)
Instantiate OCF Server(s) and enable OCF Clients to discover OCF Functions corresponding to native oneM2M functions exposed to OCF
Mirror state change(s) of oneM2M Resource(s) representing exposed oneM2M functions in corresponding OCF Resources
Execute state change(s) of OCF Resource(s) corresponding to exposed oneM2M functions provided successful change of associated oneM2M Resource(s)
OCF interfaces
retrieve / notify
retrieve / notify
create / update / delete
OCF Client(s)
Discover OCF Function(s) provided by OCF-IPE
Detect/consume changed state information of OCF Resource(s) exposed by OCF-IPE
Request state change(s) of OCF Resource(s) exposed by OCF-IPE

Figure 6.2.2-1: Exposure of native oneM2M functions to the OCF Proximal IoT Network

7 Representation of OCF and/or oneM2M functions

7.1 Representation of OCF functions by oneM2M resources

7.1.1 Representation of OCF Devices by oneM2M <*node*> resources

An OCF Device which provides functions that are exposed to the oneM2M system can be represented by a oneM2M <*node*> resource that contains device-specific information which can be used e.g. for the purpose of device management. Whether a specific OCF device shall be represented by a oneM2M <*node*> resource depends on the type of device:

- OCF Devices providing services that are exposed to the oneM2M system using specializations of <*flexContainer*> resources as defined in oneM2M TS-0023 [6], see also clause 7.1.3, shall be represented by oneM2M <*node*> resources as well. Each instance of a <*flexContainer*> resource representing a service provided by a specific OCF device is linked via the *nodeLink* attribute to a specific <*node*> resource instance that represents this specific OCF device.

For OCF Devices that are not matching with any of the listed categories, the present document does not specify any normative procedure to represent such OCF Devices as oneM2M <*node*> resources.

When a <*node*> resource is used to represent an OCF Device, it actually needs to reflect the details of the OCF Platform that hosts the OCF Device, Attributes of the <*node*> resource listed in table 7.1.1-1 shall have the specified value settings in table 7.1.1-1. All other attributes of the <*node*> resource shall be used as specified in oneM2M TS-0001 [2].

A <*node*> resource representing an OCF Device shall include exactly one [*deviceInfo*] child resource instance that represents specifics of the OCF Platform hosting the OCF Device. All other child resources of the <*node*> resource shall be used as specified in oneM2M TS-0001 [2]. Attributes of a [*deviceInfo*] resource listed in table 7.1.1-2 shall have the specified value settings in table 7.1.1-2 for the [*deviceInfo*] child resource instance representing the OCF Platform of the OCF Device. All other attributes or child resources of the [*deviceInfo*] resource shall be used as specified in oneM2M TS-0001 [2].

Table 7.1.1-1: Attribute settings for <*node*> resources representing an OCF Platform

Attribute Name	Setting
resourceName	This attribute shall be set to the value of the "pi" property (Platform ID) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7].
labels	This attribute shall include a Key:Value pair equal to "Iwked-Technology:OCF". Other Key:Value pairs may also be present.
nodeID	This attribute shall be set to the value of the "pi" property (Platform ID) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7].
hostedServiceLinks	This attribute shall contain a list of resource identifiers of <*flexContainer*> resources representing OCF services provided by OCF Servers which are hosted by the OCF Platform that is represented by this <*node*> resource.

Table 7.1.1-2: Attribute settings for a [*deviceInfo*] child-resource of a <*node*> resources representing an OCF Platform

Attribute Name	Setting
labels	This attribute shall include a Key:Value pair equal to "Iwked-Technology:OCF". Other Key:Value pairs may also be present.
deviceLabel	This attribute shall be set to the value of the "pi" property (Platform ID) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7].
manufacturer	This attribute shall be set to the value of the "mnmn" property (Manufacturer Name) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
manufacturerDetailsLink	This attribute shall be set to the value of the "mnml" property (Manufacturer Details Link) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
manufacturingDate	This attribute shall be set to the value of the "mndt" property (Date of Manufacture) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
model	This attribute shall be set to the value of the "mnmo" property (Model Number) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
subModel	This attribute shall be set to the value of the "mnpv" property (Platform Version) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
deviceType	This attribute shall be set to the value "OCF Platform".
fwVersion	This attribute shall be set to the value of the "mnfv" property (Firmware Version) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
hwVersion	This attribute shall be set to the value of the "mnhw" property (Hardware Version) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
osVersion	This attribute shall be set to the value of the "mnos" property (OS Version) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
systemTime	This attribute shall expose the system time of the device in line with the value of the "st" property (SystemTime) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.
supportURL	This attribute shall be set to the value of the "mnsl" property (Support link) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7], if present.

7.1.2 Representation of OCF Devices by oneM2M <*AE*> resources

7.1.2.1 OCF Clients

The present document does not specify any normative procedure to represent OCF Clients as oneM2M <*AE*> resources. Since the OCF specifications do not define any procedure for OCF Clients needing to register themselves with any other entity or needing to respond to any discovery procedures before trying to consume services provided by OCF Servers, it is not possible to determine which OCF Clients exist before they make any requests to consume services provided by OCF Servers. Therefore, it would be very complex to associate OCF Clients in an OCF Proximal IoT Network with oneM2M <*AE*> resources. In order to do that, the OCF-IPE would have to detect OCF Clients dynamically at the time when they try to request any services from that OCF-IPE and then create on the fly some corresponding <*AE*> resources. Furthermore, such dynamically created <*AE*> resources would also require adjustment of access control privileges when the corresponding AEs would need to access oneM2M resources. For these reasons, there are no provisions in the present document to represent OCF Clients by oneM2M <*AE*> resources.

7.1.2.2 OCF Servers

OCF Devices playing the role of an OCF Server can be represented by an <*AE*> resource that corresponds to an OCF-IPE, see figure 6.1.1-1. Depending on implementation and deployment needs, one or more OCF Servers can be exposed on the oneM2M side by a single OCF-IPE with a single <*AE*> resource. Furthermore, an OCF-IPE can expose oneM2M services by acting as one or more OCF Servers, see figure 6.1.2-1. In that case, the OCF-IPE which exposes a specific set of oneM2M services represented by a specific set of oneM2M resources needs to instantiate the corresponding OCF Server which offers the consumption of that service to other OCF entities.

If an OCF Server is intended to be exposed to the oneM2M system, exactly one OCF-IPE in a given oneM2M SP Domain shall be responsible for the exposure of services provided by that specific OCF Server in a given OCF Proximal Network. Therefore, a specific OCF Server shall be represented by a maximum of one OCF-IPE, i.e. by a maximum of one <*AE*> resource in that oneM2M SP Domain.

If a service represented by a set of specific oneM2M resources is intended to be exposed to a given OCF Proximal IoT Network, exactly one OCF-IPE for that given OCF Proximal IoT Network shall be responsible for the exposure of services represented by that specific set of oneM2M resources. Therefore, a specific set of oneM2M resources shall be represented by a maximum of one OCF Server instantiated by the OCF-IPE responsible for that exposure in a given OCF Proximal IoT Network.

Details of the OCF Server can be determined in the OCF Proximal IoT Network by means of executing OCF discovery and introspection procedures. For an OCF-IPE exposing a specific OCF-Server, any exposed services provided by that OCF Server that are meant to be exposed to the oneM2M System shall be represented by child resources of the <*AE*> resource representing that specific OCF-IPE, see clause 7.1.3.

Representing a specific set of OCF Servers exposed to the oneM2M side as child resources of the <*AE*> resource associated with an OCF-IPE has the following implications:

- The overall set of OCF Servers exposed to oneM2M entities and represented by one specific OCF-IPE can be associated with a specific M2M Service Subscriptions just like any other oneM2M Application. Therefore, the exposure of any of the services provided by the set of exposed OCF Servers associated with that specific OCF-IPE can be accounted for using the M2M Service Subscription of the OCF-IPE.

- An OCF-IPE allowing exposure of services provided by aa specific class of OCF Servers to the oneM2M side can be registered in the App-ID registry - e.g. a specific OCF-IPE that enables exposure of OCF Services to the oneM2M side for OCF Devices of a particular manufacturer.

Exposing a specific set of oneM2M services to the OCF side via instantiating a set of corresponding OCF Servers by a specific OCF-IPE represented by a specific <*AE*> resource associated with that OCF-IPE has the following implications:

- The overall set of oneM2M services exposed to the OCF Proximal IoT Network by a specific OCF-IPE can be associated with a M2M Service Subscriptions just like any other oneM2M Application. Therefore, the consumption of any of the services provided by the set of exposed oneM2M services associated with that specific OCF-IPE can be accounted for using the M2M Service Subscription of the OCF-IPE.

- An OCF-IPE allowing exposure of services provided by a specific class of oneM2M services to the OCF side can be registered in the App-ID registry - e.g. a specific OCF-IPE that enables exposure of oneM2M services to the OCF side for oneM2M Devices of a particular manufacturer.

Attributes of an <*AE*> resource listed in table 7.1.2-1 shall have the specified value settings in table 7.1.2-1 when that <*AE*> resource represents and OCF-IPE. All other attributes of the <*AE*> resource shall be used as specified in oneM2M TS-0001 [2].

Table 7.1.2-1: Attribute settings for <*AE*> resources representing an OCF-IPE

Attribute Name	Setting
labels	In order to indicate the supported external technology and which specific OCF Server(s) are represented by a specific OCF-IPE, the *labels* attribute of the <*AE*> resource of an OCF-IPE exposing OCF Server Functions to oneM2M shall contain the following information: • A Key:Value pair set to "Iwked-Technology:OCF" indicating that this AE supports interworking with OCF entities. • A Key:Value pair indicating the specific OCF Servers being exposed to the oneM2M system by this specific OCF-IPE. The Key should be set to "Iwked-Entity-IDs". The Value shall contain a coma-separated list of IDs in square brackets, e.g. "[ID1, ID2, ID3]", where each listed ID identifies one specific exposed OCF Server and is equal to the value of the "piid" property (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of the respective OCF Server as defined in the OCF Core Specification [7]. • A Key:Value pair indicating the specific oneM2M services being exposed to the OCF Proximal IoT Network by this specific OCF-IPE. The Key should be set to "Exposed-Resource-IDs". The Value shall contain a coma-separated list of oneM2M resource IDs in square brackets, e.g. "[ID1, ID2, ID3]", where each listed ID identifies one specific oneM2M resource which is the oneM2M resource representing the exposed oneM2M service. Note that depending on the resource structure used to represent an exposed oneM2M service - see for instance the oneM2M Device information models in line with oneM2M TS-0023 [6] - the resources identified by this list may contain child resources which shall not be listed separately. Other Key:Value pairs may also be present.

7.1.3 Representation of OCF services by oneM2M <*flexContainer*> resources

Services provided by OCF Servers that are intended to be exposed to the oneM2M system shall be represented by specializations of <*flexContainer*> resources in order to be exposed to the oneM2M system. Services provided by a specific OCF Server and intended to be exposed to the oneM2M system shall be represented by <*flexContainer*> child resources of the <*AE*> resource instance that represents the OCP-IPE responsible for the exposure of services provided by that specific OCF Server to oneM2M.

Services provided by OCF Servers are characterized by the device types defined in the OCF Device Specifications [8]. For each device type there is a minimum set of OCF resources defined in the OCF Device Specifications [8]. Exposure of a specific service provided by an OCF Server is accomplished by representing the corresponding set of OCF resources hosted on the OCF Server with matching oneM2M <*flexContainer*> resources hosted on the Registrar-CSE of the OCF-IPE responsible for the exposure of that OCF Server as child resources of the <*AE*> resources representing the OCF-IPE.

In oneM2M TS-0023 [6] a set of information models is defined which describes the exposure of services provided by oneM2M Devices via specializations of <*felxContainer*> resources. oneM2M TS-0023 [6] also contains a mapping between OCF Device Types and the corresponding oneM2M Devices.

When exposing services of an OCF Server that complies with any of the OCF Device Types for which oneM2M TS-0023 [6] includes a normative mapping to oneM2M Devices, an instance of the respective <*flexContainer*> specialization as defined in oneM2M TS-0023 [6] and any required child resources shall be used to represent the exposed service provided by an OCF Server.

When exposing services of an OCF Server that does not comply with any of the OCF Device Types for which oneM2M TS-0023 [6] includes a normative mapping to oneM2M Devices, an instance of a customized <*flexContainer*> resource shall be used. In line with <*flexContainer*> resources defined in oneM2M TS-0023 [6], such customized <*flexContainer*> resources shall include a *nodeLink* attribute which links to a <*node*> resource that represents the OCF Platform hosting the exposed OCF Server. Further details of such customized < *flexContainer*> resources are not in scope of this specification.

Attributes of an <*flexContainer*> resource representing services provided by an OCF Server as listed in table 7.1.3-1 shall have the specified value settings in table 7.1.3-1. All other attributes of the <*flexContainer*> resource shall be used as specified in oneM2M TS-0001 [2] or in oneM2M TS-0023 [6] if applicable.

Table 7.1.3-1: Attribute settings for <*flexContainer*> resources representing services provided by an OCF Server

Attribute Name	Setting
labels	In order to indicate the supported external technology and which specific OCF Server is represented by this <*flexContainer*> resource, the *labels* attribute of the <*flexContainer*> resource shall contain the following information: • A Key:Value pair set to "Iwked-Technology:OCF" indicating that this <*flexContainer*> supports interworking with OCF entities. • A Key:Value pair indicating the specific OCF Server being exposed to the oneM2M system by this specific <*flexContainer*>. The Key should be set to "Iwked-Entity-ID". The Value shall be equal to the value of the "piid" property (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of the respective OCF Server as defined in the OCF Core Specification [7]. Other Key:Value pairs may also be present.
nodeLink	The *resource identifier* of a <*node*> resource that stores the node specific information of the node on which the OCF Server resides which provides services that are exposed by this <*flexContainer*> resource. See clause 7.1.1 for details on representing OCF Devices by a <*node*> resource.

The procedural aspects on how to create, delete and interact with <*flexContainer*> resources for the purpose of exposing OCF Functions to the oneM2M system are specified in clause 8.1 of the present document.

7.2 Representation of oneM2M services by OCF resources

Services provided by oneM2M Devices can be exposed to an OCF Proximal IoT Network by an OCF-IPE acting as one or more OCF Servers - see clause 6.2.1. The OCF-Servers instantiated by an OCF-IPE are termed virtual OCF Servers in the present document. The OCF-IPE itself follows the concept of an OCF Bridge Device, see OCF Bridging Specification [10]. Therefore, the OCF-IPE itself shall act on the OCF side in the role of an OCF Device with the device type "oic.d.bridge" supporting the discovery of all resources exposed via the one or more virtual OCF Servers it instantiates. All bridged devices - i.e. all virtual OCF Servers instantiated by the OCF-IPE - with all their Resources shall be listed in the OCF-IPE's own "/oic/res" resource, see OCF Bridging Specification [10]. The OCF-IPE itself shall generate a value for the "di" (device ID) property value to represent itself with a unique device ID in line with OCF Core Specifications [7] as an OCF specified "oic.d.bridge" device. Furthermore, the OCF-IPE shall also generate an individual device ID property value for each virtual OCF Server it instantiates.

For a service intended to be exposed to the OCF Proximal IoT Network and provided by a oneM2M Device represented by a <*flexContainer*> resource, the corresponding OCF Device Type shall be determined according to the normative mapping defined in the oneM2M specification(s):

- oneM2M TS-0023 [6].

Then for each instance of an OCF Device Type that has been determined in the mapping, the minimum set of resources for that OCF Device Type as specified in the OCF Device Specification [8] shall be exposed to the OCF Proximal IoT Network by the OCF-IPE responsible for the exposure. The OCF-IPE responsible for the exposure to the OCF Proximal IoT Network shall act as an OCF Server for each identified OCF Device Type.

Each OCF Server, i.e. each virtual OCF Device which is instantiated by an OCF-IPE needs to serve a minimum set of resources depending on the Device Type it represents. Common to all OCF Devices is the need to support the following mandatory core resources:

- ″/oic/res″ for discovery of resources hosted by the OCF Server
- ″/oic/p" for discovery of platform specific parameters of the node hosting the OCF Server
- ″/oic/d″ for discovery of device information

Beyond these core resources, an OCF Server shall also support the resources required by the specific OCF Device Type. For the mandatory core resources supported by all OCF Servers, the property settings defined in table 7.2-1 and table 7.2-2 shall apply. Properties not listed in table 7.2-1 and table 7.2-2 may be present while the present document does not define any settings for those properties.

Table 7.2-1: Property settings for a "/oic/p" resource provided by an OCF-IPE acting as an OCF Server

Property Name	Setting
pi	This property shall be generated in line with the OCF Core Specification [7]:Unique identifier for the physical platform (UIUID); this shall be a UUID in accordance with IETF RFC 4122 [11]. It is recommended that the UUID be created using the random generation scheme (version 4 UUID) specific in the RFC. If the OCF-IPE that instantiated this OCF Server is instantiating multiple OCF Servers, it shall use the same value for all pi properties of the /oic/p resources of all its instantiated OCF Servers.
mnmn	In case the <*AEr*> resource representing the OCF-IPE that instantiated this OCF Server is linked to a <*node*> resource that has a [*deviceInfo*] child resource that includes a *manufacturer* attribute, the value of that *manufacturer* shall be used for this mnmn property. Otherwise, the string to be used for this property is implementation dependent but needs to be present.

Table 7.2-2: Property settings for a "/oic/d" resource provided by an OCF-IPE acting as an OCF Server

Property Name	Setting
n	An implementation dependent OCF Device name prefixed by the string "oneM2M-".
icv	Spec version of the OCF Core Specification this OCF Server instance of the OCF-IPE is implemented to, The syntax is "ocf.<major>.<minor>.<subversion>" where <major>, <minor>,and <sub-version> are the major, minor and sub-version numbers of the OCF Core Specification, respectively.
di	Unique identifier of the device in line with the requirements in the OCF Core Specifications [7]. The OCF-IPE shall generate a unique "di" property value to represent itself. In addition it shall also generate a unique "di" property value for each virtual OCF Server that gets instantiated by the OCF-IPE.
dmno	Model Number: Property that starts with the string "oneM2M-" followed by a concatenation of the M2M-SP-ID plus the AE-ID of the OCF-IPE that instantiated the OCF Server and a value for a model number in line with the definitions in the OCF Core Specifications [7]. This last segment - the value for a model number - shall be set to the value of the *model* attribute of a [deviceInfo] resource in case the exposed oneM2M service is represented by a <*flexContainer*> that is linked to a <*node*> resource which has a [deviceInfo] child resource. Otherwise, the setting of this value is an implementation choice.
dmv	Version of the Resource Specification to which this OCF Server instance of the OCF-IPE is implemented. This needs to be in line with the requirements on the dmv property defined in the OCF Core Specifications [7].
piid	A unique and immutable identifier for this OCF Server instance of the OCF-IPE generated in line with the OCF Core Specifications [7].

8 OCF Interworking Procedures

8.1 Procedures supporting exposure of OCF Functions to the oneM2M System

8.1.1 Determination of OCF Functions to be exposed to the oneM2M System

In an OCF Proximal IoT Network, the specific setup and security parameters to be used by OCF Clients or OCF Servers - such as credentials to be used - are provisioned during an onboarding procedure. This onboarding procedure also includes provisioning of credentials and roles etc. as described in OCF Security-Specification [9]. In order to perform that onboarding procedure, an onboarding tool is used. An OCF-IPE which intends to expose OCF Functions of OCF Servers in the OCF Proximal IoT Network to the oneM2M System needs to go through such an onboarding process as well. During the onboarding procedure, OCF-IPE is provisioned with appropriate credentials and parameters to interact with OCF Servers in the OCF Proximal IoT Network. For the OCF-IPE to properly support the intended exposure of OCF Services, it needs to be determined which particular OCF Servers are meant to be exposed via the OCF-IPE being onboarded. The set of OCF Servers to be exposed shall be identified by a set of "piid" property values (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of the respective OCF Servers, see OCF Core-Specification [7].

In what follows three different concepts of selecting the set of OCF-Servers to be exposed to the oneM2M System are outlined. However, it is not in the scope of the present document to define details on how to implement these concepts:

- Pre-Provisioning: The set of OCF Servers to be exposed to the oneM2M System is determined before the OCF-IPE is initiated. The details of the selection procedure are not specified in the present document. The resulting selection is provided to the OCF-IPE by means of configuration information - see circle termed "Configuration" in figure 6.1.2-1 - stored statically in storage accessible by the OCF-IPE such as a configuration file or a set of <*contentInstance*> resources. It is not in the scope of the present document to define any details of the storage mechanism such as storage location, format, serialization, etc. of the selected set of OCF-Servers. Upon initiation of the OCF-IPE it shall act as an OCF Client and verify that the configured OCF Servers to be exposed to oneM2M are actually accessible on the OCF Proximal IoT Network by correlating the configured "piid" values with the results of a direct resource discovery procedure targeting the pre-defined URI "/oic/d" or a corresponding indirect discovery procedure targeting the pre-defined URI "/oic/rd" in a multicast request in the OCF Proximal IoT Network, see clause 11.3 of OCF Core-Specification [7]. If configured OCF Servers are not discoverable in the OCF Proximal IoT Network, the corresponding entries need to be removed from the set of OCF-Servers to be exposed to the oneM2M System by the OCF-IPE

- Discovery: When the OCF-IPE is initiated, in will act as an OCF Client and trigger a discovery of OCF Servers in the OCF Proximal IoT Network. Among the discovered OCF Servers, a set of OCF Servers to be exposed will be selected by the stakeholder responsible for the OCF-IPE deployment. This selection may be implemented by a user-facing interface (GUI) or by other means and is not in the scope of the present document. Discovery results may also get filtered by the OCF-IPE before selecting the OCF Servers to be exposed to oneM2M. For example, the set of discovered OCF Servers can be filtered in order to limit the exposure to oneM2M to a specific set of OCF Servers with a given manufacturer name or a specific model name as indicated by the "dmn" property (Manufacturer Name) or the "dmno" property (Model Number) of the OCF device discovery resource with the pre-defined URI "/oic/d" of the respective OCF Device as defined in [7]. In line with the described discovery and selection process, the OCF-IPE needs to be onboarded to the OCF Proximal IoT Network as an OCF Client with credentials that are sufficient to access the selected OCF Servers intended to be exposed to oneM2M.

- On demand determination: This selection concept is very similar to the one described in the previous bullet point, except that the discovery of OCF Servers to be exposed to the oneM2M system is triggered by means of changing the state of a oneM2M resource - see the dashed box termed "Resource instances to trigger discovery of OCF Functions to be exposed to oneM2M" in figure 6.1.2-1. The present document does not define details for this triggering mechanism which is an implementation choice. In the remainder of this bullet point an example is given. For instance a <*container*> resource may get created by the OCF-IPE when it starts and a subscription to that <*container*> resource would be established for the OCF-IPE to get notified about creation of any new <*contentInstance*> resources in that <*container*> along with ACPs that would control which entities are authorized to trigger the OCF discovery. Upon creation of a new <*contentInstance*> child resource in that <*container*> resource, the OCF-IPE would get notified. The information in the *content* attribute of the new <*contentInstance*> resource may be used to define parameters for the discovery to be executed such as filtering OCF discovery with a specific "dmn" property (Manufacturer Name) or the "dmno" property (Model Number) of the OCF device discovery resource with the pre-defined URI "/oic/d" of the respective OCF Device as defined in [7]. The notification would then result in the OCF-IPE initiating a new discovery and selection procedure as described in the previous bullet point. After that is completed, the resource used to trigger the discovery and selection process may need to get cleaned up - i.e. the <*contentInstance*> resource may need to get removed.

Independent of which of the described selection concepts is implemented, the onboarding of the OCF-IPE as an OCF Client needs to result in appropriate credentials being provisioned to the OCF-IPE so that the OCF-IPE is authorized to interact as intended with the selected OCF Servers.

For instance if the OCF-IPE will act as an OCF Client with the intent to be able to switch on or off a set of lights implemented as OCF Servers, the onboarding procedure needs to result in provisioning of credentials that provide the OCF-IPE sufficient access rights to actually switch on or off the intended set of lights.

The present document does not contain any details on how such consistency between the onboarding procedure for the OCF-IPE and the selection of the OCF Servers to interact with can be achieved since this is implementation dependent. The stakeholder responsible for deploying and onboarding the OCF-IPE needs to be aware that the selected set of OCF Servers for which the OCF-IPE will get provisioned with credentials that allow access to that set of servers will actually be exposed to the oneM2M system. On the oneM2M side, appropriate Access Control Privileges need to be setup in order to control which oneM2M entities are authorized to consume the services provided by the set of exposed OCF Servers.

In order to avoid a loop of exposing services from one oneM2M SP domain to an OCF Proximal IoT Network and back to the same oneM2M SP domain, the OCF-IPE needs to verify that none of the selected OCF Servers to be exposed to oneM2M is actually an instantiation of an OCF Server that was previously instantiated by an OCF-IPE interfacing to the same oneM2M SP domain. This can be identified by inspecting the "dmno" (Model Number) property of the pre-defined URI "/oic/d" of the respective OCF Device defined in [7]. As specified in clause 8.2.2 of the present document, OCF Servers instantiated by OCF-IPEs shall use a value for the "dmno" (Model Number) property that starts with the string "oneM2M-" followed by a concatenation of the M2M-SP-ID of the OCF-IPE that instantiated the OCF Server and a the value for a model number as detailed in clause 8.2.2. If any of the OCF Servers selected for exposure to oneM2M uses a value for the "dmno" (Model Number) property in its "/oic/d" resource that starts with "oneM2M-" and is followed by an M2M-SP-ID which is the same as the M2M-SP-ID of the oneM2M SP domain of the OCF-IPE intended to expose that OCF Server, the OCF Server shall be removed from the set of OCF Servers to be exposed to oneM2M.

As a result of onboarding and selection of the set of OCF Servers to be exposed, it is assumed in the remainder of the present document that the following applies:

- The OCF-IPE got onboarded as an OCF Client with appropriate credentials to access the set of OCF Servers selected by the stakeholder responsible for the OCF-IPE deployment for exposure to the oneM2M system.
- A valid set of OCF Servers to be exposed to oneM2M has been determined including avoidance of loopback of services from a oneM2M SP domain to an OCF Proximal IoT Network and back to the same oneM2M SP domain.
- The set of "piid" property values (Protocol Independent ID) of the OCF device resource with the pre-defined URI "/oic/d" of the respective OCF Servers to be exposed is known to the OCF-IPE.

8.1.2 Handling of oneM2M Resource representing exposed OCF Functions

8.1.2.1 <*AE*> resource representing an OCF-IPE and the associated set of exposed OCF Servers

When an OCF-IPE completes registration with its Registrar CSE, an <*AE*> resource representing that OCF-IPE has been created as a result of that registration. As specified in clause 7.1.2.2, the *labels* attribute of this <*AE*> resource shall reflect the fact that this AE is an OCF-IPE by adding a Key:Value pair set to "Iwked-Technology:OCF", see table 7.1.2-1. The registration of the OCF-IPE including a successful creation of the <*AE*> representing the OCF-IPE is a pre-requisite for creating any other oneM2M Resources representing OCF Functions exposed by this specific OCF-IPE.

oneM2M resources representing services provided by exposed OCF Servers which are exposed by a specific OCF-IPE shall be created as child resources of the <*AE*> resource representing that OCF-IPE.

For each OCF Server that is exposed to oneM2M by a specific OCF-IPE, the value of the "piid" property (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of the respective OCF Server as defined in the OCF Core Specification [7] shall be added to the list of IDs under the Key "Iwked-Entity-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE as defined in table 7.1.2-1. The addition of the value of the "piid" property to the list of IDs under the Key "Iwked-Entity-IDs" in the *labels* attribute of the <*AE*> resource representing the OCF-IPE exposing a specific OCF Server shall be performed when all other resources and subscriptions for exposing that OCF Server to the oneM2M system have been established, see clauses 8.1.2.2, 8.1.2.3, 8.1.3 and 8.1.4 for more details. **Step 002** below defines the pre-requisites in detail.

When the OCF-IPE detects that a specific OCF Server is not accessible any longer - e.g. when the device resource with the pre-defined URI "/oic/d" of the respective OCF Server cannot be accessed any longer because it was removed from the OCF Proximal Network - the OCF-IPE shall remove the "piid" property value (Protocol Independent ID) of that specific OCF Server from the list of IDs under the Key "Iwked-Entity-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE. In this case the OCF-IPE shall also delete any child resources of its own <*AE*> resource representing services provided by the respective OCF Server that is not accessible any longer, see also clause 8.1.2.2. Before the deletion of such child resources is performed, linkage to the respective <*node*> resource shall be updated as defined in clause 8.1.2.3, including possible deletion of <*node*> resources. It is an implementation choice of the OCF-IPE to choose an appropriate timeout for detecting absence of an OCF Server after an attempt to access it has not resulted in a valid response. Furthermore, it is also an implementation choice of the OCF-IPE to re-try to discover and expose OCF Servers which have previously been exposed to oneM2M but got removed from exposure due to inability to access them.

When the OCF-IPE detects that an additional OCF Server has to be exposed to the oneM2M system - this might be triggered on demand or by entering discovery procedure on the OCF side from time to time as described in clause 8.1.1 - the OCF-IPE shall complete verification of access to the targeted OCF Server, creation of child and <*node*> resources as defined in clauses 8.1.2.2 and 8.1.2.3 as well as establishing the state monitoring functions as described in clauses 8.1.3 and 8.1.4. Only then, the OFC-IPE shall add the value of the "piid" property of the respective OCF Server to the list of IDs under the Key "Iwked-Entity-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE.

When an OCF-IPE is going to terminate, it shall properly de-register with its Registrar CSE, i.e. it shall delete the corresponding <*AE*> resource representing the OCF-IPE. With that deletion any child resources of this <*AE*> resource will also be deleted, terminating the exposure of any of the exposed OCF Functions. Before de-registration is performed, the OFC-IPE shall update the linkage between any previously created <*flexContainer*> resources and the respective <*node*> resource as defined in clause 8.1.2.3, including possible deletion of <*node*> resources.
Figure 8.1.2.1-1 depicts a high-level flow of events and processing steps throughout the OCF-IPE life cycle. Some of the processing steps consist of complex sub-procedures partially relying on functionality specified in other clauses of the present document. Therefore, the description of the different steps include references to the relevant clauses of the present document. For now it should just serve the purpose of explaining the handling of an <*AE*> resource representing an OCF-IPE and the various actions the OCF-IPE has to take in order to comply with the specified way to expose OCF functions to oneM2M. Details of the more complex processing steps are defined in subsequent clauses of the present document.

Step 001: Register OCF-IPE
The OCF-IPE registers with its Registrar CSE. The representation of the <*AE*> resource which is requested to be created shall contain a *labels* attribute which includes a "key:value" pair of "Iwked-Technology:OCF".

Step 002: Establish pre-requisites
In order to perform a proper exposure of OCF functions to the oneM2M system, some pre-requisites have to be met. Step 002 contains what is needed to establish those pre-requisites. In particular the following needs to be completed:

a) The set of OCF Servers to be exposed to oneM2M has to be determined, see clause 8.1.1 for a description on how to accomplish that. It is necessary to ensure via onboarding that the OCF-IPE is provisioned with the proper security credentials to access the set of OCF Servers to be exposed. Besides proper onboarding and selection of the set of OCF Servers to be exposed, the OCF-IPE shall also verify that it is able to access each of the selected OCF Servers and discard OCF Servers for which access is not possible. The set of OCF Servers to be exposed shall be characterized by the set of values of the "piid" property (Protocol Independent ID) of the device resources with the pre-defined URI "/oic/d" of the respective OCF Servers as defined in the OCF Core Specification [7].

b) Once the set of OCF Servers to be exposed is determined, the OCF-IPE shall create oneM2M resources to represent the exposed services and physical devices. Depending on the OCF Device types and the normative mapping to oneM2M information models and resource types as defined in OCF Device-Specification [8] and oneM2M TS-0023 [6], one <*flexContainer*> plus possibly required sub-ordinated child resources shall be created for each exposed OCF Server, see clause 8.1.2.2. It is recommended that Access Control Privileges are set such that only the OCF-IPE and possibly administration entities can access these <*flexContainer*> resources. After creation of the <*flexContainer*> resources representing exposed OCF Servers, <*node*> resources representing the physical OCF Devices hosting the exposed OCF Servers shall be linked with the corresponding <*flexContainer*> resources and - if not already present - shall be created by the OCF-IPE on its Registrar CSE, see clause 8.1.2.3. In order to be able to detect any requests on the oneM2M side to consume the exposed OCF services - which may require a state change on the corresponding OCF Server - the OCF-IPE shall establish subscriptions to the previously created oneM2M resources which expose such OCF Servers. See clause 8.1.4 for more details.

c) After creation of the oneM2M resources needed by the OCF-IPE to expose OCF Servers to oneM2M, the OCF-IPE shall establish monitoring of the state of OCF Servers which are to be exposed by using the observe mechanism defined in OCF Core Specification [7]. The OCF-IPE shall be able to receive observation of changes of state of the exposed OCF Servers. The OCF-IPE shall also ensure that this monitoring is continuously performed throughout the lifecycle of the OCF-IPE. This may require re-establishment of the observe mechanism as defined in OCF Core Specification [7], see also clause 8.1.3.

d) Upon reception of a state change observation from exposed OCF Servers, the OCF-IPE shall mirror that state change by updating the corresponding oneM2M resource(s) created earlier, see clause 8.1.3 for more details. This particular sub-step 002d - i.e. the task to mirror any reported state changes of exposed OCF Servers to the state of the corresponding oneM2M resources - is actually a procedure that can be triggered asynchronously throughout the lifetime of the OCF-IPE and shall be executed as many times as needed.

Step 003: Add list of exposed entities
The OCF-IPE has established all pre-requisites to start the exposure of the OCF Servers to oneM2M. Before doing so, the OCF-IPE needs to include a list of all "piid" property (Protocol Independent ID) values of the exposed OCF Servers in the *labels* attribute of its own <*AE*> resource as a "key:value" pair in line with the format "Iwked-Entity-IDs:[ID1, ID2, ID3]", see clause 7.1.2.2.

Step 004: Start exposure
In order to start the actual service exposure of OCF Servers to oneM2M entities, the OCF-IPE needs to set the ACPs which govern the access to the oneM2M resources representing OCF Servers such that the intended oneM2M entities are authorized to access the respective oneM2M resources.

Steps 005a, 005b, 005c define conditional procedures which shall be carried out under the conditions defined in the specific step descriptions below. They can be triggered asynchronously - i.e. not in the order described in the present document, not at any pre-defined time and not in any particular order of execution. The execution of the procedures defined for each of these steps shall be executed as many times as needed.

Step 005a: Process oneM2M request to consume OCF service
This processing step is triggered asynchronously when receiving a notification caused by a request to change state in oneM2M resources that are representing exposed OCF Servers due to the subscription(s) established in Step 002b. The OCF-IPE shall decide on the need for issuing a corresponding request for state change to the relevant OCF Server and execute the corresponding request on the OCF side if needed. The OCF-IPE shall conditionally adjust oneM2M resource state depending on the outcome of executed OCF operation(s) and send a response to the received notification. Details for this step are defined in clause 8.1.4. Since this step is triggered by occurrences of notifications which were generated by subscriptions established earlier, see step 002b, the OCF-IPE shall execute this step for each of these notifications it receives.

Step 005b: Expose additional OCF Server(s)
This processing step is triggered asynchronously when the OCF-IPE detects a need to expose additional OCF Server(s). As described in clause 8.1.1, the set of OCF Servers to be exposed to oneM2M may change dynamically (e.g. addition on demand or by asynchronous discovery on the OCF side). It is possible that additional OCF Servers are identified and are intended to be exposed via an already initialized OCF-IPE. In such a case all the pre-requisites listed for step 002 need to be established for each additional OCF Server to be exposed. After these pre-requisites are met, the OCF-IPE needs to update the list of "piid" property (Protocol Independent ID) values of all exposed OCF Servers in the *labels* attribute of its own <*AE*> resource as a "key:value" pair in line with the format "Iwked-Entity-IDs:[ID1, ID2, ID3]", see clause 7.1.2.2. Ultimately the OCF-IPE needs to adjust ACPs for the resources representing the additionally exposed OCF Servers so that the intended oneM2M entities can consume the offered services. Step 005b shall be executed when the OCF-IPE detects the need to expose additional OCF-Servers which are currently not exposed to the oneM2M side. Methods for detecting such conditions are out of the scope of the present document.

Step 005c: Stop exposure of a specific OCF Server
Upon detection of need to stop exposure of a specific OCF Server- e.g. when its reachability stalled or on demand - the OCF-IPE needs to go through the following procedure. Initially, the OCF-IPE shall update ACPs of the oneM2M resources representing the OCF Server to stop access by other oneM2M entities to the exposed services provided by the considered OCF Server. After that, the OCF-IPE shall stop any monitoring and mirroring of state of the OCF Server established in steps 002c and 002d, see clause 8.1.3. Furthermore, the OCF-IPE shall remove linkage from the <*node*> resource representing the OCF Platform hosting the OCF Server to the <flexContainer> representing the OCF Server including a possible deletion of the <*node*> resource if needed. See clauses 8.1.2.2 and 8.1.2.3. After that, the OCF-IPE shall remove the OCF Server's "ppid" property from the list associated with "Iwked-Entity-IDs" key in the *labels* attribute of the OCF-IPE <*AE*> resource. Finally, the OCF-IPE shall delete the <*flexContainer*> representing the OCF Server including its children.

Step 006: Prepare termination
When the OCF-IPE intends to terminate, it shall stop any active procedures for monitoring and mirroring of state of any of the remaining exposed OCF Servers, see steps 002c and 002d as well as clause 8.1.3. In addition, the OCF-IPE shall remove any linkage from <*node*> resources representing OCF Platforms hosting any of the exposed OCF Servers to <*flexContainer*> child resources under this OCF-IPE's own <*AE*> resource including deletion of <*node*> resources if needed. See clauses 8.1.2.3.

Step 007: De-register OCF-IPE
The OPC-IPE shall delete the <*AE*> resource representing this OCF-IPE which will result also in deletion of all its child resources - and therefore - the removal of all remaining oneM2M resources representing OCF Servers exposed by this OCF-IPE.

After successful completion of the de-registration, the OCF-IPE has terminated from a oneM2M perspective. It is an implementation choice of the OCF-IPE whether it is also terminating any remaining activity on the OCF side - such as listening to further on-boarding requests or performing further discovery procedures to discover OCF Servers to be exposed in the future. These implementation choices are not in scope of the present document.

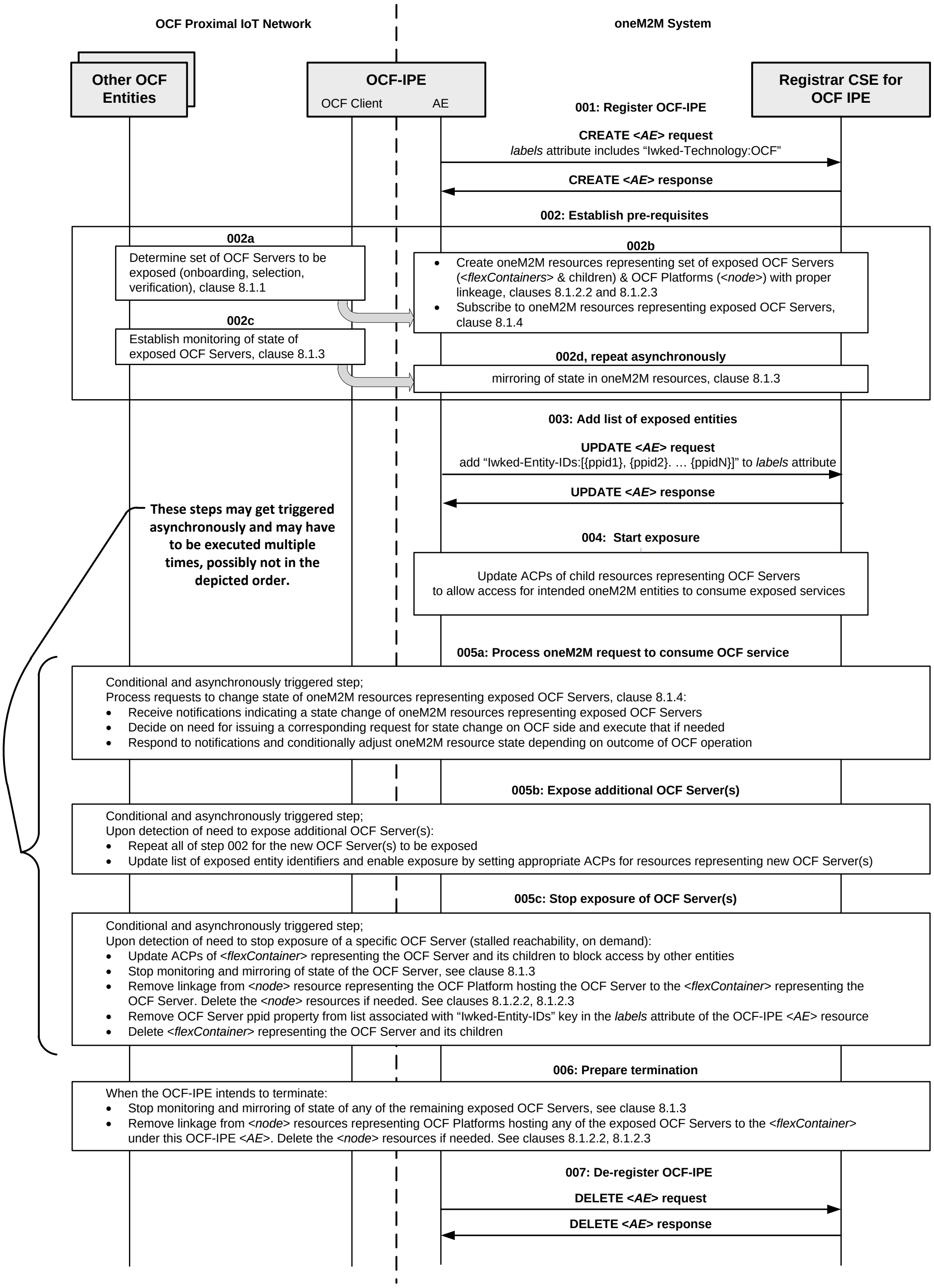

OCF Proximal IoT Network
oneM2M System
Other OCF Entities
OCF-IPE
OCF Client
AE
Registrar CSE for OCF IPE
001: Register OCF-IPE
CREATE <AE> request
labels attribute includes "Iwked-Technology:OCF"
CREATE <AE> response
002: Establish pre-requisites
002a
Determine set of OCF Servers to be exposed (onboarding, selection, verification), clause 8.1.1
002b
• Create oneM2M resources representing set of exposed OCF Servers (<flexContainers> & children) & OCF Platforms (<node>) with proper linkeage, clauses 8.1.2.2 and 8.1.2.3
• Subscribe to oneM2M resources representing exposed OCF Servers, clause 8.1.4
002c
Establish monitoring of state of exposed OCF Servers, clause 8.1.3
002d, repeat asynchronously
mirroring of state in oneM2M resources, clause 8.1.3
003: Add list of exposed entities
UPDATE <AE> request
add "Iwked-Entity-IDs:[{ppid1}, {ppid2}. … {ppidN}]" to labels attribute
UPDATE <AE> response
These steps may get triggered asynchronously and may have to be executed multiple times, possibly not in the depicted order.
004: Start exposure
Update ACPs of child resources representing OCF Servers to allow access for intended oneM2M entities to consume exposed services
005a: Process oneM2M request to consume OCF service
Conditional and asynchronously triggered step;
Process requests to change state of oneM2M resources representing exposed OCF Servers, clause 8.1.4:
• Receive notifications indicating a state change of oneM2M resources representing exposed OCF Servers
• Decide on need for issuing a corresponding request for state change on OCF side and execute that if needed
• Respond to notifications and conditionally adjust oneM2M resource state depending on outcome of OCF operation
005b: Expose additional OCF Server(s)
Conditional and asynchronously triggered step;
Upon detection of need to expose additional OCF Server(s):
• Repeat all of step 002 for the new OCF Server(s) to be exposed
• Update list of exposed entity identifiers and enable exposure by setting appropriate ACPs for resources representing new OCF Server(s)
005c: Stop exposure of OCF Server(s)
Conditional and asynchronously triggered step;
Upon detection of need to stop exposure of a specific OCF Server (stalled reachability, on demand):
• Update ACPs of <flexContainer> representing the OCF Server and its children to block access by other entities
• Stop monitoring and mirroring of state of the OCF Server, see clause 8.1.3
• Remove linkage from <node> resource representing the OCF Platform hosting the OCF Server to the <flexContainer> representing the OCF Server. Delete the <node> resources if needed. See clauses 8.1.2.2, 8.1.2.3
• Remove OCF Server ppid property from list associated with "Iwked-Entity-IDs" key in the labels attribute of the OCF-IPE <AE> resource
• Delete <flexContainer> representing the OCF Server and its children
006: Prepare termination
When the OCF-IPE intends to terminate:
• Stop monitoring and mirroring of state of any of the remaining exposed OCF Servers, see clause 8.1.3
• Remove linkage from <node> resources representing OCF Platforms hosting any of the exposed OCF Servers to the <flexContainer> under this OCF-IPE <AE>. Delete the <node> resources if needed. See clauses 8.1.2.2, 8.1.2.3
007: De-register OCF-IPE
DELETE <AE> request
DELETE <AE> response

Figure 8.1.2.1-1: High-level flow of events and processing steps throughout the OCF-IPE life cycle

8.1.2.2 <*flexContainer*> resources representing services provided by exposed OCF Servers

8.1.2.2.0 Introduction

This clause describes the procedures related to the use of <*flexContainer*> resources - and possibly any required child resources thereof - to represent exposed OCF Servers to the oneM2M system.

8.1.2.2.1 Parent resource and dependency on OCF Device types

In line with oneM2M TS-0033 [5] and clause 7.1.3 of the present document, services provided by exposed OCF Servers shall be represented by <*flexContainer*> resources on the oneM2M side - and possibly by child resources thereof. Which particular specialization of <*flexContainer*> resources shall be used to represent an OCF Server complying with a given OCF Device type depends on the information model mapping for OCF Devices defined in oneM2M TS-0023 [6]. Depending on the applicable information model and the optional resources and properties of the specific OCF Server, the top level <*flexContainer*> resource used to represent a specific OCF Server may require additional child resources. The <*flexContainer*> resources representing exposed OCF Servers - and accordingly their child resources when needed - shall be created by the OCF-IPE that is exposing those OCF Servers as descendants of its own <*AE*> resource.

8.1.2.2.2 Creation of <*flexContainer*> resources used to represent OCF Servers

8.1.2.2.2.1 Pre-requisites

A pre-requisite to create <*flexContainer*> resources used to represent OCF Servers is that the OCF-IPE has previously determined which specific OCF Servers have to be exposed, see the description in clause 8.1.1 and step 002a in clause 8.1.2.1.

Proper determination of which OCF Server to expose via the considered OCF-IPE will ensure that the OCF-IPE is provisioned with the proper security credentials to access the set of OCF Servers to be exposed. Furthermore, the OCF-IPE shall also verify that it is able to access each of the selected OCF Servers and discard OCF Servers for which access is not possible. After this proper determination of the set of OCF Servers to be exposed has been performed, the set of values of the "piid" property (Protocol Independent ID) of the device resources with the pre-defined URI "/oic/d" of the respective OCF Servers as defined in the OCF Core Specification [7] will be known to the OCF-IPE. In summary, the following shall be completed for each OCF Server to be exposed to the oneM2M system before the OCF-IPE requests creation of corresponding <*flexContainer*> resources representing exposed OCF Servers on the oneM2M side:

- proper onboarding of the OCF-IPE
- selection of set of OCF Servers to be exposed
- verification of access to the selected OCF Servers
- determination of the set of "piid" property (Protocol Independent ID) for the respective OCF Servers

These pre-requisites for the creation of <*flexContainer*> resources used to represent OCF Servers have to be established for both, the initial set of OCF Servers to be exposed (see step 002a in clause 8.1.2.1) as well as for any additional OCF Servers which may get added to the exposed set of OCF Servers later on (see step 005b in clause 8.1.2.1).

8.1.2.2.2.2 Creation process

Reasons for creation

Throughout the lifecycle of an OCF-IPE, <*flexContainer*> resources used to represent OCF Servers - and possibly required child resources thereof - shall be created in the following cases:

- when the OCF-IPE has registered and an initial set of OCF Servers to be exposed has been determined before exposure of any OCF services has started, see step 002a in clause 8.1.2.1.
- when an already active OCF-IPE which is already exposing a set of OCF services to oneM2M has detected that one or more new OCF Servers have to be added to the set of exposed OCF servers, see step 005b in clause 8.1.2.1.

<*flexContainer*> resources which are meant to represent OCF Servers - and their required child resources - shall only be created when the pre-requisites outlined in clause 8.1.2.2.2.1 are established.

Creation of top level <*flexContainer*> resource and descendant resources

For each OCF Server to be exposed to oneM2M, the OCF-IPE shall create one top level <*flexContainer*> resource in line with the appropriate device model according to the mapping defined in oneM2M TS-0023 [6] as a direct child of its own <*AE*> resource. For a given OCF Server offering services in line with a specific OCF Device type, the OCF-IPE needs to determine which optional resources are supported by this OCF Server. Each of these optional resources on the OCF side will require additional creation of the corresponding optional descendant resources of the top level <*flexContainer*> resource in the device models defined in oneM2M TS-0023 [6]. The OCF-IPE shall also create these required descendant resources of the top level <*flexContainer*> resource.

Linkage with <*node*> resources

According to oneM2M TS-0023 [6] and in line with clause 7.1.3 of the present document, the *nodeLink* attribute of the top level <*flexContainer*> resource representing a given OCF Server shall be set to the resource identifier of a <*node*> resource representing the physical hardware on which an OCF Server is hosted, which is termed OCF Platform in OCF specifications. A <*node*> resource representing a specific OCF Platform contains a *nodeID* attribute set to the "pi" property (Platform ID) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7]. If such a <*node*> resource does not yet exist, it shall be created by the OCF-IPE, see clause 8.1.2.3 for more details. The *hostedServiceLinks* attribute of the <*node*> resource representing the OCF Platform for a given OCF Server shall be present and include the resource identifier of the top level <*flexContainer*> resource representing that given OCF Server.

labels Attribute settings

In line with clause 7.1.3, the *labels* attribute of the <*flexContainer*> resource shall contain a Key:Value pair set to "Iwked-Technology:OCF" indicating that this <*flexContainer*> supports interworking with OCF entities. It shall also contain a Key:Value pair Iwked-Entity-ID:{piid}" indicating the specific OCF Server being exposed to the oneM2M system by this specific <*flexContainer*>, where {piid} is a placeholder for the value of the "piid" property (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of the respective OCF Server as defined in the OCF Core Specification [7].

Update of parent <*AE*> resource after creation completed

After the creation of a <*flexContainer*> resource - including any required descendants - and after all other pre-requisites for exposing a given OCF Server are established - see step 002 in clause 8.1.2.1 - the parent <*AE*> resource of the respective <*flexContainer*> resource used to represent the given OCF Server needs to be updated to include the value of the "piid" property (Protocol Independent ID) of the respective OCF Server in the *labels* attribute under the "Iwked-Entity-IDs" key, see clause 7.1.2.2 of the present document.

Handling of Access Control Privileges

At time of creation of <*flexContainer*> resources and descendant resources to represent OCF Servers, it is advised to set Access Control Privileges such that other entities are not able yet to consume the OCF services which shall be exposed by these resources. The reason for that is: The OCF-IPE has to establish a few more pre-requisites before starting the actual exposure - see step 002 in clause 8.1.2.1. Only after all these pre-requisites are established and after the parent <*AE*> resource has been updated with the proper information in the *labels* attribute under the "Iwked-Entity-IDs" key, the OCF-IPE should set the Access Control Privileges of <*flexContainer*> resources and descendant resources to represent OCF Servers such that intended oneM2M entities could eventually consume the exposed services.

8.1.2.2.3 Deletion of <*flexContainer*> resources used to represent OCF Servers

Reasons for deletion

An OCF-IPE shall explicitly delete <*flexContainer*> resources it is using to represent OCF Servers when the OCF-IPE detects that one or more OCF Servers among the set of exposed OCF Servers shall not be exposed to the oneM2M side any longer (e.g. due to removal from the OCF Proximal IoT Network), see step 005c in clause 8.1.2.1.

When the OCF-IPE intends to de-register - i.e. when it is planning to delete its own <*AE*> resource - any remaining child <*flexContainer*> resources will be deleted implicitly.

However, in both cases, certain preparations have to be performed for a proper end of exposure of OCF Servers.

Handling of Access Control Privileges

In order to avoid any inconsistencies between linked resources and to avoid inconsistent exposure of information on which OCF services are exposed, it is recommended that the exposure of OCF services should be stopped before any of the following actions are taken. This is accomplished by adjusting Access Control Privileges such that no new requests will proceed to consume the services which shall no longer be exposed.

Update of parent <*AE*> resource before <*flexContainer*> deletion

This only applies when the OCF-IPE is intending to stop exposure of OCF services for a sub-set of the exposed OCF Server it is handling so far. In case the OCF-IPE intends to de-register, this update action is not needed.

Before deletion of any <*flexContainer*> resources used to represent OCF Servers the OCF-IPE shall remove any "piid" property (Protocol Independent ID) values of the OCF Servers that are meant to be no longer exposed from the *labels* attribute under the "Iwked-Entity-IDs" key, see clause 7.1.2.2 of the present document.

Cleaning up linkage with <*node*> resources

Before deleting any <*flexContainer*> resources it is using to represent OCF Servers, an OCF-IPE shall remove any linkage from the *hostedServiceLinks* attribute of the <*node*> resource representing the OCF Platform that hosts a given OCF Server and the respective <*flexContainer*> representing that OCF Server. In case the *hostedServiceLinks* attribute of that <*node*> resource does not contain any other resource identifiers, the <*node*> resource itself should be deleted as well, however, this is an implementation choice.

When an OCF-IPE is preparing to de-register, it shall also perform the described removal of such linkage from <*node*> resources to <*flexContainer*> resources it is using to represent OCF Servers, including the potential deletion of the respective <*node*> resources in case no other <*flexContainer*> resources are linked via the *hostedServiceLinks* attribute.

Explicit or implicit deletion

After all the conditions outlined in this clause are met, an OCF-IPE can either explicitly delete <*flexContainer*> resources it is using to represent OCF Servers which are meant to be no longer exposed or it can de-register, which has the effect of implicitly deleting all remaining <*flexContainer*> resources the OCF-IPE is using to represent OCF Servers.

8.1.2.3 <*node*> and [*deviceInfo*] resources representing OCF Devices

8.1.2.3.1 Creation

The physical hardware on which an OCF Server is hosted is termed OCF Platform in OCF specifications. It shall be represented by a <*node*> resource and a linked [*deviceInfo*] resource in line with the attribute settings defined in clause 7.1.1. Therefore, for each OCF Server for which a <*flexContainer*> resource is getting created, see clause 8.1.2.2, the OCF-IPE shall check if its own Registrar CSE hosts a <*node*> resource matching with the OCF Platform of the represented OCF Server. A match can be detected by comparing the *nodeID* attribute of all candidate <node> resources against the "pi" property (Platform ID) of the OCF resource with the pre-defined URI "/oic/p" of the respective OCF Device as defined in the OCF Core Specification [7]. If no match is found, a new <*node*> resource and a new [*deviceInfo*] resource shall be created, jointly representing the OCF Platform. The attribute settings of this pair of new resources and the linkage among them are defined in detail in clause 7.1.1.

8.1.2.3.2 Linkage with <*flexContainer*> resources

A proper linkage between <*flexContainer*> resources representing OCF Servers and a <*node*> resource representing the OCF Platform hosting the respective OCF Server shall be established. The *nodeLink* attribute of <*flexContainer*> resources representing OCF Servers shall be set to the resource identifier of the <*node*> resource representing the OCF Platform which hosts that OCF Server. The *hostedServiceLinks* attribute of a <*node*> resource representing an OCF Platform shall contain a list of resource identifiers of all <*flexContainer*> resources representing OCF Servers hosted on that OCF Platform. Note that more than one resource identifier can be present in the *hostedServiceLinks* attribute of the <*node*> resource when more than one OCF Server is hosted on the same OCF Platform.

8.1.2.3.3 Deletion

As long as a <*node*> resource representing an OCF Platform is linked via its *hostedServiceLinks* attribute to at least one <*flexContainer*> resource representing an exposed OCF Server, the <*node*> resource shall not be deleted. When all links to <*flexContainer*> resource representing an exposed OCF Server have been removed from the *hostedServiceLinks* attribute, this attribute shall not be present in the respective <*node*> resource any longer. In that case the <*node*> resource should get deleted by the OCF-IPE, however, this is an implementation choice.

8.1.3 Mirroring state of exposed OCF Servers in oneM2M Resources

8.1.3.1 Establishment of monitoring

Once the appropriate set of resources to represent an OCF Server on the oneM2M side has been created, it is important to reflect accurate state information in the oneM2M resources so that they are kept consistent with the actual state of the OCF Servers that they represent.

In order to do so, the OCF-IPE shall establish monitoring of the state of all exposed OCF Servers. Such monitoring shall be accomplished by initializing and subsequently maintaining the "observe" mechanism as defined in the OCF Core Specification [7] for the respective OCF resources hosted on the respective OCF Servers. Using this observe mechanism enables the OCF-IPE to be informed about any state changes occurring in the exposed OCF Servers. The establishment of this monitoring is a pre-requisite for exposing OCF Servers as outlined in step 002c of clause 8.1.2.1.

Establishment of monitoring for all relevant OCF resources requires the OCF-IPE to issue a number of requests on the OCF side with an "observe" option to retrieve all OCF Resources implementing OCF Device functions on all exposed OCF Servers. Using this "observe" option means that in addition to an initial response, subsequent responses will follow on each and every change of state in the observed resource. Therefore, the OCF-IPE shall be able to receive these subsequent responses and process them according to clause 8.1.3.2.

8.1.3.2 Mirroring of state information

Upon reception of state information of OCF resources via the previously established observe mechanism, the OCF-IPE shall identify the oneM2M resource that corresponds to the observed OCF resource and translate the received observation into the corresponding request to update the state of the oneM2M resource representing the modified OCF resource. This procedure corresponds to step 002d in clause 8.1.2.1.

In order to avoid excessive discovery requests to find the right oneM2M resources for mirroring state information, the OCF-IPE shall keep a record of the mapping between OCF resources it observes and the corresponding oneM2M resources.

8.1.3.3 Stop monitoring

When an OCF Server shall no longer be exposed to the oneM2M side - this happens when steps 005c and 006 in clause 8.1.2.1 occur - then the previously established monitoring of the resources hosted by this particular OCF Server using the OCF observe mechanism needs to be terminated to avoid any further responses being sent to the OCF-IPE when state changes of these resources happen. Therefore, the OCF-IPE needs to cancel the observation of the resources it was so far observing for the given OCF Server by sending it a request indicating cancellation of the respective observation process.

8.1.4 Detection of requests from oneM2M entities to execute exposed OCF services and invocation thereof

8.1.4.1 Monitoring of oneM2M resources representing OCF Servers

In order to find out when a properly authorized oneM2M entity would like to consume an OCF Service, the OCF-IPE needs to rely on subscriptions to the oneM2M resources that are representing the exposed OCF Servers. Subscriptions shall be established by the OCF-IPE to get notified whenever an authorized oneM2M entity is modifying the state of a oneM2M resource representing and exposing an OCF Server, where that state change needs to be translated into a corresponding state change request on the OCF side. This mechanism is part of step 002a in clause 8.1.2.1.

Note that not all services provided by an OCF Server require a state change of resources hosted on that OCF Server by the entity that is intending to consume that service. For instance an OCF Server that only provides the status of a window contact sensor may be implemented using a read-only resource that reflects the current state of the contact sensor. In such a configuration, exposure of the service to oneM2M only requires state mirroring from the OCF side to the oneM2M side as already described in clause 8.1.3.

In general, however, services provided by an OCF Server - for instance a light - may require monitoring of state changes initiated on the oneM2M side in order to detect when a state change needs to be requested on the OCF side - for instance when a an OCF light needs to be switched on or off by a oneM2M entity. Therefore, the OCF-IPE needs to decide which resources representing OCF Servers on the oneM2M side it needs to subscribe to. This decision depends on the specific device model as defined in oneM2M TS-0023 [6] that was used to create the respective oneM2M resources representing OCF Servers. Only those resources that are meant to be modified (updated or deleted) by the service consuming entity need to be subscribed to.

When supported by the hosting CSE, the OCF-IPE shall use subscriptions with the condition tag *notificationEventType* in the *eventNotificationCriteria* attribute of the <*subscription*> resources set to "G". This type of subscription will block any update request to the subscribed-to resource while sending a notification to the OCF-IPE and waiting for a response from the OCF-IPE. Only after receiving a response, the hosting CSE will complete the requested update operation. The outcome of the update operation will then depend on the status indicated in the notification response. This allows the OCF-IPE to take appropriate actions on the OCF side, see clause 8.1.4.2, before actually allowing a state change on oneM2M resource which are actually representing state that resides in OCF resources.

When the hosting CSE does not support setting "G" for the condition tag *notificationEventType* in the *eventNotificationCriteria* attribute of the <*subscription*> resource - for instance due to being implemented against on older release of oneM2M specifications - then the OCF-IPE has to take case of any remaining state alignments needed after the OCF interaction completed, see also clause 8.1.4.2.

8.1.4.2 Invocation of OCF services

The procedure outlined in this clause correspond to step 005a in clause 8.1.2.1.

When the OCF-IPE has successfully established all pre-requisites for exposing a set of OCF-Servers to oneM2M - see step 002 in clause 8.1.2.1 - and when it has initiated the exposure - see steps 003 and 004 in clause 8.1.2.1 - it needs to detect relevant state changes of oneM2M resources that need to be translated into OCF requests for corresponding state changes. As specified in clause 8.1.4.1, the OCF-IPE is supposed to receive notification on such events based on subscriptions established earlier.

However, when receiving notifications triggered by the subscriptions established according to clause 8.1.4.1, not all notifications received will need to be translated into corresponding OCF requests. For instance if a notification was sent because of an update request issued by the OCF-IPE itself due to an incoming OCF observation, it shall not translate that back into another OCF request to avoid loopbacks. Furthermore, update requests on the oneM2M side may trigger a notification request while the actual state of the resource is not altered - e.g. when switching power state from on to on. Also in that case, the OCF-IPE shall not trigger any action on the OCF side.

Therefore, notifications received by the OCF-IPE need to be evaluated first and the OCF-IPE needs to decide whether a state change request is needed on the OCF side. If so, the OCF-IPE shall issue the corresponding state change request on the OCF side. Which exact request that is and what changed state values to request depends on the specific device model as defined in oneM2M TS-0023 [6] that was used to create the respective oneM2M resources representing OCF Servers.

Upon completion of the OCF interaction - in case the OCF decided to initiate one - or after deciding that no OCF interaction was needed after receiving a notification, the OCF-IPE shall send a notification response. The following cases need to be treated differently:

1) Subscription was established with the condition tag *notificationEventType* in the *eventNotificationCriteria* attribute of the <*subscription*> resources set to "G":

   a) No operation on the OCF side was needed: Send back a notification response back indicating successful reception of the notification and successful completion of requested operation.

   b) A request was issued on the OCF side: Send a notification response back indicating a successful reception of the notification and a status for the requested operation corresponding to the outcome of the requested OCF operation.

2) Subscription was established with a different setting of the condition tag *notificationEventType* in the *eventNotificationCriteria* attribute of the <*subscription*> resources or with no setting:

   a) No operation on the OCF side was needed: Send back a notification response back indicating successful reception of the notification.

   b) A request was issued on the OCF side: Send a notification response back indicating a successful reception of the notification. If the requested operation on the OCF side resulted in a different state than the current state of the subscribed-to resource, re-adjust the state of the subscribed to resource accordingly.

In order to better understand case 2b above a short example is provided:

a) oneM2M entity tries to switch an OCF light from on to off;

b) State in oneM2M resource representing OCF light gets changed;

c) Notification request is sent to OCF-IPE;

d) OCF-IPE request OCF Server to turn off light;

e) OCF Server denies request (might be overridden by some locking);

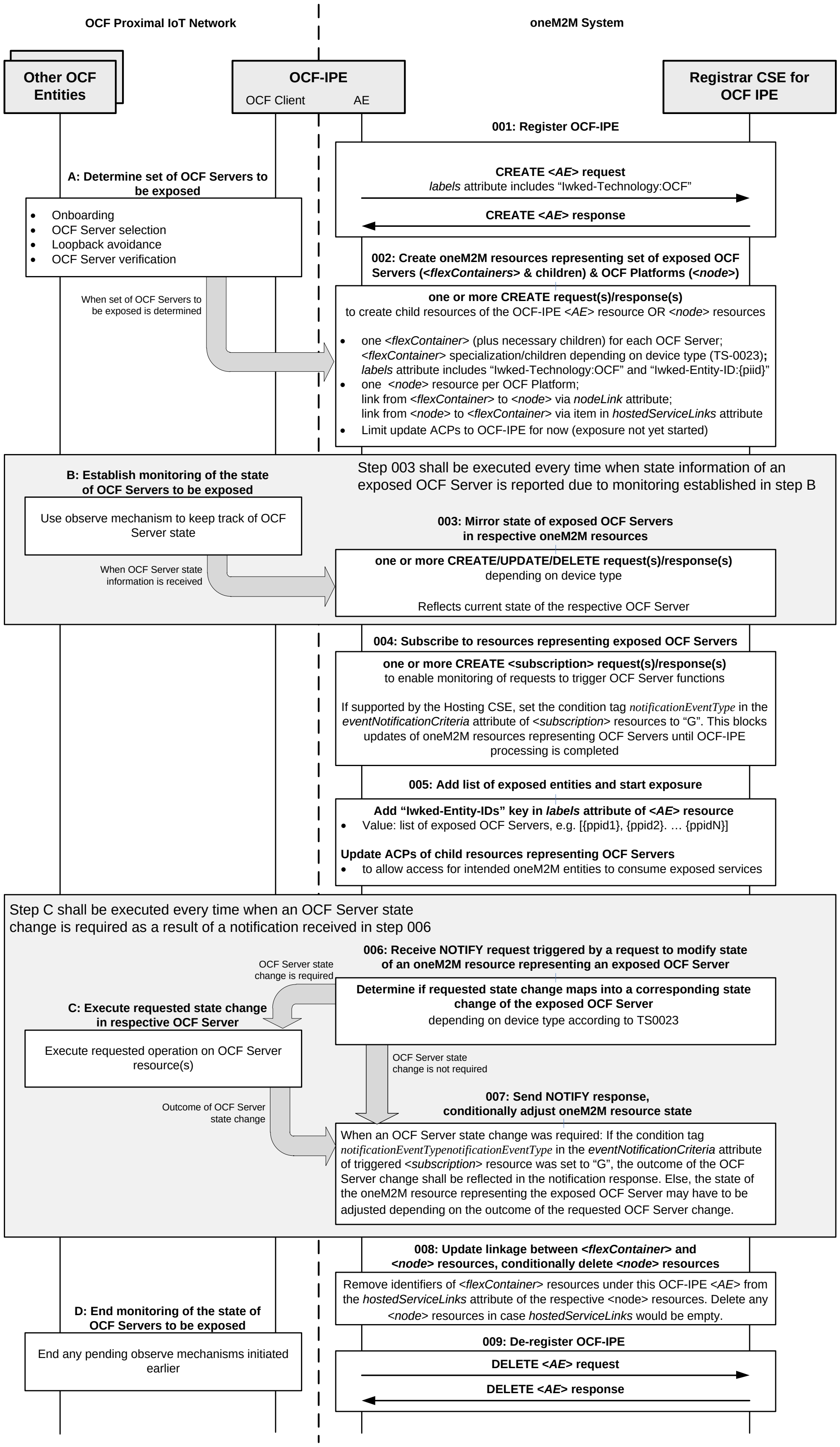
f) OCF-IPE sends back notification response;

g) OCF-IPE reverts state of oneM2M resource back from off to on.

8.1.5 Overall flows for procedures supporting exposure of OCF Functions to the oneM2M System

In this clause the overall flow of events and processing steps is summarized as depicted in figure 8.1.5-1 for the case that a static set of OCF Servers - only determined once during the life cycle of the OCF-IPE - is meant to be exposed to the oneM2M system. For enumerating steps carried out on the OCF side the letters A-D are used, for the steps on the oneM2M side numbers 1-9 are used. All the details of the flow are defined in the previous clauses 8.1.1 through 8.1.4. In essence figure 8.1.5-1 is a more specific variant of figure 8.1.2.1-1 outlining in more details which steps happen on the OCF side versus the oneM2M side.

Note that the processing steps within the boxes shaded in grey may occur multiple times and are triggered by OCF observe responses or oneM2M notifications, respectively.


OCF Proximal IoT Network
oneM2M System
Other OCF Entities
OCF-IPE
OCF Client
AE
Registrar CSE for OCF IPE
When set of OCF Servers to be exposed is determined
When OCF Server state information is received
OCF Server state change is required
OCF Server state change is not required
Outcome of OCF Server state change

001: Register OCF-IPE

CREATE <*AE*> request
labels attribute includes "Iwked-Technology:OCF"

CREATE <*AE*> response

A: Determine set of OCF Servers to be exposed

- Onboarding
- OCF Server selection
- Loopback avoidance
- OCF Server verification

002: Create oneM2M resources representing set of exposed OCF Servers (<*flexContainers*> & children) & OCF Platforms (<*node*>)

one or more CREATE request(s)/response(s)
to create child resources of the OCF-IPE <*AE*> resource OR <*node*> resources

- one <*flexContainer*> (plus necessary children) for each OCF Server; <*flexContainer*> specialization/children depending on device type (TS-0023)**;** *labels* attribute includes "Iwked-Technology:OCF" and "Iwked-Entity-ID:{piid}"
- one <*node*> resource per OCF Platform; link from <*flexContainer*> to <*node*> via *nodeLink* attribute; link from <*node*> to <*flexContainer*> via item in *hostedServiceLinks* attribute
- Limit update ACPs to OCF-IPE for now (exposure not yet started)

B: Establish monitoring of the state of OCF Servers to be exposed

Use observe mechanism to keep track of OCF Server state

Step 003 shall be executed every time when state information of an exposed OCF Server is reported due to monitoring established in step B

003: Mirror state of exposed OCF Servers in respective oneM2M resources

one or more CREATE/UPDATE/DELETE request(s)/response(s)
depending on device type

Reflects current state of the respective OCF Server

004: Subscribe to resources representing exposed OCF Servers

one or more CREATE <subscription> request(s)/response(s)
to enable monitoring of requests to trigger OCF Server functions

If supported by the Hosting CSE, set the condition tag *notificationEventType* in the *eventNotificationCriteria* attribute of <*subscription*> resources to "G". This blocks updates of oneM2M resources representing OCF Servers until OCF-IPE processing is completed

005: Add list of exposed entities and start exposure

Add "Iwked-Entity-IDs" key in *labels* attribute of <*AE*> resource

- Value: list of exposed OCF Servers, e.g. [{ppid1}, {ppid2}. … {ppidN}]

Update ACPs of child resources representing OCF Servers

- to allow access for intended oneM2M entities to consume exposed services

Step C shall be executed every time when an OCF Server state change is required as a result of a notification received in step 006

006: Receive NOTIFY request triggered by a request to modify state of an oneM2M resource representing an exposed OCF Server

Determine if requested state change maps into a corresponding state change of the exposed OCF Server
depending on device type according to TS0023

C: Execute requested state change in respective OCF Server

Execute requested operation on OCF Server resource(s)

007: Send NOTIFY response, conditionally adjust oneM2M resource state

When an OCF Server state change was required: If the condition tag *notificationEventTypenotificationEventType* in the *eventNotificationCriteria* attribute of triggered <*subscription*> resource was set to "G", the outcome of the OCF Server change shall be reflected in the notification response. Else, the state of the oneM2M resource representing the exposed OCF Server may have to be adjusted depending on the outcome of the requested OCF Server change.

008: Update linkage between <*flexContainer*> and <*node*> resources, conditionally delete <*node*> resources

Remove identifiers of <*flexContainer*> resources under this OCF-IPE <*AE*> from the *hostedServiceLinks* attribute of the respective <node> resources. Delete any <*node*> resources in case *hostedServiceLinks* would be empty.

D: End monitoring of the state of OCF Servers to be exposed

End any pending observe mechanisms initiated earlier

009: De-register OCF-IPE

DELETE <*AE*> request

DELETE <*AE*> response

Figure 8.1.5-1: Overall flow of processing steps when exposing a static set of OCF Servers to oneM2M entities

8.2 Procedures supporting exposure of native oneM2M services to an OCF Proximal IoT Network

8.2.1 Determination of oneM2M services to be exposed to the OCF Proximal IoT Network

In a oneM2M system, the specific setup and security parameters to be used by AEs intending to consume specific services exposed via oneM2M resources - such as the set of resource IDs of resources representing the services to be consumed or credentials and access control privileges to access those resources - are assumed to be established before the consuming AE is supposed to consume a specific service. The oneM2M specifications do not define a standardized procedure to establish these pre-requisites for consuming specific services. While procedures, such as discovery of resources or registration of Application-IDs, can help to find and identify the resources that an AE may possibly access to consume specific services, there is no standardized onboarding procedure defined in oneM2M specifications, that would support a uniform mechanism to find specific services and establish adequate credentials and access control parameters to enable consumption of the respective services. Therefore, the identification of a specific set of resources representing services that an AE may want to consume as well as the establishment of the required security credentials and access control parameters needs to rely on implementation-dependent procedures that are not within the scope of oneM2M specifications. Also dynamic establishment of identifiers and credentials for authorization can be used for this purpose, see oneM2M TS-003 [4] for more information.

As for any other AE which is meant to consume a specific set of services exposed to oneM2M entities by a specific set of resources, or an OCF-IPE intending to expose services represented by oneM2M resources, they will have to go through the establishment of the afore-mentioned pre-requisites:

- the OCF-IPE will have to determine the set of oneM2M resources representing the services that are meant to be exposed to the OCF Proximal IoT Network, and
- security credentials and access control privileges need to be established such that the OCF-IPE is allowed to consume the respective services represented via the set of determined oneM2M resources.

Note that it is possible that the set of oneM2M services to be exposed to a given OCF Proximal IoT Network may not be static, i.e. oneM2M services to be exposed to a given OCF Proximal IoT Network may be added or removed over time. In that case, the OCF-IPE responsible for the exposure to the OCF Proximal IoT Network needs to be capable of dynamically learning about such changes in the set of exposed oneM2M services and instantiate or remove virtual OCF Servers representing the exposed services in a given OCF Proximal IoT Network.

In the text below, three different concepts of determining the set of oneM2M services to be exposed to an OCF Proximal IoT Network are outlined. However, it is not in the scope of the present document to define details on how to implement these concepts:

- Pre-Provisioning: The set of oneM2M services to be exposed to the OCF Proximal IoT Network and the corresponding set of oneM2M resources representing those services are determined before the OCF-IPE is initiated. The details of the selection procedure are not described in any further detail. The resulting selection is provided to the OCF-IPE by means of configuration information - see circle termed "Configuration" in figure 6.2.2-1 - stored statically in storage accessible by the OCF-IPE such as a configuration file or a set of <*contentInstance*> resources. It is not in the scope of this description to define any details of the storage mechanism such as storage location, format, serialization etc. of the selected set of oneM2M services. Upon initiation of the OCF-IPE it shall verify that the configured oneM2M services to be exposed to an OCF Proximal IoT Network are actually accessible on the oneM2M side by attempting to access the respective oneM2M resources representing the configured oneM2M services to be exposed. If any of the configured oneM2M services are not accessible in the oneM2M system, the corresponding entries need to be removed from the set of oneM2M services to be exposed to the OCF Proximal IoT Network by the OCF-IPE.

- Discovery: When the OCF-IPE is initiated, it triggers a discovery of oneM2M resources representing oneM2M services of interest to the OCF-IPE using some given constraints, e.g. limiting the discovery to a specific Hosting CSE. Among the discovered oneM2M resources, a set of resources representing services to be exposed to the OCF Proximal IoT Network is selected by the stakeholder responsible for the OCF-IPE deployment. This selection may be implemented by a user-facing interface (GUI) or by other means and is not in the scope of the present description. Discovery results may also get filtered by the OCF-IPE before selecting the oneM2M services to be exposed to the OCF Proximal IoT Network. For example, the set of discovered oneM2M services can be filtered in order to limit the exposure to the OCF Proximal IoT Network to a specific set of oneM2M services. For instance the discovery results may get filtered to match with a given manufacturer name or a specific model name as indicated by the *manufacturer* or *model* attributes of a [*deviceInfo*] child-resource of a <*node*> resource representing the device providing the discovered oneM2M service. In addition to the described discovery and selection of oneM2M services to be exposed, the OCF-IPE needs to be configured in the oneM2M system with appropriate credentials and access control privileges that are sufficient to allow access to the selected oneM2M services intended to be exposed to the OCF Proximal IoT Network.

- On demand determination: This selection concept is very similar to the one described in the previous bullet point, except that the discovery of oneM2M services to be exposed to the OCF Proximal IoT Network is triggered by means of changing the state of a oneM2M resource - see the dashed box termed "Resource instances to trigger discovery/change of set of exposed native oneM2M function(s)" in figure 6.2.2-1. This specification does not define details for this triggering mechanism which is an implementation choice. In the remainder of this paragraph an example is given. For instance a <*container*> resource may get created by the OCF-IPE when it starts and a subscription to that <*container*> resource would be established for the OCF-IPE to get notified about creation of any new <*contentInstance*> resources in that <*container*> along with ACPs that would control which entities are authorized to trigger the OCF discovery. Upon creation of a new <*contentInstance*> child resource in that <*container*> resource, the OCF-IPE would get notified. The information in the *content* attribute of the new <*contentInstance*> resource may be used to define parameters for the discovery to be executed such as filtering oneM2M resource discovery results to match with a specific manufacturer name and a specific model name as indicated by the *manufacturer* and *model* attributes of [*deviceInfo*] child-resources of discovered <*node*> resources representing candidate devices providing oneM2M services. The notification would then result in the OCF-IPE initiating a new discovery and selection procedure as described in the previous paragraph. After that is completed, the resource used to trigger the discovery and selection process may need to get cleaned up - i.e. the <*contentInstance*> resource may need to get removed.

Independent of which selection concept is implemented, the security and access control privileges of the OCF-IPE in the oneM2M side need to be established such that the OCF-IPE is authorized to interact as intended with the selected oneM2M services.

For instance if the OCF-IPE will act as a service consuming AE with the intent to be able to switch on or off a set of lights exposed via a set of oneM2M resources, the provisioned IDs, credentials and access control privileges need to enable the OCF-IPE to actually switch on or off the intended set of lights.

The present specification does not contain any details on how such consistency between the provisioned set of credentials, IDs and access control privileges for the OCF-IPE and the selection of the oneM2M services to interact with can be achieved, since this is implementation dependent. The stakeholder responsible for deploying and provisioning the OCF-IPE needs to be aware that the selected set of oneM2M Services for which the OCF-IPE will get provisioned with credentials that allow access to that set of services will actually be exposed to the OCF Proximal IoT Network. On the OCF side, appropriate security credentials need to be setup in order to control which OCF Clients are authorized to consume the services provided by the set of exposed oneM2M resources.

As specified in clauses 7.2 and 8.2.2, a virtual OCF Server instantiated by an OCF-IPE shall use a value for the "dmno" (Model Number) property of the device resource with the pre-defined URI "/oic/d" that starts with the string "oneM2M-" followed by a concatenation of the M2M-SP-ID and AE-ID of the OCF-IPE that instantiated the virtual OCF Server and a value for a model number, see also table 7.2-2. This mechanism is needed in order to detect a possible loop of exposing services from one oneM2M SP domain to an OCF Proximal IoT Network and back to the same oneM2M SP domain. As described in clause 8.1.1 the OCF-IPE needs to verify that none of the OCF Servers it intends to expose to oneM2M are actually virtual OCF Server(s) that were previously instantiated by an OCF-IPE interfacing to the same oneM2M SP domain.

For the opposite direction - so to avoid a potential loop of exposing OCF Servers to oneM2M via the creation of corresponding oneM2M resources and then exposing that same set of oneM2M resources back to the original OCF Proximal IoT Network - the OCF-IPE needs to check that none of the oneM2M resources selected for exposure to a given OCF Proximal IoT Network are actually representing an OCF Service that was previously exposed to the oneM2M system. In order to do so, the OCF-IPE intending to expose a specific oneM2M service represented by a specific <*flexContainer*> resource needs to check if a Key:Value pair is present in the labels attribute of that specific <*flexConatiner*> for which the value would match the "piid" property (Protocol Independent ID) of the device resource with the pre-defined URI "/oic/d" of any of the discoverable OCF Servers present in the targeted OCF Proximal IoT Network. If that is the case, the respective <*flexContainer*> resources shall not be exposed to the OCF Proximal IoT Network since it is in fact already an exposed mirror of a native OCF resource in that same OCF Proximal IoT Network.

As a result of establishing all pre-requisites and the selection of the set of oneM2M resources to be exposed to a given OCF Proximal IoT Network, it is assumed in the remainder of the present specification that the following applies:

- The OCF-IPE is registered as a oneM2M AE with appropriate credentials and access control privileges to access the set of oneM2M services selected by the stakeholder responsible for the OCF-IPE deployment for exposure to the OCF Proximal IoT Network.

- A valid set of oneM2M resources representing the set of services to be exposed to the OCF Proximal IoT Network has been determined including avoidance of loopback of services exposed from the OCF Proximal IoT Network to the oneM2M SP domain and back to the same OCF Proximal IoT Network.

- The set of resource IDs identifying the set of oneM2M resources which represent the services to be exposed to the OCF Proximal IoT Network is known to the OCF-IPE.

8.2.2 Instantiation/removal of OCF Servers representing exposed oneM2M services

8.2.2.1 High-level procedure to expose oneM2M services

When an OCF-IPE completes registration with its Registrar CSE, an <*AE*> resource representing that OCF-IPE is created as a result of that registration. As specified in clause 7.1.2.2, the *labels* attribute of this <*AE*> resource shall reflect the fact that this AE is an OCF-IPE by adding a Key:Value pair set to "Iwked-Technology:OCF", see table 7.1.2-1. The registration of the OCF-IPE including a successful creation of the <*AE*> representing the OCF-IPE is a pre-requisite for instantiating any virtual OCF Servers representing oneM2M services exposed by this specific OCF-IPE. Note that the same OCF-IPE may also expose OCF Services to the oneM2M system, however, independent OCF-IPEs may also be used to implement exposure in the two different directions. This is an implementation choice.

For each oneM2M service that is exposed to a given OCF Proximal IoT Network by a specific OCF-IPE, the oneM2M resource ID of the top-level <*flexContainer*> resource representing that service shall be added to the list of IDs under the Key "Exposed-Resource-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE as defined in table 7.1.2-1. The addition of this oneM2M resource ID shall be performed when all subscriptions for exposing that oneM2M service to the OCF Proximal IoT Network have been established and a corresponding virtual OCF Server has been instantiated, see clauses 8.2.2.2, 8.2.3 and 8.2.4 for more details. **Step 002** below defines the pre-requisites in detail.

When the OCF-IPE detects that a specific oneM2M service is not accessible any longer - e.g. when the corresponding set of oneM2M resources are deleted - the OCF-IPE shall remove the oneM2M resource ID of the top-level <*flexContainer*> resource representing that service from the list of IDs under the Key "Exposed-Resource-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE. In this case the OCF-IPE shall also terminate the corresponding virtual OCF Server offering services provided by the respective oneM2M service that is not accessible any longer, see also clause 8.2.2.2. It is an implementation choice of the OCF-IPE to choose an appropriate timeout for detecting the absence of an oneM2M service after an attempt to access it has not resulted in a valid response. Furthermore, it is also an implementation choice of the OCF-IPE to re-try to discover and expose oneM2M services which have previously been exposed to the OCF Proximal IoT Network but have been removed from exposure due to inability to access them.

When the OCF-IPE detects that an additional oneM2M service has to be exposed to the OCF Proximal IoT Network - this might be triggered on demand or by entering a discovery procedure on the oneM2M side from time to time as described in clause 8.2.1 - the OCF-IPE shall complete verification of access to the targeted oneM2M service and establishment of oneM2M resource state monitoring functions as described in clauses 8.2.3 as well as instantiation of a corresponding virtual OCF Server and start detection of any requests to consume the service from the OCF side as described in clause 8.1.4. Only then, the OFC-IPE shall add the oneM2M resource ID of the top-level <*flexContainer*> resource representing that service to the list of IDs under the Key "Exposed-Resource-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE.

When an OCF-IPE is going to terminate, it shall properly de-register with its Registrar CSE, i.e. it shall delete the corresponding <*AE*> resource representing the OCF-IPE. Note that an OCF-IPE may stop exposure of oneM2M services to the OCF Proximal IoT Network while continuing to expose OCF Services to the oneM2M system. Before de-registration is performed or before terminating any exposure of oneM2M services to the OCF Proximal IoT Network, the OFC-IPE shall delete any related subscriptions to oneM2M resources that it has previously created in order to monitor the state of exposed oneM2M resources.

Figure 8.2.2.1-1 depicts a high-level flow of events and processing steps throughout the OCF-IPE life cycle regarding aspects of exposing oneM2M services to an OCF Proximal IoT Network. Some of the processing steps consist of complex sub-procedures partially relying on functionality specified in other clauses of the present document. Therefore, the description of the different steps include references to the relevant clauses of the present document. For now it should just serve the purpose of explaining the various actions the OCF-IPE has to take in order to comply with the specified way to expose oneM2M services to an OCF Proximal IoT Network. Details of the more complex processing steps are defined in subsequent clauses of the present document.

Step 001: Register OCF-IPE
The OCF-IPE registers with its Registrar CSE. The representation of the <*AE*> resource which is requested to be created shall contain a *labels* attribute which includes a "key:value" pair of "Iwked-Technology:OCF". Note that in case the OCF-IPE handles exposure in both directions, this step is the same as Step 001 in figure 8.1.2.1-1.

Step 002: Establish pre-requisites
In order to perform a proper exposure of oneM2M services to the OCF Proximal IoT Network, some pre-requisites have to be met. Step 002 contains what is needed to establish those pre-requisites. In particular the following needs to be completed:

a) The set of oneM2M resources representing oneM2M services to be exposed to the OCF Proximal IoT Network has to be determined, see clause 8.2.1 for a description on how to accomplish that. It is necessary to ensure that the OCF-IPE and Hosting CSE(s) for the exposed resources are provisioned with the proper security credentials and access control privileges to access the set of oneM2M resources to be exposed. Besides proper provisioning and selection of the set of oneM2M resources to be exposed, the OCF-IPE shall also verify that it is able to access each of the selected oneM2M resources and discard oneM2M resources for which access is not possible. The set of oneM2M resources to be exposed shall be characterized by the list of resource IDs under the Key "Exposed-Resource-IDs" in the *labels* attribute of the <*AE*> resource representing that OCF-IPE as defined in table 7.1.2-1, see Step 003.

b) Once the set of oneM2M resources to be exposed is determined, the OCF-IPE shall instantiate an OCF Bridge Device - see clause 8.2.2.2.1 for more details - to support discovery for exposed oneM2M service on the OCF side. The OCF-IPE shall also instantiate virtual OCF Server(s) to represent the exposed oneM2M services. Depending on the oneM2M services, their information models and the normative mapping to OCF Device types and resource types as defined in OCF Device-Specification [8] and oneM2M TS-0023 [6], a separate OCF resource structure shall be created in the previously instantiated virtual OCF Server for each top-level oneM2M <*flexContainer*> representing an exposed oneM2M service, see clause 8.2.2.2. It is recommended that access control for the resources on such a newly instantiated virtual OCF Server is set at this point in time to block any access by entities other than the OCF-IPE until Step 0004 is completed.

c) After instantiation of the virtual OCF Server(s) needed by the OCF-IPE to expose oneM2M services to OCF, the OCF-IPE shall establish monitoring of the state of the exposed oneM2M resources by using the subscription mechanism. The OCF-IPE shall be able to detect changes of state of the exposed oneM2M resources. The OCF-IPE shall also ensure that this monitoring is continuously performed throughout the lifecycle of the OCF-IPE. At this point in time, the OCF-IPE shall mirror the state of the monitored oneM2M resource(s) at least once in the respective OCF Server resource(s)

d) Upon reception of a state change notification from exposed oneM2M resource(s), the OCF-IPE shall mirror that state change by updating the corresponding virtual OCF Server resource(s) created earlier, see clause 8.2.3 for more details. This particular sub-step 002d - i.e. the task to mirror any reported state changes of exposed oneM2M resource(s) to the state of the corresponding virtual OCF Server resources - is actually a procedure that can be triggered asynchronously throughout the lifetime of the OCF-IPE and shall be executed as many times as needed.

Step 003: Add list of exposed entities
The OCF-IPE has established all pre-requisites to start the exposure of the oneM2M service(s) to OCF. Before doing so, the OCF-IPE needs to include a list of all oneM2M resource IDs of the top-level <*flexContainer*> resources representing the exposed oneM2M service(s) in the *labels* attribute of its own <*AE*> resource as a "key:value" pair in line with the format "Exposed -Entity-IDs:[ID1, ID2, ID3]", see clause 7.1.2.2.

Step 004: Start exposure
In order to start the actual service exposure of oneM2M services to OCF Clients, the OCF-IPE needs to enable discovery/introspection for the virtual OCF Servers it has instantiated. The OCF-IPE needs to support credentials that allow authorized OCF Clients to access the resources on these OCF Servers. This will be handled by the onboarding process on the OCF side. The OCF Servers instantiated in Step 002 above shall then start listening to and processing of incoming requests of OCF Clients.

Steps 005a, 005b, 005c define conditional procedures which shall be carried out under the conditions defined in the specific step descriptions below. They can be triggered asynchronously - i.e. not in the order described in the present flow chart, not at any pre-defined time and not in any particular order of execution. The execution of the procedures defined for each of these steps shall be executed as many times as needed.

Step 005a: Process OCF request to consume oneM2M service
This processing step is triggered asynchronously when receiving a request to change state in an OCF resource that is representing an exposed oneM2M resource. The OCF-IPE shall decide on the need for issuing a corresponding request for state change of the corresponding oneM2M resource and execute the corresponding request on the oneM2M side if needed. The OCF-IPE shall conditionally adjust the OCF resource state depending on the outcome of executed oneM2M operation(s) and send a response to the received request. Details for this step are defined in clause 8.2.4. Since this step is triggered by occurrences of requests issued by OCF Clients asynchronously in the OCF Proximal IoT Network, the OCF-IPE shall execute this step for each of these requests it receives.

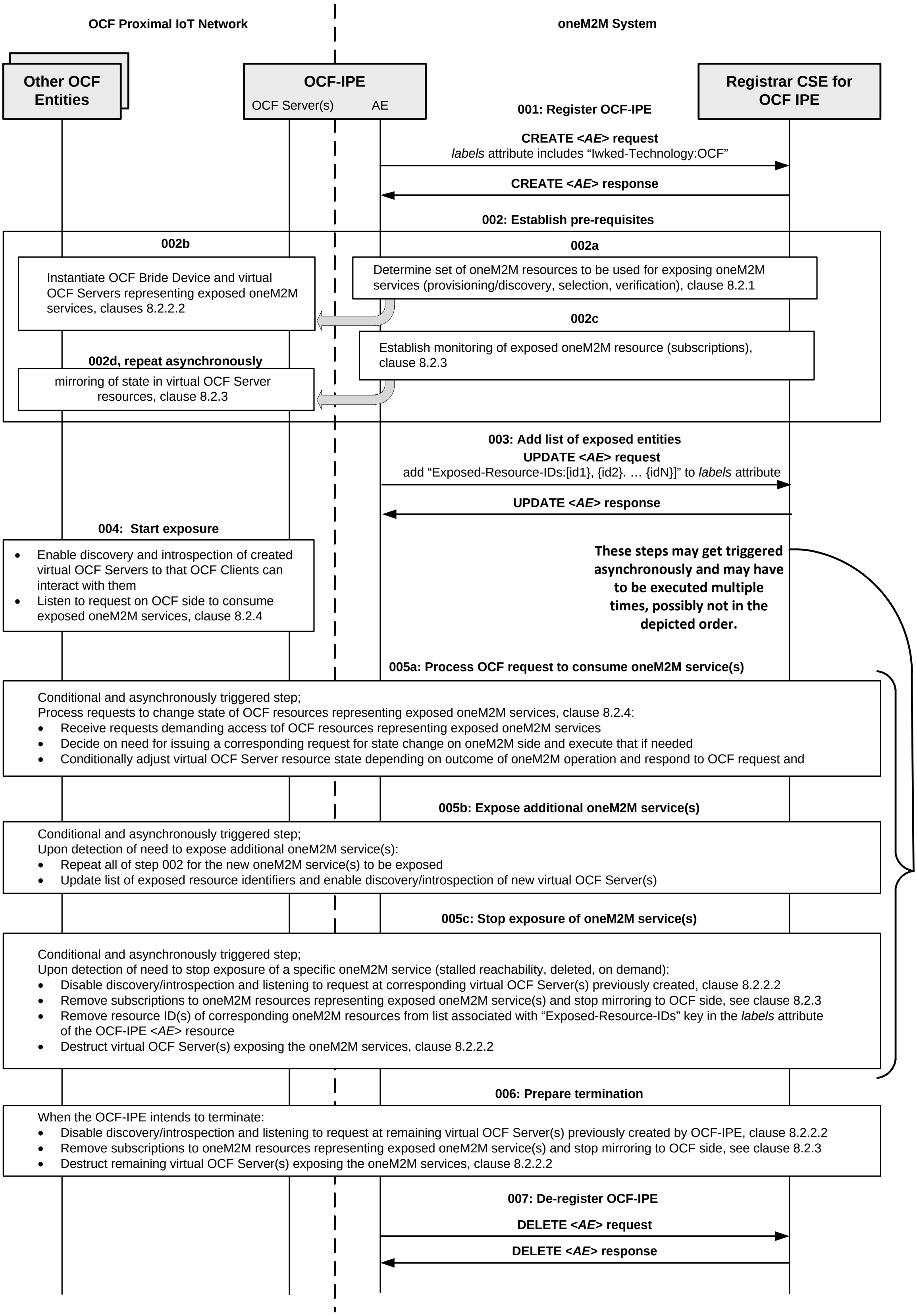
Step 005b: Expose additional oneM2M service(s)
This processing step is triggered asynchronously when the OCF-IPE detects a need to expose additional oneM2M service(s). As described in clause 8.2.1, the set of oneM2M resources to be exposed to OCF may change dynamically (e.g. addition on demand or by asynchronous discovery on the oneM2M side). It is possible that additional oneM2M services are identified and are intended to be exposed via an already initialized OCF-IPE. In such a case all the pre-requisites listed for step 002 need to be established for each additional oneM2M service to be exposed. After these pre-requisites are met, the OCF-IPE needs to update the list of oneM2M resource IDs of all exposed oneM2M resources in the *labels* attribute of its own <*AE*> resource as a "key:value" pair in line with the format "Exposed-Resource-IDs:[ID1, ID2, ID3]", see clause 7.1.2.2. Ultimately the OCF-IPE needs to access control for the OCF resources representing the additionally exposed oneM2M service(s) so that the intended OCF Clients can consume the offered services. Step 005b shall be executed when the OCF-IPE detects the need to expose additional oneM2M service(s) which are currently not exposed to the OCF side. Methods for detecting such conditions are out of the scope of the present specification.

Step 005c: Stop exposure of specific oneM2M service(s)
Upon detection of need to stop exposure of a specific oneM2M service - e.g. when its reachability stalled or on demand - the OCF-IPE needs to go through the following procedure. Initially, the OCF-IPE shall disable support for discovery/introspection/listening to requests at the corresponding virtual OCF Server resources to stop OCF Clients from finding the service(s) to be terminated, see clause 8.2.2.2. After that, the OCF-IPE shall stop any monitoring and mirroring of state of the oneM2M resources into the corresponding OCF resources established in steps 002c and 002d, see clause 8.2.3, including removal of any subscriptions on the oneM2M side. Then the OCF-IPE shall remove the corresponding oneM2M resource IDs from the list associated with "Exposed-Resource-IDs" key in the *labels* attribute of the OCF-IPE <*AE*> resource. Finally, the OCF-IPE shall destruct the virtual OCF Server representing the exposed oneM2M services that are subject to end of exposure, see clause 8.2.2.2.

Step 006: Prepare termination
When the OCF-IPE intends to terminate, it shall stop any active procedures for monitoring and mirroring of state of any of the remaining exposed oneM2M service(s), see steps 002c and 002d as well as clause 8.2.3 including removal of any subscriptions still active for monitoring the exposed oneM2M resources. Finally, the OCF-IPE shall destruct any remaining virtual OCF Servers it has instantiated previously.

Step 007: De-register OCF-IPE
The OPC-IPE shall delete the <*AE*> resource representing this OCF-IPE which will result also in deletion of all its child resources.

After successful completion of the de-registration, the OCF-IPE has been terminated from a oneM2M perspective. It is an implementation choice of the OCF-IPE whether it keeps its registration alive or is attempts to re-register at later points in time, e.g. for initiating further discovery procedures to discover oneM2M service(s) to be exposed in the future. These implementation choices are not in scope of the present specification.



001: Register OCF-IPE

CREATE <*AE*> request
labels attribute includes “Iwked-Technology:OCF”

CREATE <*AE*> response

002: Establish pre-requisites

002a

Determine set of oneM2M resources to be used for exposing oneM2M services (provisioning/discovery, selection, verification), clause 8.2.1

002b

Instantiate OCF Bride Device and virtual OCF Servers representing exposed oneM2M services, clauses 8.2.2.2

002c

Establish monitoring of exposed oneM2M resource (subscriptions), clause 8.2.3

002d, repeat asynchronously

mirroring of state in virtual OCF Server resources, clause 8.2.3

003: Add list of exposed entities

UPDATE <*AE*> request
add “Exposed-Resource-IDs:[id1}, {id2}. … {idN}]” to *labels* attribute

UPDATE <*AE*> response

004: Start exposure

- Enable discovery and introspection of created virtual OCF Servers to that OCF Clients can interact with them
- Listen to request on OCF side to consume exposed oneM2M services, clause 8.2.4

These steps may get triggered asynchronously and may have to be executed multiple times, possibly not in the depicted order.

005a: Process OCF request to consume oneM2M service(s)

Conditional and asynchronously triggered step;
Process requests to change state of OCF resources representing exposed oneM2M services, clause 8.2.4:

- Receive requests demanding access tof OCF resources representing exposed oneM2M services
- Decide on need for issuing a corresponding request for state change on oneM2M side and execute that if needed
- Conditionally adjust virtual OCF Server resource state depending on outcome of oneM2M operation and respond to OCF request and

005b: Expose additional oneM2M service(s)

Conditional and asynchronously triggered step;
Upon detection of need to expose additional oneM2M service(s):

- Repeat all of step 002 for the new oneM2M service(s) to be exposed
- Update list of exposed resource identifiers and enable discovery/introspection of new virtual OCF Server(s)

005c: Stop exposure of oneM2M service(s)

Conditional and asynchronously triggered step;
Upon detection of need to stop exposure of a specific oneM2M service (stalled reachability, deleted, on demand):

- Disable discovery/introspection and listening to request at corresponding virtual OCF Server(s) previously created, clause 8.2.2.2
- Remove subscriptions to oneM2M resources representing exposed oneM2M service(s) and stop mirroring to OCF side, see clause 8.2.3
- Remove resource ID(s) of corresponding oneM2M resources from list associated with “Exposed-Resource-IDs” key in the *labels* attribute of the OCF-IPE <*AE*> resource
- Destruct virtual OCF Server(s) exposing the oneM2M services, clause 8.2.2.2

006: Prepare termination

When the OCF-IPE intends to terminate:

- Disable discovery/introspection and listening to request at remaining virtual OCF Server(s) previously created by OCF-IPE, clause 8.2.2.2
- Remove subscriptions to oneM2M resources representing exposed oneM2M service(s) and stop mirroring to OCF side, see clause 8.2.3
- Destruct remaining virtual OCF Server(s) exposing the oneM2M services, clause 8.2.2.2

007: De-register OCF-IPE

DELETE <*AE*> request

DELETE <*AE*> response

Figure 8.2.2.1-1: High-level procedure to expose oneM2M services to OCF

8.2.2.2 Handling of virtual OCF Server(s) representing exposed oneM2M service(s)

8.2.2.2.1 Instantiation of an OCF Bridge Device

The OCF-IPE shall instantiate an OCF Server acting as an OCF Bridge Device with OCF Device Type set to "oic.d.bride". The main responsibility for this device is to support the discovery of all the resources hosted by all virtual OCF Servers instantiated to expose the selected oneM2M services to the OCF Proximal IoT Network.

In order to make oneM2M services exposed by the OCF-IPE via virtual OCF Servers discoverable in the OCF Proximal IoT Network, the OCF-IPE shall be responsible for hosting the mandatory OCF resource "/oic/res" which shall include a collection of all resources exposed by the OCF-IPE to the OCF Proximal IoT Network via all virtual OCF Servers that it instantiates, see the OCF Core Specification [7] for details on the structure of "/oic/res" and the OCF Bridging Specification [10] for details on responsibilities to support discovery of OCF resources.

The OCF-IPE shall generate a unique value for its own OCF device ID to be used as a value for the "di" property of its own "/oic/d" resource in line with the OCF Core Specification [7].

Instantiation and destruction of virtual OCF Servers representing exposed oneM2M services - see clauses 8.2.2.2.2 and 8.2.2.2.3 - shall be taken into account by the OCF-IPE in order to keep the content of the "/oic/res" resource of the OCF Bridge Device instantiated by the OCF-IPE up-to-date. The OCF-IPE shall be responsible to carry out corresponding updates to its OCF Bridge Device resource "/oic/res" so that other OCF entities can discover up-to-date information on the overall set of resources that are discoverable for all currently active virtual OCF Servers representing oneM2M services or be notified about any changes of that set via observations.

8.2.2.2.2 Instantiation of virtual OCF Servers

8.2.2.2.2.1 Pre-requisites

A pre-requisite to instantiate virtual OCF Servers used to expose oneM2M services to the OCF Proximal IoT Network is that the OCF-IPE has previously determined which specific set of oneM2M resources representing oneM2M services have to be exposed, see the description in clause 8.2.1 and step 002a in clause 8.2.2.1.

Proper determination of the set of oneM2M resources to expose via the considered OCF-IPE will ensure that the OCF-IPE is able to access the set of oneM2M resources representing the oneM2M services to be exposed. The OCF-IPE shall discard oneM2M resources from exposure if proper access is not possible. After this proper determination of the set of oneM2M resources to be exposed has been performed, the set of oneM2M resource IDs of the oneM2M resources to be exposed will be known to the OCF-IPE. In summary, the following shall be completed for each oneM2M service to be exposed to the OCF Proximal IoT Network before the OCF-IPE attempts to instantiate any virtual OCF Servers exposing oneM2M services to the OCF Proximal IoT Network:

- proper provisioning of credentials and access control privileges on the oneM2M side so that the OCF-IPE can discover and access the oneM2M resources representing the oneM2M services to be exposed;
- selection of set of oneM2M resources to be exposed, determination of the respective oneM2M resource IDs;
- verification of proper access to the selected oneM2M resources, discarding of inaccessible oneM2M resources;
- determination of OCF Device Types corresponding to the selected oneM2M resources for each exposed oneM2M service;
- instantiation of an OCF Device or type "oic.d.bridge" by the OCF-IPE.

These pre-requisites for the instantiation of virtual OCF Servers used to represent OCF Servers have to be established for both, the initial set of OCF Servers to be exposed (see step 002a in clause 8.1.2.1) as well as for any additional OCF Servers which may get added to the exposed set of OCF Servers later on (see step 005b in clause 8.1.2.1).

8.2.2.2.2.2 Instantiation process

Reasons for instantiation

Throughout the lifecycle of an OCF-IPE, virtual OCF Servers used to represent oneM2M services - and the resources hosted by them - shall be instantiated by the OCF-IPE in the following cases:

- when the OCF-IPE has registered and an initial set of oneM2M services to be exposed has been determined before exposure of any oneM2M services has started, see step 002a in clause 8.2.2.1;
- when an already active OCF-IPE which is already exposing a set of oneM2M services to oneM2M has detected that one or more new oneM2M services have to be added to the set of exposed oneM2M services, see step 005b in clause 8.2.2.1.

Virtual OCF Servers which are meant to represent oneM2M services - and their hosted resources - shall only be created when the pre-requisites outlined in clause 8.2.2.2.2.1 are established.

Virtual OCF Server instantiation

For a given oneM2M service to be exposed to OCF, the OCF-IPE shall instantiate a virtual OCF Server - i.e. an OCF Server that only exposes services originally provided by a oneM2M service in line with the concepts defined in the OCF Bridge Specification [10] - including the mandatory resources it shall host in line with the associated OCF Device Type according to the mapping from the exposed oneM2M service to an equivalent OCF Device Type defined in oneM2M TS-0023 [6]. Each instantiated virtual OCF Server shall be reachable via the OCF Proximal IoT Network that the OCF-IPE interworks with.

As specified in clause 8.2.2.2.1, instantiation of virtual OCF Servers representing exposed oneM2M services shall be taken into account by the OCF-IPE in order to keep the content of the "/oic/res" resource of the OCF Bridge Device instantiated by the OCF-IPE up-to-date. The OCF-IPE shall be responsible to carry out corresponding additions to the set of links in its OCF Bridge Device resource "/oic/res" so that other OCF entities can discover up-to-date information on the overall set of resources that are discoverable for all currently active virtual OCF Servers representing oneM2M services or be notified about any changes of that set via observations.

As defined in clause 7.2, a newly instantiated virtual OCF Server needs to support the mandatory core resources with the pre-defined URIs "/oic/res", "/oic/p" and "/oic/d", see also the OCF Core Specification [7]. Depending on the specific OCF Device Type that an instantiated virtual OCF Server implements to represent the corresponding oneM2M service, additional mandatory resources as defined in the OCF Device Specification [8] shall be supported by the respective virtual OCF Server.

Mandatory resource "/oic/res" of virtual OCF Server(s) instantiated by the OCF-IPE

For each virtual OCF Server that the OCF-IPE instantiates, the mandatory OCF core resource "/oic/res" shall be supported. This resource contains a collection of links to all resources hosted by the respective virtual OCF Server in order to support OCF Clients in discovery of services exposed by the respective virtual OCF Server. Note that multicast request to retrieve the "/oic/res" resource do not need to be responded to by any of the virtual OCF Servers instantiated by the OCF-IPE as the OCF Bridge Device instantiated by the OCF-IPE will respond properly with a list of all discoverable OCF resources across all virtual OCF Servers it has instantiated.

Mandatory resource "/oic/d" of virtual OCF Server(s) instantiated by the OCF-IPE

For each virtual OCF Server that the OCF-IPE instantiates, the OCF-IPE shall generate a unique value for the OCF device ID to be used by the corresponding virtual OCF Server as a value for the "di" property of the respective "/oic/d" resource in line with the OCF Core Specification [7].

This the value of this "di" property will also be used as a context for the links to all discoverable resources hosted by the respective virtual OCF Server as they appear in the "/oic/res" resource of the OCF Bridge Device instantiated by the OCF-IPE. It is the responsibility to update the "/oic/res" resource of the OCF Bridge Device upon instantiation of any new virtual OCF Server.

For each virtual OCF Server that the OCF-IPE instantiates, the OCF-IPE shall generate a value for the "dmno" (device model number) as detailed in table 7.2-2. This format for the "dmno" property allows to avoid loops in exposing services from a oneM2M SP domain to an OCF Proximal IoT Network and back to the same oneM2M SP domain.

Mandatory resource "/oic/p" of virtual OCF Server(s) instantiated by the OCF-IPE

For each virtual OCF Server that the OCF-IPE instantiates, the OCF-IPE shall be responsible to support the mandatory OCF core resource "/oic/p" with properties as defined in table 7.2-1.

Update of OCF-IPE <*AE*> resource after virtual OCF Server instantiation completed

After successful instantiation of a virtual OCF Server exposing oneM2M services to the OCF side - including any required mandatory OCF resources - and after all other pre-requisites for exposing a given OCF Server are established - see step 002 in clause 8.2.2.1 - the <*AE*> resource representing the OCF-IPE needs to be updated to include the value of the resource ID of the respective top-level oneM2M resource used to expose the corresponding oneM2M service in the *labels* attribute under the "Exposed-Resource-IDs" key, see clause 7.1.2.2 of the present document.

Handling of access control for resources hosted on virtual OCF Server(s) instantiated by the OCF-IPE

At time of instantiation of virtual OCF Servers to represent exposed oneM2M services, it is advised to set access control governing access to the resources hosted on a newly instantiated OCF Server such that other OCF entities are not able yet to consume the oneM2M services which shall be exposed by these resources. The reason for that is: The OCF-IPE has to establish a few more pre-requisites before starting the actual exposure - see step 002 in clause 8.2.2.1. Only after all these pre-requisites are established and after the parent <*AE*> resource has been updated with the proper information in the *labels* attribute under the "Exposed-Resource-IDs" key, the OCF-IPE should set the access control governing access to the resources hosted on a newly instantiated OCF Server such that intended OCF entities could eventually consume the exposed services. This may require execution of additional onboarding procedures on the OCF side.

8.2.2.2.3 Destruction of virtual OCF Servers

Reasons for destruction

An OCF-IPE shall destruct virtual OCF Servers it is using to represent oneM2M services when the OCF-IPE detects that one or more oneM2M services among the set of exposed oneM2M services shall not be exposed to the OCF side any longer, e.g. due to deletion of the respective oneM2M resources representing these services, see step 005c in clause 8.2.2.1.

Also when the OCF-IPE intends to de-register - i.e. when it is planning to delete its own <*AE*> resource - any remaining virtual OCF Servers it has instantiated earlier need to be destructed first.

In both cases, the actions listed in the remainder of this clause have to be completed for a proper end of exposure of oneM2M services, see the following paragraphs. Note that the sequence of actions does not necessarily need to be in line with the sequence of descriptions below.

Update of OCF-IPE <*AE*> resource after virtual OCF Server destruction completed

This only applies when the OCF-IPE is intending to stop exposure of oneM2M services for a sub-set of the exposed oneM2M services it is handling so far. In case the OCF-IPE intends to de-register, this update action is not needed.

Before actual termination of virtual OCF Servers used to expose oneM2M services to the OCF side, the OCF-IPE shall remove any oneM2M resource ID values of the associated oneM2M resources which represent the exposed oneM2M services that are meant to be no longer exposed from the *labels* attribute under the "Exposed-Resource-IDs" key, see clause 7.1.2.2 of the present document.

Updating "/oic/res" resource of the OCF-IPE's OCF Bridge Device

As specified in clause 8.2.2.2.1, destruction of virtual OCF Servers representing exposed oneM2M services shall be taken into account by the OCF-IPE in order to keep the content of the "/oic/res" resource of the OCF Bridge Device instantiated by the OCF-IPE up-to-date. The OCF-IPE shall be responsible to remove the respective item from the set of links in its OCF Bridge Device resource "/oic/res" so that other OCF entities can discover up-to-date information on the overall set of resources that are discoverable for all currently active virtual OCF Servers representing oneM2M services or be notified about any changes of that set via observations.

Stop listening to any requests directed to the virtual OCF Server(s) to be destructed

The OCF-IPE shall end any procedures to listen for incoming requests directed to the virtual OCF Server(s) to be destructed.

Stop monitoring oneM2M resources representing services not to be exposed any longer

The OCF-IPE shall end monitoring of oneM2M resources representing services that are not to be exposed any longer to the OCF side, i.e. any corresponding subscriptions or polling loops for the respective oneM2M resources shall be terminated.

Termination of virtual OCF Server(s)

When all listening procedures for detecting incoming requests on the OCF side have been stopped and also no more monitoring activities - i.e. subscriptions or polling loops - exist on the oneM2M side, the respective virtual OCF Servers shall be terminated.

8.2.3 Mirroring state of oneM2M Resources representing exposed oneM2M services in OCF resources hosted on virtual OCF Servers

8.2.3.1 Establishment of monitoring

Once the virtual OCF Server to represent an exposed oneM2M service on the OCF side has been instantiated, it is important to reflect accurate state information in the resources hosted by the virtual OCF Server so that they are kept consistent with the actual state of the exposed oneM2M resources that they represent.

In order to do so, the OCF-IPE shall establish monitoring of the state of all exposed oneM2M resources representing an exposed oneM2M service. Such monitoring shall be accomplished by either using the subscription mechanism defined in oneM2M specifications, see oneM2M TS-0001 [2], or by periodically polling the state of the relevant oneM2M resources with sufficiently small polling period length. It is an implementation choice to select an appropriate monitoring mechanism.

Establishment of monitoring for all relevant oneM2M resources requires the OCF-IPE to issue a number of requests on the oneM2M side to either establish appropriate subscriptions to the relevant oneM2M resources or to retrieve the values of all exposed oneM2M resources. As a result of establishing monitoring of relevant oneM2M resources for the exposed oneM2M services, changes of state in the monitored resource will be visible to the OCF-IPE and may result in a large number of state change detections over time. The OCF-IPE shall be able to process these state changes according to clause 8.1.3.2. Note that, depending on the choice of the monitoring mechanism, there is a risk to detect state changes with a certain delay or not at all if state is toggling very quickly. It is an implementation choice to select an appropriate monitoring mechanism with reasonable parameters.

8.2.3.2 Mirroring of state information

Upon detection of state changes of oneM2M resources via the previously established monitoring mechanism, the OCF-IPE shall identify the virtual OCF Server that corresponds to the oneM2M resource for which a state change was detected and translate the received state change information of the oneM2M resource into a corresponding update of the state of an OCF resource representing the modified oneM2M resource. This procedure corresponds to step 002d in clause 8.2.2.1.

However, when detecting state changes of monitored oneM2M resources, e.g. by receiving notifications triggered by subscriptions established according to clause 8.2.3.1, not all detected state changes of oneM2M resources will need to be translated into corresponding OCF requests. For instance if a notification was sent because of an update request issued by the OCF-IPE itself due to an incoming request to a virtual OCF Server, it shall not translate that back into another OCF request to avoid loopbacks or redundant operations.

The OCF-IPE shall keep a record of the mapping between oneM2M resources it monitors and the corresponding OCF resources hosted on virtual OCF Servers. Note that changes of OCF resources triggered by this mirroring activity may result in the need to send out notifications on the OCF side if the changed OCF resources were monitored by other OCF entities using the "observe" mechanism defined in OCF Core Specifications [7].

8.2.3.3 Stop monitoring

When a oneM2M service shall no longer be exposed to the OCF side - this happens when steps 005c and 006 in clause 8.2.2.1 occur - then the previously established monitoring of the oneM2M resources representing the exposed services which are not to be exposed any longer according to clause 8.2.3.1 needs to be terminated to avoid any further state changes of monitored oneM2M resources being processed by the OCF-IPE.

8.2.4 Detection of requests to consume exposed oneM2M services and execution thereof

8.2.4.1 Incoming requests to virtual OCF Servers

In order to find out when a properly authorized OCF Client would like to consume an exposed oneM2M service, the virtual OCF Server responsible for exposing a given oneM2M service needs to listen to incoming requests via any of the supported transport protocols within the OCF Proximal IoT Network as outlined in OCF Core Specifications [7].Upon detection of a request by an authorized OCF Client trying to modifying the state of a resource on a given virtual OCF Server representing and exposing a oneM2M service, that state change attempt needs to be translated into a corresponding state change request on the oneM2M side. This mechanism is part of step 005a in clause 8.2.2.1.

Note that not all oneM2M services require a state change of oneM2M resources by the entity that is intending to consume that service. For instance a oneM2M service that provides the status of a window contact sensor may be implemented using a read-only resource that reflects the current state of the contact sensor. In such a configuration, exposure of the service to OCF only requires state mirroring from the oneM2M side to the OCF side as already described in clause 8.2.3. Incoming requests from OCF Clients to change the state of the corresponding OCF resource on the respective virtual OCF Server would not make sense in that case and would not be allowed, e.g. by only allowing read access.

In general, however, oneM2M services - for instance a light - may require monitoring of requests demanding state changes on the OCF side in order to detect when a subsequent state change needs to be requested on the oneM2M side - for instance when a an oneM2M light needs to be switched on or off by an OCF Client. Therefore, the OCF-IPE needs to decide which resources hosted by virtual OCF Servers are subject to incoming request that may demand a state change. This decision depends on the specific device model as defined in oneM2M TS-0023 [6] that was used to create the respective oneM2M resources and which was the mapped into the corresponding OCF Device Type implemented by the corresponding virtual OCF Servers. Only for those resources that are meant to be modified (updated or deleted) by the service consuming entity, the virtual OCF Server needs to handle incoming requests for state changes.

8.2.4.2 Invocation of oneM2M services

The procedure outlined in this clause correspond to step 005a in clause 8.2.2.1.

When the OCF-IPE has successfully established all pre-requisites for exposing a set of oneM2M services to an OCF Proximal IoT Network - see step 002 in clause 8.2.2.1 - and when it has initiated the exposure - see steps 003 and 004 in clause 8.2.2.1 - it needs to detect relevant state change request of resources hosted on virtual OCF Servers that need to be translated into oneM2M requests for corresponding state changes in the oneM2M resources that represent the exposed services. As specified in clause 8.2.4.1, the OCF-IPE is supposed to receive such information by listening to incoming requests at the virtual OCF Servers instantiated by the OCF-IPE.

However, when receiving incoming requests at a virtual OCF Server according to clause 8.2.4.1, not all requests will need to be translated into corresponding oneM2M requests. For instance if a request was sent to initiate an update which would result in the same state as before - e.g. when switching power state from on to on - the OCF-IPE shall not translate that into a sub-sequent oneM2M request to avoid redundant operations.

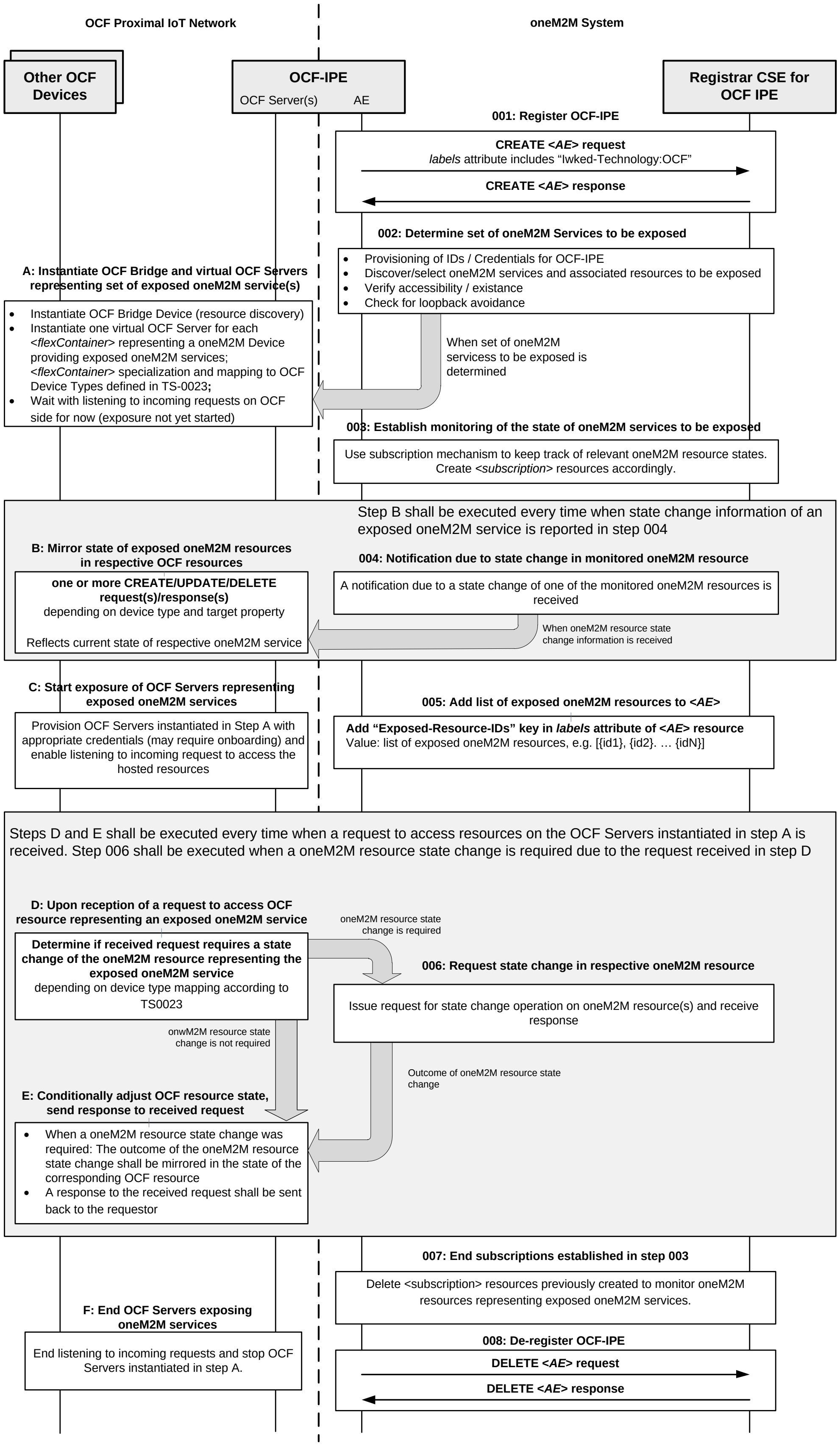
Therefore, requests for state changes received by virtual OCF Servers instantiated by the OCF-IPE need to be evaluated first and the OCF-IPE needs to decide whether a state change request is needed on the oneM2M side as well. If so, the OCF-IPE shall issue the corresponding state change request on the oneM2M side. Which exact request that is and what changed state values to request depends on the specific device model as defined in oneM2M TS-0023 [6] that was used to create the respective oneM2M resources and the corresponding OCF Device Type implemented by the respective virtual OCF Server.

Upon completion of the oneM2M operation - in case the OCF-IPE decided to initiate one - the virtual OCF Server exposing the oneM2M service needs to update its internal resource state in line with the outcome of the requested oneM2M operation. For instance if an OCF Client was requesting to change the power state of a oneM2M light exposed by a virtual OCF Server from on to off, the OCF-IPE would trigger a corresponding request to change the state of the mapped oneM2M resource accordingly. Only after receiving the result of the requested operation on the oneM2M side, the OCF-IPE shall reflect the new state in the internal resource state of the virtual OCF Server hosting the resource(s) representing the oneM2M light. Finally, the OCF-IPE shall send a response via the respective virtual OCF Server to the issuer of the original request accurately reflecting the success or failure to process the requested state change.

8.2.5 Overall flows for procedures supporting exposure of oneM2M services to an OCF Proximal IoT Network

In this clause the overall flow of events and processing steps is summarized as depicted in figure 8.2.5-1 for the case that a static set of oneM2M services - only determined once during the life cycle of the OCF-IPE - is meant to be exposed to the OCF Proximal IoT Network. For enumerating steps carried out on the OCF side the letters A-F are used, for the steps on the oneM2M side numbers 001 - 007 are used. All the details of the flow are defined in the previous clauses 8.2.1 through 8.2.4. In essence figure 8.2.5-1 is a more specific variant of figure 8.2.2.1-1 outlining in more details which steps happen on the OCF side versus the oneM2M side.

Note that the processing steps within the boxes shaded in grey may occur multiple times and are triggered asynchronously by requests received at the virtual OCF Servers instantiated by the OCF-IPE or by oneM2M notifications due to changes of monitored oneM2M resources, respectively.



001: Register OCF-IPE

CREATE <*AE*> request
labels attribute includes "Iwked-Technology:OCF"

CREATE <*AE*> response

002: Determine set of oneM2M Services to be exposed

- Provisioning of IDs / Credentials for OCF-IPE
- Discover/select oneM2M services and associated resources to be exposed
- Verify accessibility / existance
- Check for loopback avoidance

When set of oneM2M servicess to be exposed is determined

A: Instantiate OCF Bridge and virtual OCF Servers representing set of exposed oneM2M service(s)

- Instantiate OCF Bridge Device (resource discovery)
- Instantiate one virtual OCF Server for each <*flexContainer*> representing a oneM2M Device providing exposed oneM2M services; <*flexContainer*> specialization and mapping to OCF Device Types defined in TS-0023**;**
- Wait with listening to incoming requests on OCF side for now (exposure not yet started)

003: Establish monitoring of the state of oneM2M services to be exposed

Use subscription mechanism to keep track of relevant oneM2M resource states. Create <*subscription*> resources accordingly.

Step B shall be executed every time when state change information of an exposed oneM2M service is reported in step 004

B: Mirror state of exposed oneM2M resources in respective OCF resources

one or more CREATE/UPDATE/DELETE request(s)/response(s)
depending on device type and target property

Reflects current state of respective oneM2M service

004: Notification due to state change in monitored oneM2M resource

A notification due to a state change of one of the monitored oneM2M resources is received

When oneM2M resource state change information is received

C: Start exposure of OCF Servers representing exposed oneM2M services

Provision OCF Servers instantiated in Step A with appropriate credentials (may require onboarding) and enable listening to incoming request to access the hosted resources

005: Add list of exposed oneM2M resources to <*AE*>

Add "Exposed-Resource-IDs" key in *labels* attribute of <*AE*> resource
Value: list of exposed oneM2M resources, e.g. [{id1}, {id2}. … {idN}]

Steps D and E shall be executed every time when a request to access resources on the OCF Servers instantiated in step A is received. Step 006 shall be executed when a oneM2M resource state change is required due to the request received in step D

D: Upon reception of a request to access OCF resource representing an exposed oneM2M service

Determine if received request requires a state change of the oneM2M resource representing the exposed oneM2M service
depending on device type mapping according to TS0023

oneM2M resource state change is required

006: Request state change in respective oneM2M resource

Issue request for state change operation on oneM2M resource(s) and receive response

onwM2M resource state change is not required

Outcome of oneM2M resource state change

E: Conditionally adjust OCF resource state, send response to received request

- When a oneM2M resource state change was required: The outcome of the oneM2M resource state change shall be mirrored in the state of the corresponding OCF resource
- A response to the received request shall be sent back to the requestor

007: End subscriptions established in step 003

Delete <subscription> resources previously created to monitor oneM2M resources representing exposed oneM2M services.

F: End OCF Servers exposing oneM2M services

End listening to incoming requests and stop OCF Servers instantiated in step A.

008: De-register OCF-IPE

DELETE <*AE*> request

DELETE <*AE*> response

Figure 8.1.5-1: Overall flow of processing steps when exposing a static set of oneM2M services to OCF Clients

Annex A (informative): Bibliography

- OIC-Core-Specification-V1.0.0: "OIC Core Specification".

History

Publication history		
V3.2.2	April 2019	Release 3 - Publication