ETSI TS 118 124 V2.0.2 (2020-03)

TECHNICAL SPECIFICATION

**oneM2M;
OIC Interworking
(oneM2M TS-0024 version 2.0.2 Release 2A)**

Reference

RTS/oneM2M-000024v2A

Keywords

interworking, IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document specifies the interworking technologies for oneM2M and OIC interworking using the architecture identified in annex F of ETSI TS 118 101 [2] for the following scenario:

- Interworking using oneM2M Resource Types for transparent transport of encoded OIC Resources and commands in oneM2M Resource Types between OIC Devices and M2M Applications.

NOTE: The present document limits Content Sharing Resources to <container> and <contentInstance> resources.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[1] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[2] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[3] OIC-Core-Specification-V1.0.0: "OIC Core Specification".

[4] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

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 referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 118 111 [1] and ETSI TS 118 101 [2] apply.

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI TS 118 111 [1] and ETSI TS 118 101 [2].

3.2   Symbols

Void.

3.3   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   Architecture Model

5.1   Introduction

The architecture model followed in the present document is based on the architecture model in Annex F of ETSI TS 118 101 [2]. It describes interworking using specialized Interworking Proxy application Entity (IPE). The present document describes the OIC IPE that supports the following scenarios.
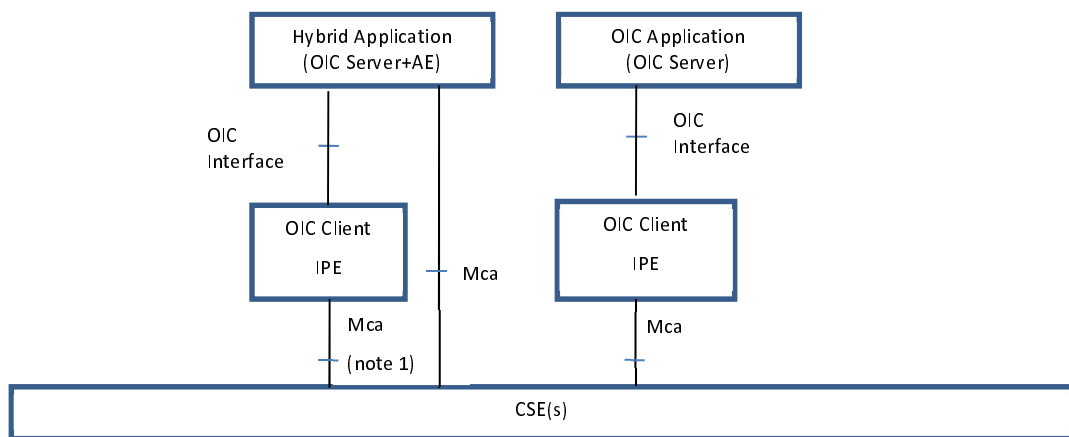
Figure 5.1-1: OIC Interworking Scenarios

In the scenarios depicted in Figure 5.1-1, the Hybrid and OIC Applications represent applications that implement the OIC Server role defined in the OIC Protocol [3].

5.2   Interworking Reference Model

The OIC Interworking reference model utilizes the Functional Architecture's reference model in ETSI TS 118 101 [2]; augmenting the ETSI TS 118 101 [2] reference model with capabilities provided by the OIC IPE.
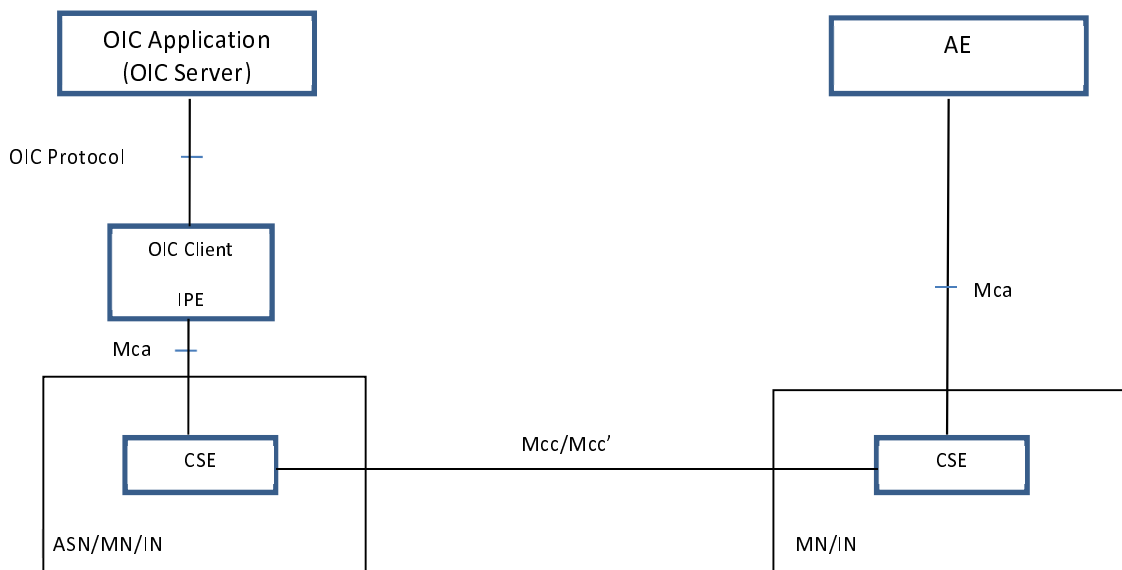
NOTE: The AE in the reference model could be registered with the same CSE as the OIC IPE.

Figure 5.2-1: OIC Reference Model

5.3   Function of Interworking Proxy Entity

The OIC IPE participation in the OIC Protocol as described in clause 5 does so in the role of an OIC Client to which OIC Applications (OIC Servers) interact. For each OIC Server (Endpoint) that is maintained by the OIC Client in the OIC IPE, the OIC IPE shall instantiate and maintains an instance of a Resource of type <AE>.
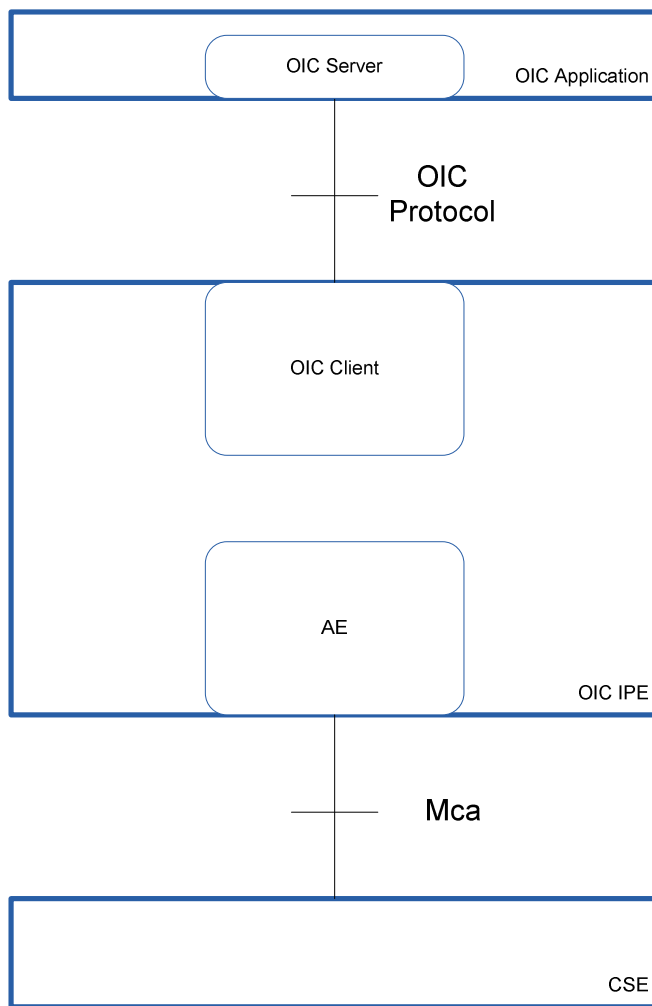
Figure 5.3-1: OIC IPE Architecture

Mapping OIC Servers to AEs provides the following:

1) Application Registry: OIC Servers can now be registered as oneM2M Applications.

2) Service Subscriptions: OIC Servers can now be attached to M2M Service Subscriptions just like any other oneM2M Application.

5.4 Types of Interworking

OIC IPEs provide the following types of interworking in the present document:

1) Interworking using the <container> resource for transparent transport of encoded OIC Resources that are available to AEs as depicted in Figure 5.4-1.
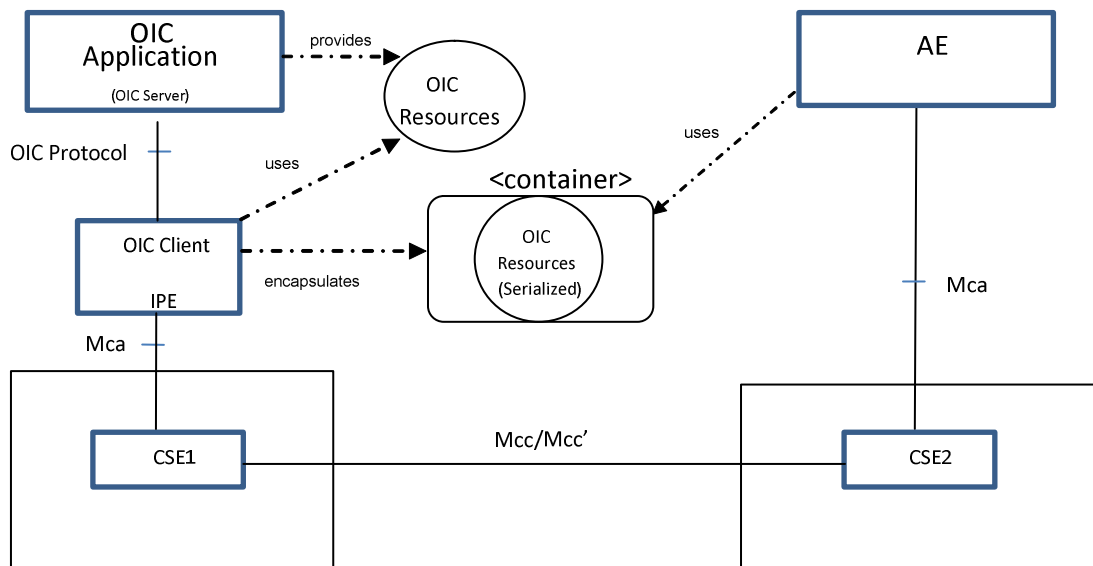
Figure 5.4-1: OIC Transparent Interworking Function

In Figure 5.4-1, the OIC Resources are provided by the OIC Application to the OIC IPE using the OIC Protocol [3]. The OIC IPE then encapsulates the OIC Resources in Content Sharing Resources and then hosts the Content Sharing Resources in a CSE using the Mca reference points for use by AEs. The AE accesses the Content Sharing Resource from the CSE that hosts the resource using the Mca reference point. Once the AE receives the Content Sharing Resource, the AE extracts the OIC Resource from the Content Sharing Resource for the AE's purpose.

6   Architectural Aspects

6.1   Introduction

The OIC IPE participation in the OIC Protocol as described in clause 5 does so in the role of an OIC Client to which OIC Applications (OIC Servers) interact. As an OIC Client, the IPE provides the following Architecture Aspects based on the OIC Protocol Aspects:

- OIC Device Lifecycle.

- OIC Resource Discovery.

- OIC Interworking Procedure.

- OIC Subscription Notification.

- OIC Device Management.

- OIC Provisioning and Security.

6.2   OIC Device Lifecycle

6.2.1   Introduction

As the OIC IPE discovers OIC Devices when the OIC IPE interacts with the OIC Server over the OIC protocol, the OIC IPE shall maintain the associated resources in the CSE that represents the OIC Device.

6.2.2   OIC Device Representation

6.2.2.1   Introduction

OIC Device provides the management and control functions for any M2M application. As such, the CSE that hosts the M2M Applications shall represent the OIC Device as a <AE> resource (OIC Device <AE> resource). The OIC physical Device that hosts the logical OIC Device shall be represented as a <node> resource.

The properties carried by OIC Device (i.e. device type) shall be translated into the labels attribute of the <AE> Resource as separate entries with the following format:

- OIC-DT: Device Type (e.g. oic.d.light).

6.2.2.2   OIC Device Identification

OIC Devices are identified by their "di" property as described in OIC Core Specification [3]. The "di" property is used as the AE-ID of the associated <AE> resource that represents the OIC Device.

In most deployment scenarios, OIC physical Devices host one (1) OIC Device. In this scenario the OIC physical Device's <node> resource's M2M-Node-ID should be the same as the "di" property. Also the deviceIdentifier attribute of <serviceSubscribedNode> resource should be same as the "di" property. When an OIC physical Device hosts more than one (> 1) OIC Device, the determination of the <node> resource's M2M-Node-ID is implementation specific. In all deployment scenarios, the <AE> resource is linked with the <node> resource as described in ETSI TS 118 101 [2].

As the OIC Device is represented as an <AE> resource and a OIC Resource is represented as a Content Sharing Resource in the M2M Service Layer, a reference shall be made between the <AE> resource that represents the OIC Device and the Content Sharing Resources which represents the list of OIC Resources available in that OIC Server.

In order to identify interworked entities hosted in a CSE for the OIC technology described in the present document, the <AE> resource that represents the OIC Device and the Content Sharing Resources which represent the OIC Resources, shall have a Iwked_Technology *labels* attribute set to OIC.

In addition the <AE> resource uses the Hierarchical and Non-Hierarchical mechanisms for Resource Addressing as defined in clause 9.3.1 of ETSI TS 118 101 [2] where the *resourceName* attribute of the <AE> shall be same as "di" property.

6.2.2.3   OIC Device Discovery and Forget

The OIC Client can periodically get the OIC Server details by requesting them using procedures defined in OIC specifications [3]. The details that the OIC Client gets become stale or invalid once the time to live expires.

The OIC operations and events map to the following operations on the <AE> and <node> resources.

Table 6.2.2.3-1: OIC Device Discovery Translation - Operations

OIC Operation (Discovery)	oneM2M Resource and Operation
GET	create <AE>, create <Node>

Table 6.2.2.3-2: OIC Device Discovery Translation - OIC Client Events

OIC Client Events	oneM2M Resource and Operation
<ttl> expires	delete <AE>, delete <Node>, delete <container> resource associated with the <AE> resource

Table 6.2.2.3-3: OIC Device Discovery Attribute Translation

OIC Properties (Discovery)	oneM2M Resource Attribute
di	<AE>: AE-ID, resourceName <Node>: M2M-Node-ID when the Device only supports one Endpoint (OIC Device); resourceName
ttl	<AE>, <Node>: expirationTime
OIC version	<AE>, <Node>: labels. Value is "Iwked-Entity-Version:" appended with the value of the OIC Version

Table 6.2.2.3-4: OIC Device Discovery Response Code Translation

OIC Errors (Discovery)	oneM2M Resource Operation Response
GET 2.01 Success: Created 4.00 Bad Request 4.03 Forbidden	create <AE>, create <Node> 2001 Created All other codes 4105 Conflict

6.2.2.4 Configuration of CMDH Policies

In the present document, the CMDH Policies associated with the <Node> resource for the AE is implementation specific.

6.3 OIC Resource Discovery

6.3.1 Introduction

OIC Server provides the information of supported OIC Resources to an OIC Client. The OIC IPE uses its OIC Client function to synchronize which OIC Resources are supported by the OIC Device and what is stored in the hosting CSE for the M2M Application representing the OIC Device. This clause specifies how discovered OIC Resources are translated to discoverable Content Sharing Resources along with the associated linkages to other resources.

6.3.2 OIC Resource Representation

6.3.2.1 Introduction

OIC Server provides the list of supported OIC Resources, where information of each resource is specified in an oic-link format as specified in OIC Core specification [3]. The oic-link format contains information like the resource type, uri and interface.

Optionally other information can be carried by that list as the capability for all the OIC Resources in the OIC Server:

- a specific Content-Format (e.g. OIC JSON/ OIC CBOR Content-Format);

- time to live.

For discovery of OIC Resources by M2M Applications, the properties carried by OIC Resources list (i.e. technology, resource type, uri, interface, optional content format, time to live) shall be translated into the labels attribute of the Content Sharing Resource as separate entries with the following format:

- Iwked-Technology:OIC.

- Iwked-Entity-Type: Resource Type.

- Iwked-Entity-ID: Resource URI (href).

- OIC-IF: Resource Interfaces.

- Iwked-Content-Type: Supported Content Format (OIC default supported ContentFormat is CBOR. Others could be JSON, XML).

- OIC-TTL: time to live.

For each OIC Resource discovered there will be a separate Content Sharing resource represented.

6.3.2.2 OIC Resource Identification

OIC Resources are identified by their URI within the context of the OIC Device as described in OIC Core specification [3].

As the OIC Device is represented as an <AE> resource and a OIC Resource is represented as a Content Sharing Resource in the M2M Service Layer, a reference shall be made between the <AE> resource that represents the OIC Device and the Content Sharing Resources which represent the list of OIC Resources available in the OIC Server.

In addition, Content Sharing Resources that represents the OIC Resources use the Hierarchical and Non-Hierarchical mechanisms for Resource Addressing as defined in clause 9.3.1 of ETSI TS 118 101 [2] where the *resourceName* attribute of the Content Sharing Resource shall be the value of the OICURI.

6.3.2.3 OIC Resource Discovery and Forget

The OIC Client can periodically get the OIC Server details by requesting them using procedures defined in OIC specifications [3]. The details that the OIC Client gets become stale or invalid once the time to live expires.

The OIC operations and events map to the following operations on the Content Sharing resource.

Table 6.3.2.3-1: OIC Resource Discovery Translation - Operations

OIC Operation (Discovery)	oneM2M Resource and Operation
GET	create <container> or

Table 6.3.2.3-2: OIC Resource Discovery Translation - OIC Client Events

OIC Client Events	oneM2M Resource and Operation
<ttl> expires	delete <container>

Table 6.3.2.3-3: OIC Resource Discovery Attribute Translation

OIC Attributes (Discovery)	oneM2M Resource Attribute
di	Not Applicable
Resource URI	<container> resourceName
ttl	<container> expirationTime

Table 6.3.2.3-4: OIC Resource Discovery Response Code Translation

OIC Errors (Discovery)	oneM2M Resource Operation Response
GET 2.01 Success: Created 4.00 Bad Request 4.03 Forbidden	create <container> 2001 Created All other codes 4105 Conflict

6.4 OIC Interworking Procedure

6.4.1 Introduction

When an oneM2M request is addressed from a CSE/AE to a hosting CSE containing the representation of an OIC Server, the oneM2M response to the Originator of the request is returned through the cooperation of the hosting CSE and the IPE.

The OIC Server provides the capabilities for the OIC Client of the IPE to access available OIC Resources from the OIC Server.

A hosting CSE maintains a representation of OIC Resources as instances of oneM2M resource types. These oneM2M resources are instantiated and discovered as described in clause 6.3 allowing oneM2M AEs and CSEs to exchange data with OIC Servers.

In reference to clause 6.3, at the end of the discovery phase all declared OIC Resources are associated to a Content Sharing Resource created with the resourceName attribute set to OICURI.

6.4.2 Interworked Resource Settings

An OIC Resource is represented in oneM2M as a Content Sharing Resource with 2 direct children resource types: a <subscription> resource and a <contentInstance> resource when used with a <container> resource.

For supporting the OIC interworking process, a few attributes for the Content Sharing Resource and the <notification> resource shall have a specified set of parameters:

a) Attributes of Content Sharing Resource

Table 6.4.2-1: <container> resource - Relevant Interworked Attributes

Attributes of *<container> resource*	Value
accessControlPolicyIDs	ACP set (see clause 6.7)
maxNrOfInstances	1

b) Child resource types of *<container>* resource

Table 6.4.2-2: <container> resource - Relevant Child resource types

Child resources of *<container> resource*
<contentInstance> resource
<subscription> resource

c) Attributes of *<subscription>* resource

Table 6.4.2-3: <subscription> resource - Relevant Interworked Attributes

Attributes of *<subscription>*	Description / Value
notificationURI	IPE URI
eventType	Event Type values used are "B", "C" or "E" as defined in [2].

6.4.3 Further Considerations for Interworking

Cooperation between IPE and the oneM2M hosting CSE requires efficient mechanisms to maintain the latest state of the targeted OIC Resources. These mechanisms include data synchronization between the IPE and hosting CSE.

Data synchronization relies on the oneM2M Subscription/Notification and OIC Observation/Notification mechanisms. For automated data synchronization between the IPE and hosting CSE to be achieved, the solution shall be granular enough to allow data synchronization for each OIC Resource.

Access Control mechanisms relies on an interworking between oneM2M and OIC Access Control Policies.

OIC and oneM2M mechanisms used to achieve Data Synchronization and Access Control is specified in more details in clauses 6.5 and 6.7.

These following clauses specify the sequences of operations involved for each type of supported oneM2M requests following the general procedures specified in clause 10 of ETSI TS 118 101 [2] (CREATE, RETRIEVE, UPDATE, DELETE) as used within the context of the interworking for the present document.

6.4.4 Retrieve Procedure

This procedure describes the retrieval of a resource using the oneM2M RETRIEVE request. The information contained within the resource is related to the OIC Resources that are interworked through the IPE. This clause shall be treated in conformance with the RETRIEVE Procedure specified in ETSI TS 118 101 [2], clause 10.1.2.

The Receiver performs local processing to verify the existence of requested Resource and checks privileges for retrieving the information related to the resource. After successful verification, the Receiver shall return the requested information according to the procedures for interworking as described in clause 7, otherwise an error response shall be returned to the Originator.
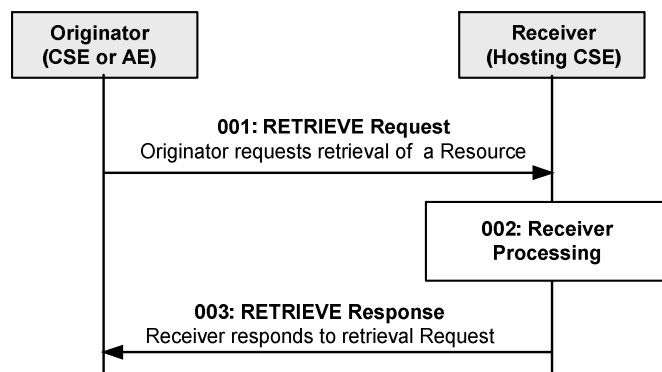

Figure 6.4.4-1: Procedure for Retrieving a Resource (ETSI TS 118 101 [2], clause 10)

Specific steps of the Receiver Processing according to the interworking process shall be as follows:

Step 001: Find and verify the targeted Content Sharing Resource: the resourceName corresponds to clause 6.3.2.

Step 002: Using the hosting CSE Access Control mechanisms, check for Access Control Policy for retrieving the <contentInstance> resource related to the <container> resource.

Step 002a: On successful validation of the Access Control Policy, check if the latest <contentInstance> resource contained within the targeted <container> resource has expired or does not exist:

> **Step 002a.1:** When the <contentInstance> resource for the <container> resource is obsolete or not existing an event for Retrieval attempt (eventType 'E') is triggered to the Entity that subscribed to the event (i.e. IPE); as a Blocking Procedure, the hosting CSE shall monitor the arrival of the new data or decide to report a timeout error in jumping to Step 003.

> **Step 002a.1.1:** On receiving the event 'Retrieval attempt of obsolete or non-existing direct child resource (eventType 'E') the IPE performs a OIC GET request on the OIC Resource of the targeted OIC Server.

> **Step 002a.1.2:** Once the targeted OIC Resource is available to IPE, the IPE creates and populates a <contentInstance> resource in the requested <container> resource.

Step 003: The hosting CSE returns the appropriate response back to the Originator (e.g. Acknowledgment, Errors, and Data).

> NOTE: As an OBSERVATION has been set up on the targeted OIC Resource, the automatic synchronization between the OIC Resource and its representation in the hosting CSE is performed. Further oneM2M accesses to the resource should be simplified in minimizing impact of Step002a (up-to-date data already present from the hosting CSE resources).

General Exceptions:

1) The targeted resource/attribute in *To* parameter does not exist. The Receiver shall respond with an error.

2) The Originator does not have privileges to retrieve information stored in the resource on the Receiver. The Receiver shall respond with an error.

Table 6.4.4-1: OIC Response Codes to oneM2M Resource Operation Response Codes

OIC Server Response Codes	oneM2M Resource Operation Response
Read 2.05 Content: 4.01 Unauthorized 4.04 Not Found 4.05 Method Not Allowed	2000 OK 4103 4004 4005

6.5 OIC Resource Subscription and Notification

6.5.1 Introduction

The oneM2M Subscription capabilities permit subscription changes to an oneM2M resource's attributes and its direct child resources. Likewise, the oneM2M Notification capabilities include a rich set of criteria for when a subscribed-to oneM2M resource is notified of a change.

oneM2M Subscription and Notification function can be mapped to OIC observe mechanism which utilizes the RETRIEVE operation to request the OIC Device for updates in case if OIC Resource state changes.

6.5.2 OIC Subscription (Observe Request) Procedure

The OIC IPE interworks the oneM2M resource's <subscription> child resource with the corresponding OIC Resources using the oneM2M <subscription> resource's attributes.

When the OIC IPE creates a oneM2M Content Sharing Resource, the OIC IPE creates a subscription on the Content Sharing Resource to be notified whenever the oneM2M resource's subscription attribute is changed by setting the <subscription> resource's attributes as follows.

Table 6.5.2-1: OIC Subscription Procedure - <subscription> resource

Attributes of *<subscription>*	Description
accessControlPolicyIDs	Link a <accessControlPolicy> resource with the privileges: accessControlOriginator originatorID set to the OIC IPE AE's AE-ID accessControlOperations: Set to RETRIEVE, CREATE, UPDATE, DELETE, DISCOVER, NOTIFY
pendingNotification	Set to "sendLatest"
latestNotify	Set to "latest"
notificationContentType	Set to "resource"
<schedule>	Set to immediate notification

Whenever another AE or CSE creates or deletes a subscription to the <container> resource, the OIC IPE shall be notified of the change and shall perform the following steps:

Step 001: Find the associated OIC Resource for notification's subscriptionReference.

Step 002: If the oneM2M notification indicates a subscription deletion:

   Step 002a: If the associated OIC Resource has an outstanding Observation request from the OIC IPE then issue the OIC Cancel Observation operation.

Step 003: If the oneM2M notification indicates a subscription creation:

   Step 003a: If the associated OIC Resource does not have an outstanding Observation request from the OIC IPE then:

      Step 003a001: Retrieve the Parent resource of the <subscription> resource from the notification's subscriptionReference.

      Step 003a003: Issue the OIC Observe request.

General Exceptions: The processing for recovery of a failed OIC Cancel Observation or Observation request is vendor specific.

Table 6.5.2-2: OIC Subscription Procedure

OIC Operation	oneM2M Resource and Operation
Observe	NOTIFY (m2m:notification subscriptionDeletion=false)
Cancel Observation	NOTIFY (m2m:notification subscriptionDeletion=true)

6.5.3 OIC Notification (Observe Response) Procedure

When the OIC IPE gets an observe response from the OIC Server of a change in a OIC Resource, the OIC IPE creates a new <contentInstance> for the associated <container> resource according to the procedures for the type of interworking (e.g. Transparent) as described in clause 7.

6.6 OIC Device Management

Interworking of OIC Device Management (which includes Device Diagnostics and Maintenance) is out of the scope of the present document.

6.7 OIC Provisioning and Security

6.7.1 Introduction

OIC and oneM2M Access Control Policies shall collaborate in order to assure for the Interworked resources to follow the oneM2M Authorization Procedure specified in clause 11.3.4 (M2M Authorization Procedure) of ETSI TS 118 101 [2] and clause 7 (Authorization) of ETSI TS 118 103 [4].

6.7.2 OIC Interworking Access Control Policy

The oneM2M Access Control Policy mechanisms specified in clause 7 of ETSI TS 118 103 [4], allow for checking and validating the parameters of a request message to access a <container> resource against the ACPs (<accessControlPolicy> resources) which have been assigned through the accessControPolicyIDs attribute of this resource.

In order to assure a proper OIC Interworking with oneM2M, the IPE shall setup the hosting CSE:

1)   in providing a mandatory set of <accessControlPolicy> (ACPs) resources.

2)   in assigning a proper ACP set to the accessControlPolicyIDs attribute of each <container> resource allocated during the CSE registration phase (clause 6.3 "OIC Resource Discovery").

Mechanisms to provision an IPE in order to perform such a setup is out of scope of the present document.

In addition, Access Control Policy mechanisms specified in clause 7 of ETSI TS 118 103 [4] shall be applicable to interworking's of the present document.

6.8 IPE Management

6.8.1 IPE Administration

The OIC IPE provides the functionality that plays the role of the OIC Client in order to communicate with OIC Servers.

In order for communication to be established information should be provisioned into the OIC Client where the following artefacts are necessary to be established for the OIC Client:

•   OIC Client Credentials.

•   OIC Access control lists.

The mechanisms used to administer and maintain the OIC Client functionality within the OIC IPE is out of scope of the present document.

6.8.2   Maintaining IPE Context

The OIC IPE maintains information related to its operational context. Specifically the following elements are maintained for the OIC IPE:

- List of currently discovered OIC Devices.

- List of OIC Resources supported.

Whenever an OIC Device <AE> resource is created, updated or deleted as described in clause 6.2, the OIC IPE shall manage the list of OIC Device <AE> resources using a oneM2M <group> resource.

The oneM2M <group> resource's lifecycle is linked to the OIC IPE <AE> resource's lifecycle.

Table 6.8.2-1: OIC IPE <AE> resource - Group Lifecycle

OIC IPE <AE> resource Operation	oneM2M Resource and Operation
create	create <group>. The group resourceName is the AE-ID of the OIC IPE <AE>.resource
update	update <group>
delete	delete <group>

The OIC Device <AE> resources lifecycle operation maps to the following operations on the oneM2M <group> resource.

Table 6.8.2-2: OIC Device <AE> resource - Group member Lifecycle

OIC Device <AE> resource Operation	oneM2M Resource and Operation
Create	update <group> (add member)
Delete	update <group> (delete member)

7   Transparent Interworking Function

7.1   Introduction

Clause 5.4 introduced the Transparent Interworking function as depicted in Figure 5.4-1. This clause specifies the mappings of the attributes of the <contentInstance> resource for a <container> resource in order to allow an AE that uses the Content Sharing Resource to understand that the Content Sharing Resource has an encapsulated OIC Resource.

7.2   Attribute Mapping for the Content Sharing Resources

When an AE accesses a <contentInstance> resource, the AE needs to know that the <contentInstance> resource encapsulates an OIC Resource as well as how the OIC Resource is encoded.

Table 7.2-1: Transparent Interworking Function Mapping

Interworking Function Mapping	oneM2M Resource Attribute
Indication that an OIC Resource is encapsulated in the <contentInstance> resource with the content type and encoding of the OIC Resource.	<contentInstance> resource: labels. Value is "OIC-Resource-Encapsulation e.g. oic.r.switch.binary"
The content type of the OIC Resource based on the Content-Type option	<contentInstance>: contentInfo. Possible contentInfo values are translated from the OIC Content-Type option.
NOTE: The OIC Core Specification [3] defines the value to be used for the [encoding] if the Content-Type option is not present.	

History

Document history		
V2.0.0	September 2016	Publication
V2.0.2	March 2020	Publication