



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4500.32

(06/2018)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,
NEXT-GENERATION NETWORKS, INTERNET OF
THINGS AND SMART CITIES

Internet of things and smart cities and communities –
Frameworks, architectures and protocols

oneM2M- MAF and MEF Interface Specification

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T Y.4500.32

oneM2M- MAF and MEF Interface Specification

Summary

This Recommendation specifies communication between the M2M Authentication Function (MAF) and MAF clients on the reference point Mmaf and between the M2M Enrolment Function (MEF) and MEF clients on the reference point Mmef.

Keywords

oneM2M, Security, Provisioning, Authentication, Enrolment

Recommendation ITU-T Y.4500.32

oneM2M- MAF and MEF Interface Specification

1 Scope

This Recommendation specifies communication between the M2M Authentication Function (MAF) and MAF clients on the reference point Mmaf and between the M2M Enrolment Function (MEF) and MEF clients on the reference point Mmef.

The Recommendation contains oneM2M Release 2 specification - oneM2M MAF and MEF Interface Specification V2.0.0 and is equivalent to standards of oneM2M partners including ARIB, ATIS, CCSA, ETSI [ETSI TS 118 132 V2.0.0], TIA, TSDSI, TTA and TTC.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

[ITU-T Y.4500.11]	Recommendation ITU-T Y.oneM2M.CT, <i>Common Terminology</i>
[ITU-T Y.4500.1]	Recommendation ITU-T Y.oneM2M.ARC, <i>Functional Architecture</i>
[ITU-T Y.4500.4]	Recommendation ITU-T Y.oneM2M.SLCP, <i>Service Layer Core Protocol</i>
[ITU-T Y.4500.8]	Recommendation ITU-T Y.oneM2M.PB.CoAP, <i>CoAP Protocol Binding</i>
[ITU-T Y.4500.9]	Recommendation ITU-T Y.oneM2M.PB.HTTP, <i>HTTP Protocol Binding</i>
[ITU-T Y.4500.10]	Recommendation ITU-T Y.oneM2M.PB.MQTT, <i>MQTT Protocol Binding</i>
[ITU-T Y.4500.20]	Recommendation ITU-T Y.oneM2M.PB.WebSocket, <i>WebSocket Protocol Binding</i>
[ITU-T Y.4500.22]	Recommendation ITU-T Y.oneM2M.FDC, <i>Field Device Configuration</i>
[ETSI TS 118.103]	ETSI TS 118 103: "oneM2M; Security solutions".

3 Definitions

For the purposes of the present document, the terms and definitions given in oneM2M TS-0011 [ITU-T Y.4500.11], oneM2M TS-0003 [ETSI TS 118.103] and the following apply.

3.1 Terms defined elsewhere

3.1.1 Application Entity(AE): [ITU-T Y.4500.11] represents an instantiation of Application logic for end-to-end M2M solutions

3.1.2 Common Services Entity (CSE): [ITU-T Y.4500.11] represents an instantiation of a set of Common Service Functions of the M2M environments. Such service functions are exposed to other entities through reference points

3.2 Terms defined in this Recommendation

3.2.1 MAF Client: functionality for performing MAF procedures on behalf of an associated CSE or AE, or on behalf of CSE or AE(s) present on an associated Node.

3.2.2 MAF interface: Communication interface between a MAF and a MAF Client identified by reference point Mmaf.

3.2.3 MEF Client: functionality for performing MEF procedures on behalf of an associated CSE or AE, or on behalf of CSE or AE(s) present on an associated Node, or an associated MAF.

3.2.4 MEF interface: Communication interface between a MEF and a MEF Client identified by reference point Mmef.

4 Abbreviations and acronyms

For the purposes of the present document, the abbreviations given in oneM2M TS-0011 [ITU-T Y.4500.11], oneM2M TS-0003 [ETSI TS 118.103] and the following apply:

AE	Application Entity
CSE	Common Services Entity
MAF	M2M Authentication Function
MEF	M2M Enrolment Function
MTE	M2M Trust Enabler

5 Conventions

The key words “Shall”, ”Shall not”, “May”, ”Need not”, “Should”, ”Should not” in the present document are to be interpreted as described :

Shall/Shall not:

Requirements:

- 1.) effect on Standard: Standard needs to describe the required feature (i.e. specify a technical solution for the Requirement);
- 2.) effect on products: every implementation (M2M Solution that complies to this Standard) must support it
- 3.) effect on deployments: every deployment (M2M Service based on this Standard) must use the Standardized feature where applicable – otherwise e.g. interoperability problems with other services could arise.

Should/Should not

Recommendation

- 1.) effect on Standard: Standard needs to describe a solution that allows the presence and the absence of the feature.
- 2.) effect on products: an implementation may or may not support it, however support is recommended
- 3.) effect on deployments: a deployment may or may not use it, however usage is recommended .

May/Need not:

Permission/Option

- 1.) effect on Standard: Standard needs to describe a solution that allows the presence and the absence of the required feature;
- 2.) effect on products: an implementation may or may not support it
- 3.) effect on deployments: A deployment may or may not use it

6 General Description

6.1 MAF Interface

6.1.1 Introduction

The MAF Interface is a simple variant of the Mcc/Mca reference points specifying the interaction of MAF Clients with a M2M Authentication Function (MAF), acting on behalf of an *administrating stakeholder* such as an M2M SP or third party M2M Trust Enabler (MTE). The present document does not specify the operation and management of the MAF required to support these procedures.

A MAF Client interacts with the MAF on behalf of a Node (ADN, ASN, IN or MN), or a CSE or an AE.

Figure 6.1.1-1 defines the reference point Mmaf between MAF clients and a MAF.

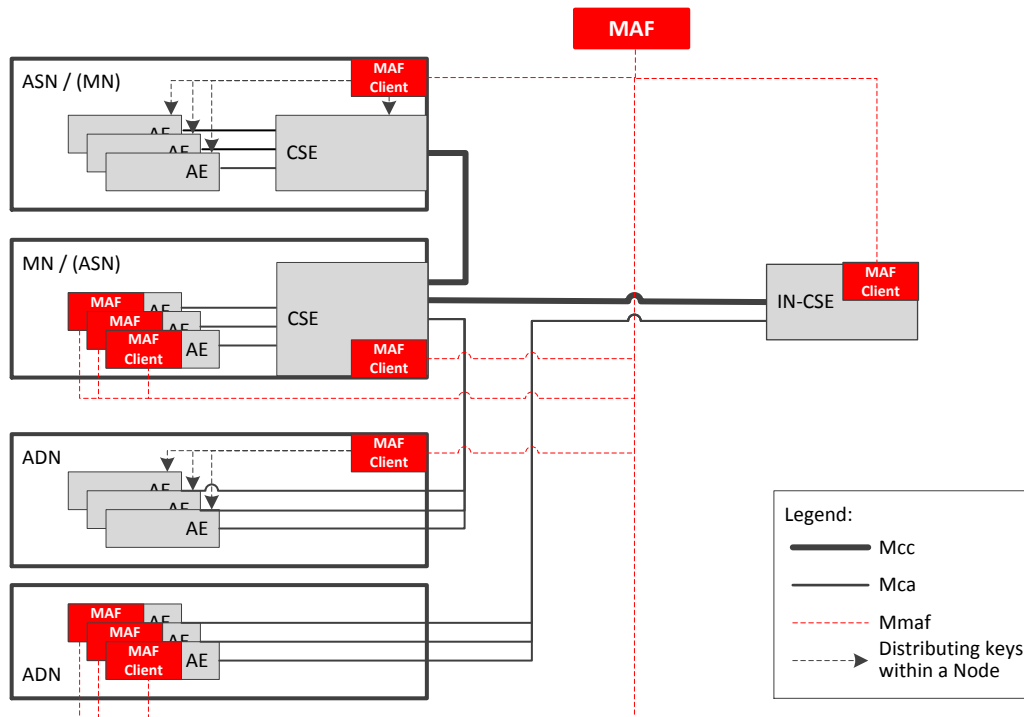


Figure 6.1.1-1: Reference Architecture for MAF

The administrating stakeholder authorizes the MAF's services to MAF clients, and oversees authorizing the distribution of symmetric keys. A MAF may provide its services on behalf of multiple administrating stakeholders. A MAF Client may be associated with multiple administrating stakeholders, each administrating the use of the MAF within a different scope.

NOTE 1: The administrating stakeholder could be an M2M SP administrating the registration and distribution of credentials used for SAEFs and ESPrim within the M2M SP's Domain.

NOTE 2: The administrating stakeholder could be an MTE administrating the registration and distribution of credentials for ESPrim and ESData to MAF Clients belonging to a particular Application Service Provider, where the MAF Clients could be distributed over multiple M2M SP domains.

The present specification has no impact on the specifications in TS-0001 [ITU-T Y.4500.1] and TS-0004 [ITU-T Y.4500.4]. However, the MAF Interface uses much of the specification in TS-0004 [ITU-T Y.4500.4] and in particular allows use of the HTTP binding in TS-0008 [ITU-T Y.4500.8], the CoAP binding in TS-0009 [ITU-T Y.4500.9] and the WebSocket binding in TS-0020 [ITU-T Y.4500.20].

NOTE: The MQTT binding in TS-0010 [ITU-T Y.4500.10] is not suitable for the MAF Interface, because the MAF Interface assumes a TLS or DTLS connection from the MAF Client to the MAF – which is not possible using the MQTT binding

The MAF Interface incorporates the following concepts from the Mcc/Mca reference points:

- The concept of operations acting on resources.
- The resource addressing from Mcc/Mca is used.
- The universal attributes and some common attributes of resources.

The MAF Interface differs from Mcc/Mca in the following ways:

- The MAF Client can only communicate directly with the MAF – there are no transited CSEs. Only Blocking Mode communication method is supported.
- None of the resource types applicable on Mcc/Mca are used.
 - Access control decisions use simple access control list for Retrieve access, and *<accessControlPolicy>* resources are not used for resources hosted by the MAF. A consequence of this is that the *accessControlPolicyIDs* attributes are not needed in the resources hosted by the MAF.
 - The *<subscription>* resource and NOTIFY operations are not supported.
 - There is no AE registration or CSE registration, but a similar process where a MAF Client creates a *<mafClientReg>* (MAF Client registration record) resource on the MAF.
 - There are no announced resources.

The hierarchy of resources hosted by a MAF shall be as follows:

- *<MAFBase>* resource type is the structural root for all the resources that are residing on a MAF. This resource is implicitly created by the MAF and uses the fixed resource name “maf” and contains following child resources:
 - *<mafClientReg>* resource. It confirms the MAF Client’s registration to an administrating stakeholder, and can contain configuration information to be returned to the MAF Client.
 - *<symmKeyReg>* resources. It is created by the MAF Client, and contains symmetric keys for retrieval by another MAF Client.

6.1.2 MAF Interface Overview

This MAF Interface overview is based on the specification in clause 6 of oneM2M TS-0004 [ITU-T Y.4500.4].

Identifiers such as M2M-SP-ID, AE-ID and CSE-ID as defined in 6.2.3 of [ITU-T Y.4500.4] also apply to the MAF Interface. M2M Trust Enablers (MTEs) are identified using an M2M-SP-ID.

Resources are addressed as specified in clause 6.2.4 in [ITU-T Y.4500.4].

Common data types applicable to the MAF Interface are inherited from clause 6.3 of [ITU-T Y.4500.4].

Table 6.2-1 and 6.2-2 list the request and response primitive parameters inherited from clauses 6.4.1 and 6.4.2 in [ITU-T Y.4500.4], respectively; the data types of these parameters are unchanged. The **From** parameter shall include the MAF client ID which can be a Node-ID, AE-ID or CSE-ID, depending on whether the client acts on behalf of a node, AE or CSE. Note that this is in contrast to primitives on the Mca and Mcc interface, where the **From** primitive parameter cannot include a Node-ID.

NOTE: All other optional request and response primitive parameters defined in clause 6.4.1 of [ITU-T Y.4500.4] are not used on the MAF Interface.

Table 6.1.2-1: MAF Interface request primitive parameters

Parameter	Multiplicity	Notes
Operation	1	
To	1	
From	0..1	If not present, the MAF internally assigns From to be the identity of the Node, CSE or AE associated with the credential used for the MAF Handshake procedure.
Request Identifier	1	
Resource Type	0..1	
Content	0..1	
Result Content	0..1	

Table 6.1.2-2: MAF Interface response primitive parameters

Parameter	Multiplicity	Notes
Response Status Code	1	
Request Identifier	1	
Content	0..1	

Data types associated with the resources applicable to the MAF Interface are defined in clause 9.

Table 6.1.2-3 lists the response status codes from clause 6.6 of [ITU-T Y.4500.4] which are supported by the MAF Interface.

Table 6.1.2-3: Response status codes supported by the MAF Interface

Response status codes	Interpretation
2000	OK
2001	CREATED
2002	DELETED
2004	UPDATED
4000	BAD_REQUEST
4004	NOT_FOUND
4005	OPERATION_NOT_ALLOWED
4103	ACCESS_DENIED
5000	INTERNAL_SERVER_ERROR

The MIME media types defined in clause 6.7 of [ITU-T Y.4500.4] shall be supported on the MAF interface. The notification related Media types vnd.onem2m-ntfy+json, vnd.onem2m-ntfy+cbor, vnd.onem2m-preq+xml do not apply to the MAF interface.

Virtual resources (clause 6.8 of [ITU-T Y.4500.4]) are not supported by the MAF Interface.

6.2 MEF Interface

6.2.1 Introduction

The M2M Enrolment Function (MEF) is an essential part of the oneM2M Remote Security Provisioning architecture.

Clause 6.1.2.1 of TS-0003 [ETSI TS 118.103] defines the following three variants of Remote Security Provisioning Frameworks (RSPF):

- Pre-Provisioned Symmetric Key RSPF,
- Certificate-Based RSPF,
- GBA-based RSPF.

The MEF interface defined in the present specification applies to Pre-Provisioned Symmetric Key RSPF and Certificate-Based RSPF only. For interfaces and procedures applicable to GBA-based RSPF see clause 8.3.2.3 of TS-0003 [ETSI TS 118.103].

When using Pre-Provisioned Symmetric Enrollee Key RSPF or Certificate-Based RSPF, the MEF serves a number of different use cases which are summarized as follows:

1. The MEF provisions an Enrollee to perform MAF Security Framework procedures with a MAF as defined in clause 8.8.2 of TS-0003 [ETSI TS 118.103].
2. The MEF provisions an Entity A and an Entity B to perform Security Association Establishment as defined in clauses 8.2.2.1 and 8.2.2.2 of TS-0003 [ETSI TS 118.103].
3. The MEF provisions an originator and a receiver of a primitive with credentials to enable End-to-End Security of Primitives (ESPrim) with security credentials as specified in clause 8.4 of TS-0003 [ETSI TS 118.103].
4. The MEF provisions the source and target endpoints of End-to-End Security of Data (ESData) as specified in clause 8.5 of TS-0003 [ETSI TS 118.103].

This specification defines messages and procedures for the above listed MEF use cases.

NOTE 1: A MEF may also be implemented as a Device Management server using device management protocols such as OMA DM, OMA LwM2M and BBF TR-069. Such procedures are defined in TS-0003 [ETSI TS 118.103] and TS-0022 [ITU-T Y.4500.22].

Like the Mmaf Interface, the Mmef Interface is a simple variant of the Mcc/Mca reference points specifying the interaction of MEF Clients with a M2M Enrolment Function (MEF), managing symmetric keys on behalf of an *administrating stakeholder* such as an M2M SP or third party M2M Trust Enabler (MTE). The present document does not specify the operation and management of the MEF required to support these procedures.

A MEF Client interacts with the MEF on behalf of a Node (ADN, ASN, IN or MN), or a CSE or an AE for use case 1 and 2 in the above list. Figure 6.2.1-1 defines the reference point Mmef between MEF clients and a MEF, and between MEF and MAF.

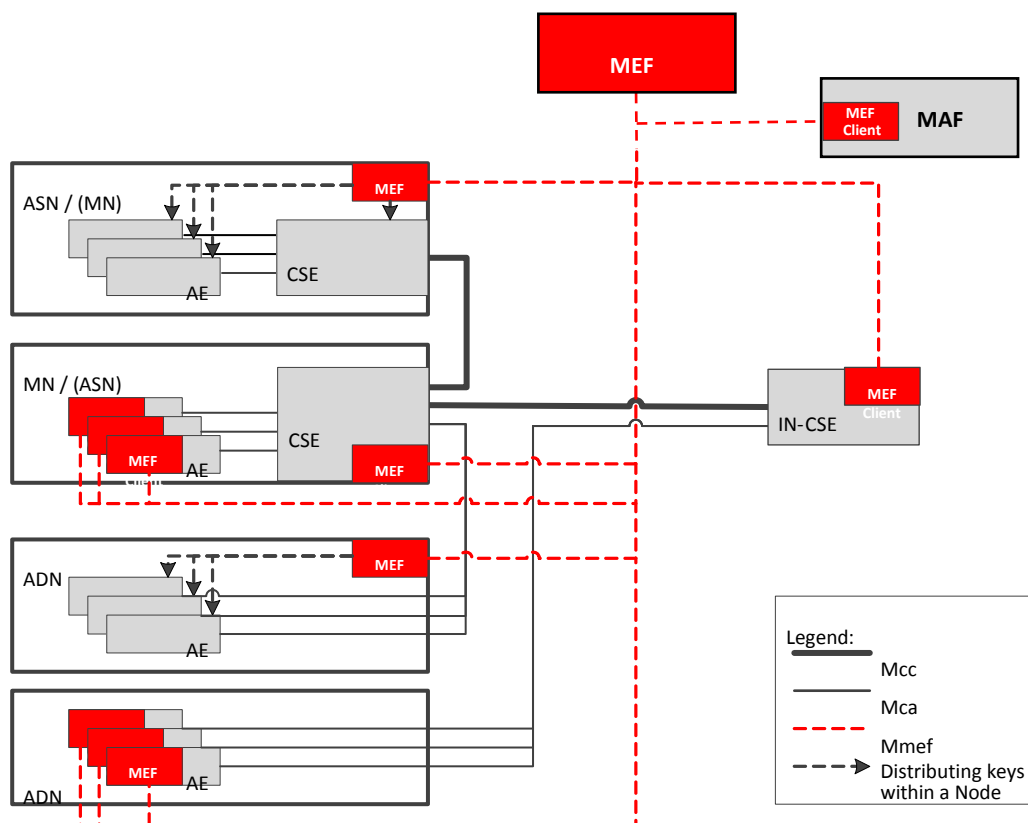


Figure 6.2.1-1: Reference Architecture for MEF

The administrating stakeholder authorizes the MEF's services to MEF clients. A MEF may provide its services on behalf of multiple administrating stakeholders. A MEF Client may be associated with multiple administrating stakeholders, each administrating the use of the MEF within a different scope.

NOTE 1: The administrating stakeholder could be an M2M SP administrating the registration and distribution of credentials used for SAEFs and ESPrim within the M2M SP's Domain.

NOTE 2: The administrating stakeholder could be an MTE administrating the registration and distribution of credentials for ESPrim and ESData to MEF Clients belonging to a particular Application Service Provider, where the MEF Clients could be distributed over multiple M2M SP domains.

The present specification has no impact on the specifications in TS-0001 [ITU-T Y.4500.1] and TS-0004 [ITU-T Y.4500.4]. However, the MEF Interface uses much of the specification in TS-0004 [ITU-T Y.4500.4] and in particular allows use of the HTTP binding in TS-0008 [ITU-T Y.4500.8], the CoAP binding in TS-0009 [ITU-T Y.4500.9] and the WebSocket binding in TS-0020 [ITU-T Y.4500.20].

NOTE: The MQTT binding in TS-0010 [ITU-T Y.4500.10] is not suitable for the MEF Interface, because the MEF Interface assumes a TLS or DTLS connection from the MEF Client to the MEF – which is not possible using the MQTT binding

The MEF Interface incorporates the following concepts from the Mcc/Mca reference points:

1. The concept of operations acting on resources.

2. The resource addressing from Mcc/Mca is used.
3. The universal attributes and some common attributes of resources.

The MEF Interface differs from Mcc/Mca in the following ways:

4. The MEF Client can only communicate directly with the MEF – there are no transited CSEs. Only Blocking Mode communication method is supported.
5. None of the resource types applicable on Mcc/Mca are used.
 - Access control decisions use simple access control list for Retrieve access, and *<accessControlPolicy>* resources are not used for resources hosted by the MEF. A consequence of this is that the *accessControlPolicyIDs* attributes are not needed in the resources hosted by the MEF.
 - The *<subscription>* resource and NOTIFY operations are not supported.
 - There is no AE registration or CSE registration, but a similar process where a MEF Client creates a *<mefClientReg>* (MEF Client registration record) resource on the MEF.
 - There are no announced resources.

The hierarchy of resources hosted by a MEF shall be as follows:

6. *<MEFBase>* resource type is the structural root for all the resources that are residing on a MEF. This resource is implicitly created by the MEF and uses the fixed resource name “mef” and contains following child resources:
 - *<mefClientReg>* resource. It confirms the MEF Client’s registration to an administrating stakeholder, and can contain configuration information to be returned to the MEF Client.
 - *<symmKeyReg>* resources. It is created by the MEF Client, and contains symmetric keys for retrieval by another MEF Client.

6.2.2 MEF Interface Overview

This MEF Interface overview is based on the specification in clause 6 of oneM2M TS-0004 [ITU-T Y.4500.4].

Identifiers such as M2M-SP-ID, AE-ID and CSE-ID as defined in 6.2.3 of [ITU-T Y.4500.4] also apply to the MEF Interface. M2M Trust Enablers (MTEs) are identified using an M2M-SP-ID.

Resources are addressed as specified in clause 6.2.4 in [ITU-T Y.4500.4].

Common data types applicable to the MEF Interface are inherited from clause 6.3 of [ITU-T Y.4500.4].

Table 6.2-1 and 6.2-2 list the request and response primitive parameters inherited from clauses 6.4.1 and 6.4.2 in [ITU-T Y.4500.4], respectively; the data types of these parameters are unchanged. The **From** parameter shall include the MEF client ID which can be a Node-ID, AE-ID or CSE-ID, depending on whether the client acts on behalf of a node, AE or CSE. Note that this is in contrast to primitives on the Mca and Mcc interface, where the **From** primitive parameter cannot include a Node-ID.

NOTE: All other optional request and response primitive parameters defined in clause 6.4.1 of [ITU-T Y.4500.4] are not used on the MEF Interface.

Table 6.2.2-1: MEF Interface request primitive parameters

Parameter		Multiplicity	Notes
Operation		1	
To		1	
From		0..1	If not present, the MEF internally assigns From to be the identity of the Node, CSE or AE associated with the credential used for the MEF Handshake procedure.
Request Identifier		1	
Resource Type		0..1	
Content		0..1	
Result Content		0..1	

Table 6.2.2-2: MEF Interface response primitive parameters

Parameter	Multiplicity	Notes
Response Status Code	1	
Request Identifier	1	
Content	0..1	

Data types associated with resources applicable to the MEF Interface are defined in clause 9.

The response status codes listed in Table 6.1.2-3 also apply to the MEF Interface.

The MIME media types defined on clause 6.7 of [ITU-T Y.4500.4] shall be supported on the MEF interface. The notification related Media types vnd.onem2m-ntfy+json, vnd.onem2m-ntfy+cbor, vnd.onem2m-preq+xml do not apply to the MEF interface.

Virtual resources (clause 6.8 in [ITU-T Y.4500.4]) are not supported by the MEF Interface.

7 Processing and Representation of Primitives

7.1 Common aspects of the MAF and MEF interface

This clause corresponds to the specification in clause 7 and 8 of oneM2M TS-0004 [ITU-T Y.4500.4].

Both, MAF and MEF Interface request primitive formats conform to clause 7.2.1.1 [ITU-T Y.4500.4], constrained to the CRUD operations, with request parameters listed in Table 5.1.2-1 and Table 5.2.2-1, respectively.

Both, MAF and MEF Interface response primitive formats conform to clause 7.2.1.2 in [ITU-T Y.4500.4], constrained to the CRUD operations, with response parameters listed in Table 7.1.2-2 and Table 7.2.2-2, respectively.