

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

Recommendation ITU-T Y.4500.32

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

FUTURE NETWORKS

CLOUD COMPUTING

BIG DATA

QUANTUM KEY DISTRIBUTION NETWORKS

INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES

General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4500.32

oneM2M – MAF and MEF interface specification

Summary

Recommendation ITU-T Y 4500.32 specifies communication between the machine-to-machine (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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4500.32	2018-06-29	20	11.1002/1000/13642

Keywords

Authentication, enrolment, oneM2M, provisioning, security.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2022

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 General description.....	3
6.1 MAF interface	3
6.2 MEF interface	6
7 Processing and representation of primitives	10
7.1 Common aspects of the MAF and MEF interface.....	10
7.2 MAF interface	10
7.3 MEF interface	11
8 Resource types definitions.....	12
8.1 Namespaces used for resource and data types.....	12
8.2 Resource type <MAFBase>	12
8.3 Resource type <MEFBase>	12
8.4 Resource type <mafClientReg>	13
8.5 Resource type <mefClientReg>	14
8.6 Resource type <symmKeyReg>	14
8.7 Resource type <mefClientCmd>	15
9 Resource-type specific procedures and definitions	16
9.1 Resource type <MAFBase>	16
9.2 Resource type <MEFBase>	17
9.3 Resource type <mafClientReg>	19
9.4 Resource type <mefClientReg>	22
9.5 Resource type <symmKeyReg>	26
9.6 Resource type <mefClientCmd>	29
10 Short names	32
10.1 Introduction	32
10.2 Security-specific oneM2M resource attributes.....	33
10.3 Security-specific oneM2M resource types	33
10.4 Security-specific oneM2M complex data type members	34
Annex A – oneM2M specification update and maintenance control procedure.....	36
Bibliography.....	37

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 Association of Radio Industries and Businesses (Japan) (ARIB), Alliance for Telecommunications Industry Solutions (ATIS), China Communications Standards Association (CCSA), European Telecommunications Standards Institute (ETSI) [b-ETSI TS 118 132], Telecommunications Industry Association (US) (TIA), Telecommunications Standards Development Society India (TSDSI), Telecommunications Technology Association (TTA) and Telecommunication Technology Committee (TTC).

2 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.

- [ITU-T Y.4500.1] Recommendation ITU-T Y 4500.1 (2018), *oneM2M – Functional architecture*.
- [ITU-T Y.4500.4] Recommendation ITU-T Y 4500.4 (2018), *oneM2M – Service layer core protocol specification*.
- [ITU-T Y.4500.8] Recommendation ITU-T Y 4500.8 (2018), *oneM2M – CoAP protocol binding*.
- [ITU-T Y.4500.9] Recommendation ITU-T Y 4500.9 (2018), *oneM2M – HTTP protocol binding*.
- [ITU-T Y.4500.10] Recommendation ITU-T Y 4500.10 (2018), *oneM2M – MQTT protocol binding*.
- [ITU-T Y.4500.11] Recommendation ITU-T Y 4500.11(2018), *oneM2M – Common terminology*.
- [ITU-T Y.4500.20] Recommendation ITU-T Y 4500.20 (2018), *oneM2M – WebSocket protocol binding*.
- [ITU-T Y.4500.22] Recommendation ITU-T Y 4500.22 (2018), *oneM2M – Field device configuration*.
- [ETSI TS 118 103] ETSI TS 118 103 V2.12.01 (2016), *oneM2M, Security solutions*.

3 Definitions

For the purposes of this Recommendation, the terms and definitions given in [ITU-T Y.4500.11], [ETSI TS 118 103] and the following apply.

3.1 Terms defined elsewhere

This Recommendation uses the following 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

This Recommendation defines the following terms:

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

This Recommendation uses the following abbreviations and acronyms:

For the purposes of this Recommendation, the abbreviations given in [ITU-T Y.4500.11], [ETSI TS 118 103] and the following apply:

AE	Application Entity
AE-ID	Application Entity Identifier
API	Application Program Interface
CoAP	Constrained Application Protocol
CRUD	Create Retrieve Update Delete
CSE	Common Services Entity
CSE-ID	Common Service Entity Identifier
DTLS	Datagram Transport Layer Security
ESData	End-to-end Security of Data
ESPrim	End-to-end Security of Primitives
FQDN	Fully Qualified Domain Name
GBA	Generic Bootstrapping Architecture
MAF	M2M Authentication Function
MEF	M2M Enrolment Function

MQTT	Message Queue Telemetry Transport
MTE	M2M Trust Enabler
RSPF	Remote Security Provisioning Framework
SP	Service Provider
SUID	Security Usage Identifier
TLS	Transport Layer Security

5 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in this Recommendation are to be interpreted as described:

Shall/Shall not:

Requirements

- 1) effect on this Recommendation: This Recommendation 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 with this Recommendation) must support it;
- 3) effect on deployments: Every deployment (M2M service based on this Recommendation) must use the standardized feature where applicable – otherwise e.g., interoperability problems with other services could arise.

Should/Should not:

Recommendation

- 1) effect on this Recommendation: This Recommendation 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 this Recommendation: This Recommendation 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 MAF, acting on behalf of an *administrating stakeholder* such as an M2M service provider (SP) or third party M2M trust enabler (MTE). This Recommendation 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 common services entity (CSE) or an application entity (AE).

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

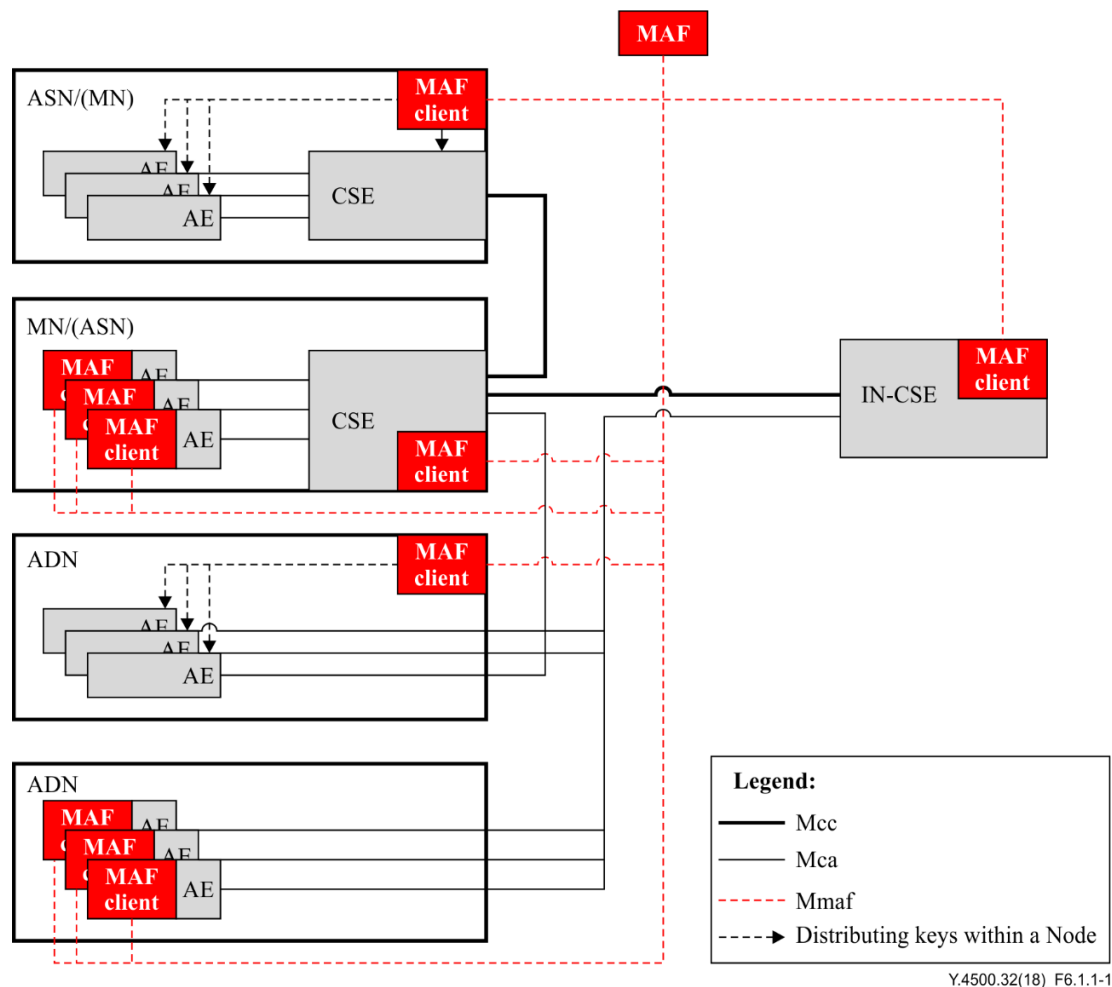


Figure 6.1.1-1 – Reference architecture for MAF

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 end-to-end security of primitives (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 end-to-end security of data (ESData) to MAF clients belonging to a particular application service provider, where the MAF clients could be distributed over multiple M2M SP domains.

This Recommendation 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 constrained application protocol (CoAP) binding in TS-0009 [ITU-T Y.4500.9] and the WebSocket binding in TS-0020 [ITU-T Y.4500.20].

NOTE 3 – The message queue telemetry transport (MQTT) binding in TS-0010 [ITU-T Y.4500.10] is not suitable for the MAF interface, because the MAF interface assumes a transport layer security (TLS) or datagram transport layer security (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 [ITU-T Y.4500.4].

Identifiers such as M2M-SP-ID, application entity identifier (AE-ID) and common service entity identifier (CSE-ID) as defined in clause 6.2.3 of [ITU-T Y.4500.4] also apply to the MAF interface. 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].

Tables 6.1.2-1 and 6.1.2-2 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. 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 <i>From</i> 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 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):

- 1) pre-provisioned symmetric key RSPF;
- 2) certificate-based RSPF;
- 3) generic bootstrapping architecture (GBA)-based RSPF.

The MEF interface defined in this Recommendation 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 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 ESData as specified in clause 8.5 of TS-0003 [ETSI TS 118 103].

This Recommendation 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 Open Mobile Alliance device management (OMA-DM), OMA lightweight M2M (LwM2M) and Broadband Forum (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 MEF, managing symmetric keys on behalf of an *administrating stakeholder* such as an M2M SP or third party MTE. This Recommendation 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.

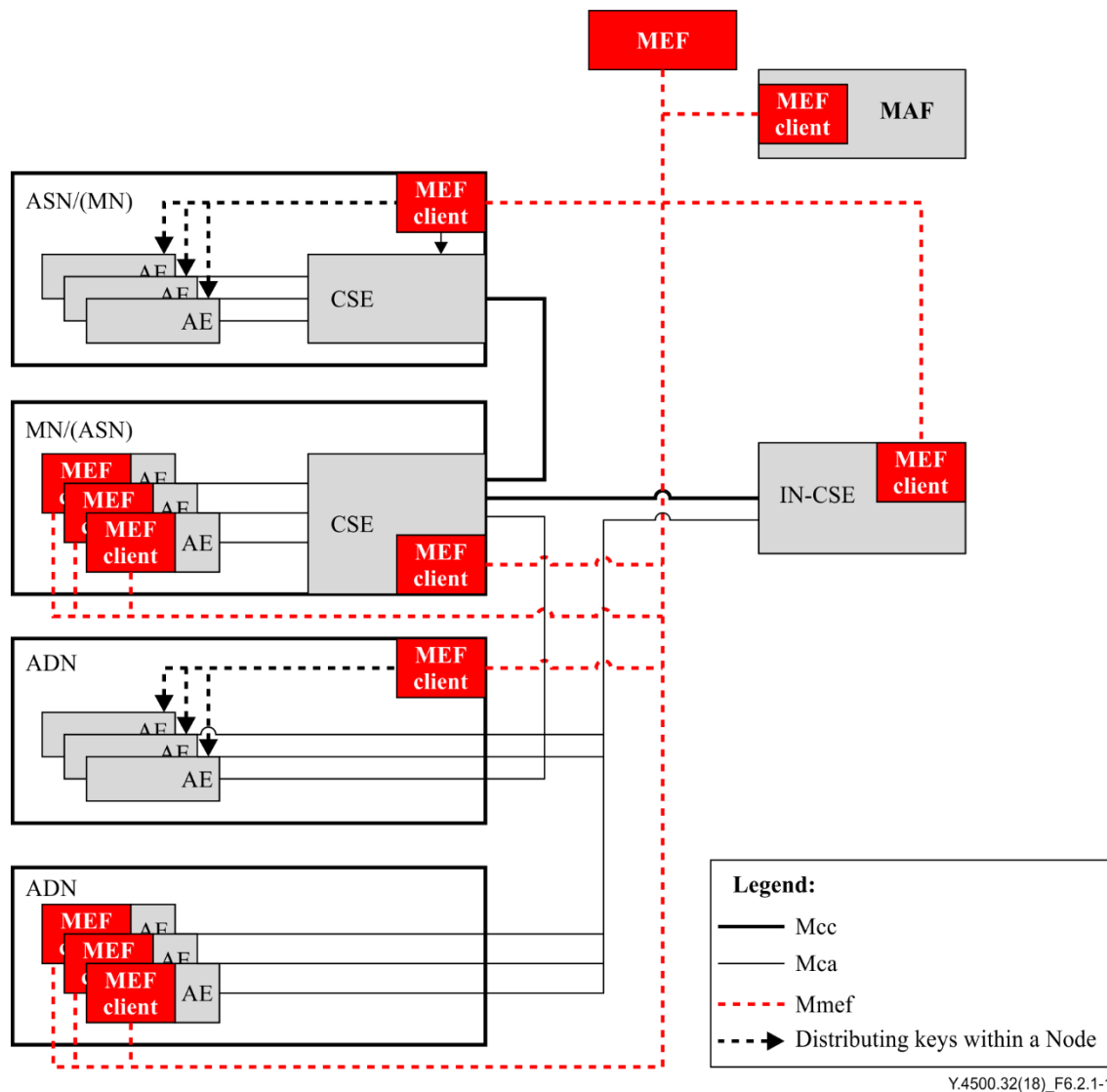


Figure 6.2.1-1 – Reference architecture for MEF

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 2 – 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 3 – 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.

This Recommendation 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 4 – 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 and 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 [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. 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].

Tables 6.2.2-1 and 6.2.2-2 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. 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 <i>From</i> 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 in 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 clauses 7 and 8 of [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 create retrieve update delete (CRUD) operations, with request parameters listed in Table 7.2.1.1-1 of [ITU-T Y.4500.4].

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 7.2.1.2-1 of [ITU-T Y.4500.4].

7.2 MAF interface

The MAF interface generic resource request procedure for originators and receivers conforms to clauses 7.2.2.1 and 7.2.2.2 of [ITU-T Y.4500.4], with the following clarification:

- the MAF client acts as the originator, and the MAF acts as the receiver and resource hosting entity;
- the MAF handshake procedure (clause 8.8.2.2 of [ETSI TS 118 103]) is used for mutual authentication of the MAF client and MAF;

- the operation shall be one of the CRUD operations;
- the request and response parameters shall conform to Tables 6.1.2-1 and 6.2.2-2, respectively;
- "blocking mode" communication method shall be used;
- the step Recv-6.3: "Check authorization of the Originator" is replaced by the authorization processes described in the MAF interface resource-type specific procedures in clause 9.

The originator actions, receiver actions and hosting CSE actions conform to clause 7.3 of [ITU-T Y.4500.4], with clause 7.3.3.15 of [ITU-T Y.4500.4] replaced by the authorization processes described in the MAF interface resource-type specific procedures in clause 9.

The management common operations in clause 7.3.4 of [ITU-T Y.4500.4] do not apply to the MAF interface.

The resource-type-specification conventions apply to the specification in clause 8, but the remainder of clause 7.4 of [ITU-T Y.4500.4] does not apply to the MAF interface.

Clause 7.5.1 of [ITU-T Y.4500.4] (regarding notification) does not apply to the MAF interface. Elements contained in the Content primitive parameter conform to clause 7.5.2 of [ITU-T Y.4500.4].

The representation of MAF interface primitives in data transfer conforms to clause 9. Clause 10 contains additional short names specific to both, the MAF and MEF interfaces.

7.3 MEF interface

The MEF interface generic resource request procedure for originators and receivers conforms to clauses 7.2.2.1 and 7.2.2.2 of [ITU-T Y.4500.4] with the following clarification:

- the MEF client acts as the originator, and the MEF acts as the receiver and resource hosting entity;
- the MEF handshake procedure (clause 8.8.2.2 of [ETSI TS 118 103]) is used for mutual authentication of the MEF client and MEF;
- the operation shall be one of the CRUD operations;
- the request and response parameters shall conform to Tables 6.2.2-1 and 6.2.2-2;
- the "Blocking Mode" communication method shall be used;
- the step Recv-6.3: "Check authorization of the Originator" is replaced by the authorization processes described in the MEF interface resource-type specific procedures in clause 9.

The originator actions, receiver actions and hosting CSE actions conform to clause 7.3 of [ITU-T Y.4500.4], with clause 7.3.3.15 of [ITU-T Y.4500.4] replaced by the authorization processes described in the MEF interface resource-type specific procedures in clause 9.

The management common operations in clause 7.3.4 of [ITU-T Y.4500.4] do not apply to the MEF interface.

The resource-type-specification conventions apply to the specification in clause 9, but the remainder of clause 7.4 of [ITU-T Y.4500.4] does not apply to the MEF interface.

Clause 7.5.1 of [ITU-T Y.4500.4] (regarding notification) does not apply to the MEF interface. Elements contained in the content primitive parameter conform to clause 7.5.2 of [ITU-T Y.4500.4].

The representation of MEF interface primitives in data transfer conforms to clause 9. Clause 10 contains additional short names specific to the both, the MAF and MEF interfaces.

8 Resource types definitions

8.1 Namespaces used for resource and data types

Representations of resources applicable to the MAF and MEF interfaces employ the namespace identifier "sec:" for global XML elements associated with a resource type. Data types of the attributes and complex-type elements of these resource types may use any of the namespace identifiers listed in Table 8.1-1.

Any data types of XML elements defined for use in this Recommendation shall be one of namespaces in Table 8.1-1.

Table 8.1-1 – Namespaces applicable to resource types defined in this Recommendation

Name space	prefix	Namespace definition	Types defined in
oneM2M Security	sec:	http://www.onem2m.org/xml/securityProtocols	TS-0032 and TS-0003
oneM2M protocol CDT	m2m:	http://www.onem2m.org/xml/protocol	TS-0004
Device Configuration	dcfg:	http://www.onem2m.org/xml/deviceConfig	TS-0022

XML schema documents produced by oneM2M relevant to this specification can be found at [b-oneM2M.XML].

8.2 Resource type <MAFBase>

The <MAFBase> resource shall represent a MAF.

The <MAFBase> resource shall contain the child resources specified in Table 8.2-1.

Table 8.2-1 – Child resources of <MAFBase> resource

Child resources of <MAFBase>	Child resource type	Multiplicity	Description
[variable]	<mafClientReg>	0..n	See clause 8.4
[variable]	<symmKeyReg>	0..n	See clause 8.6

The <MAFBase> resource shall contain the attributes specified in Table 8.2-2.

Table 8.2-2 – Attributes of <MAFBase> resource

Attributes of <MAFBase>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceName	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]. Shall be fixed to "maf"
creationTime	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
labels	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]

8.3 Resource type <MEFBase>

The <MEFBase> resource shall represent a MEF.

The <MEFBase> resource shall contain the child resources specified in Table 8.3-1.

Table 8.3-1 – Child resources of <MEFBase> resource

Child resources of <MEFBase>	Child resource type	Multiplicity	Description
[variable]	<mefClientReg>	0..n	See clause 8.5
[variable]	<symmKeyReg>	0..n	See clause 8.6

The <MEFBase> resource shall contain the attributes specified in Table 8.3-2.

Table 8.3-2 – Attributes of <MEFBase> resource

Attributes of <MEFBase>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceName	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]. Shall be fixed to "mef"
creationTime	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
labels	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]

8.4 Resource type <mafClientReg>

The <mafClientReg> resource shall represent a MAF client enrolled with an M2M SP or MTE.

NOTE – A single MAF client can be enrolled with at most one M2M SP and any number of MTEs (typically enabling end-to-end security to MAF clients outside the MAF client's M2M SP's domain). Consequently, a single MAF client can be associated with multiple <mafClientReg> resources on multiple MAFs. It is also possible that a single MAF client can be associated with multiple <mafClientReg> resources on a single MAF acting on behalf of multiple administrating stakeholders.

The <mafClientReg> resource shall contain no child resources.

The <mafClientReg> resource shall contain the attributes specified in Table 8.4-1.

Table 8.4-1 – Attributes of <mafClientReg> resource

Attributes of <mafClientReg>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
resourceName	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
parentID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
creationTime	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]
labels	1	RW	See clause 9.6.1.3 of [ITU-T Y.4500.1]
expirationTime	1	WO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
creator	1	WO	His attribute shall include the identifier of the MAF client which has created this resource.
adminFQDN	1	WO	FQDN of the M2M SP or MTE who is the administrating stakeholder of this enrolment.
assignedSymmKeyID	0..1	RO	When the MAF client uses a symmetric key to authenticate to the MAF, then the MAF may use this attribute to provide a symmetry key identifier within the domain of the MAF. Assigned by the MAF.

8.5 Resource type <mefClientReg>

The <mefClientReg> resource shall represent a MEF client enrolled with an M2M SP or MTE.

NOTE – A single MEF client can be enrolled with at most one M2M SP and any number of MTEs (typically enabling end-to-end security to MEF clients outside the MEF client's M2M SP's domain). Consequently, a single MEF client can be associated with multiple <mefClientReg> resources on multiple MEFs. It is also possible that a single MEF client can be associated with multiple <mefClientReg> resources on a single MEF acting on behalf of multiple administrating stakeholders.

The <mefClientReg> resource shall contain the child resources specified in Table 8.5-1.

Table 8.5-1 – Child resources of <mefClientReg> resource

Child resources of <mefClientReg>	Child resource type	Multiplicity	Description
"cmd"	<mefClientCmd>	1	See clause 8.7

The <mefClientReg> resource shall contain the attributes specified in Table 8.5-2.

Table 8.5-2 – Attributes of <mefClientReg> resource

Attributes of <mefClientReg>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
resourceName	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
labels	1	RW	See clause 9.6.1.3 of [ITU-T Y.4500.1].
expirationTime	1	WO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
creator	1	WO	This attribute shall include the identifier of the MEF client which has created this resource.
adminFQDN	1	WO	Fully qualified domain name (FQDN) of the M2M SP or MTE who is the administrating stakeholder of this enrolment
assignedSymmKeyID	0..1	RO	When the MEF client uses a symmetric key to authenticate to the MEF, then the MEF may use this attribute to provide a symmetry key identifier within the domain of the MEF. Assigned by the MEF.
sourceIDs	0..1	RW	List of AE-IDs and CSE-IDs associated with a MEF client acting on behalf of a node. This attribute shall be supplied if the creator attribute includes a Node-ID

8.6 Resource type <symmKeyReg>

The <symmKeyReg> resource shall represent a symmetric key that a source MAF client or a source MEF client has established with the MAF or MEF, respectively, for distributing to authorized target MAF or MEF clients and/or another MAF or MEF. The MAF or MEF client provides a list of authorized targets when the resource is created – this Recommendation does not specify how the MAF or MEF associates the list with the resource. The MAF or MEF, in coordination with the

identified administrating stakeholder (M2M SP or MTE), can modify the list of authorized targets and the *expirationTime*.

The *<symmKeyReg>* resource shall contain no child resources.

The *<symmKeyReg>* resource shall contain the attributes specified in Table 8.6-1.

Table 8.6-1 – Attributes of *<symmKeyReg>* resource

Attributes of <i><symmKeyReg></i>	Multiplicity	RW/ RO/ WO	Description
<i>resourceType</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>resourceID</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>resourceName</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1]. This value is used as the relative part of the identifier for the symmetric key in security protocols.
<i>parentID</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>creationTime</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>labels</i>	0..1	RW	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>expirationTime</i>	1	WO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>creator</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>adminFQDN</i>	1	WO	FQDN of the administrating stakeholder (M2M SP or MTE) associated with this enrolment.
<i>SUID</i>	1	WO	A security usage identifier (SUID) constraining the use of the symmetric key associated with this resource
<i>targetIDs</i>	1 (L)	RW	List of AE-ID(s) and/or CSE-ID(s) and/or and/or Node-ID(s) identifying the AE(s) and/or CSE(s) and/or Node(s) authorized to retrieve the resource. Only the creator and administrating stakeholder (identified by adminFQDN) are authorized to access this attribute.
<i>keyValue</i>	1	WO	The value of the key to be provided to the identifier targets. May be provided in the Create request or derived by the MAF or MEF client and MAF or MEF from the TLS handshake parameters.

8.7 Resource type *<mefClientCmd>*

A *<mefClientCmd>* resource includes instructions for the MEF client associated with the parent *<mefClientReg>* resource to be executed.

The *<mefClientCmd>* resource shall contain no child resources.

The *<mefClientCmd>* resource shall contain the attributes specified in Table 8.7-1.

Table 8.7-1 – Attributes of <mefClientCmd> resource

Attributes of <mefClientCmd>	Multiplicity	RW/ RO/ WO	Description
<i>resourceType</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>resourceID</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>resourceName</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>parentID</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>creationTime</i>	1	RO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>labels</i>	1	RW	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>expirationTime</i>	1	WO	See clause 9.6.1.3 of [ITU-T Y.4500.1].
<i>cmdID</i>	1	RW	This attribute shall include a MEF-assigned identifier of a command issued by the MEF. See clause 8.3.9.1 of [ETSI TS 118 103] for further details.
<i>cmdDescription</i>	1	RO	This attribute provides the description of a command issued by the MEF to be executed by the MEF client. See clause 8.3.9.4 of [ETSI TS 118 103] for further details.
<i>cmdStatusCode</i>	1	RW	This attribute shall be used for the status of the command issued by the MEF. See clause 8.3.9.5 of [ETSI TS 118 103] for further details.

9 Resource-type specific procedures and definitions

9.1 Resource type <MAFBase>

9.1.1 Introduction

A <MAFBase> resource shall represent a MAF. This <MAFBase> resource shall be the root for all the resources that are residing on the MAF.

Table 9.1.1-1 – Data type definition of <MAFBase>

Data type ID	File name	Note
MAFBase	SEC-MAFBase-v2_0_0.xsd	available at [b-oneM2M.XML]

The <MAFBase> resource has no resource-specific attributes.

Table 9.1.1-2 – Child resources of <MAFBase> resource

Child resource type	Child resource name	Multiplicity	Ref. to resource type definition
<mafClientReg>	[variable]	0..n	Clause 8.4
<symmKeyReg>	[variable]	0..n	Clause 8.6

9.1.2 <MAFBase> resource specific procedures on CRUD operations

9.1.2.1 Create

Originator:

The <MAFBase> resource shall not be created via application program interface (API).

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

If the request is received, the MAF shall execute the following steps in order:

- 1) "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
- 2) "Send the Response primitive".

9.1.2.2 Retrieve

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and performing the following step in the place of step Recv-6.3: "Check authorization of the Originator":

The Receiver shall allow all Originator's to retrieve this resource.

9.1.2.3 Update

Originator:

The <MAFBase> resource shall not be updated via API.

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

- 1) If the request is received, the MAF shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

9.1.2.4 Delete

Originator:

The <MAFBase> resource shall not be DELETED via API.

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

- 1) If the request is received, the MAF shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

9.2 Resource type <MEFBase>

9.2.1 Introduction

A <MEFBase> resource shall represent a MEF. This <MEFBase> resource shall be the root for all the resources that are residing on the MEF.

Table 9.2.1-1 – Data type definition of <MEFBase>

Data type ID	File name	Note
MEFBase	SEC-MEFBase-v2_0_0.xsd	available at [b-oneM2M.XML]

The <MEFBase> resource has no resource-specific attributes.

Table 9.2.1-2 – Child resources of <MEFBase> resource

Child resource type	Child resource name	Multiplicity	Ref. to resource type definition
<mefClientReg>	[variable]	0..n	Clause 8.5
<symmKeyReg>	[variable]	0..n	Clause 8.6

9.2.2 <MEFBase> resource specific procedures on CRUD operations

9.2.2.1 Create

Originator:

The <MEFBase> resource shall not be created via API.

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

If the request is received, the MEF shall execute the following steps in order:

- 1) "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
- 2) "Send the Response primitive".

9.2.2.2 Retrieve

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and performing the following step in the place of step Recv-6.3: "Check authorization of the Originator":

The Receiver shall allow all Originator's to retrieve this resource.

9.2.2.3 Update

Originator:

The <MEFBase> resource shall not be updated via API.

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

- 1) If the request is received, the MEF shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

9.2.2.4 Delete

Originator:

The <MEFBase> resource shall not be DELETEed via API.

Receiver:

Primitive specific operation on Recv-1.0 "Check the syntax of received message":

- 1) If the request is received, the MEF shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

9.3 Resource type <mafClientReg>

9.3.1 Introduction

A <mafClientReg> resource shall represent a MAF client enrolled with the MAF on behalf of an M2M SP or M2M trust enabler. A <mafClientReg> resource shall be a child resource of the MAF's <MAFBase> resource.

Table 9.3.1-1 – Data type definition of <mafClientReg>

Data type ID	File name	Note
mafClientReg	SEC-mafClientReg-v2_0_0.xsd	available at [b-oneM2M.XML]

Table 9.3.1-2 – Universal/Common attributes of <mafClientReg> resource

Attribute name	Request optionality	
	Create	Update
@resourceName	NP	NP
resourceType	NP	NP
resourceID	NP	NP
parentID	NP	NP
creationTime	NP	NP
labels	O	O
expirationTime	M	M
creator	NP	NP

Table 9.3.1-3 – Resource specific attributes of <mafClientReg> resource

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
adminFQDN	M	NP	xs:anyURI	No default
assignedSymmKeyID	NP	NP	sec:credentialID	No default

The <mafClientReg> resource shall contain no child resources.

9.3.2 <mafClientReg> resource specific procedures on CRUD operations

9.3.2.1 Create

This procedure is denoted *MAF Client Registration* in clause 8.8.2.3 of TS-0003 [ETSI TS 118 103]. The **To** parameter of the <mafClientReg> create request primitive includes the MAF-FQDN and the character "-" (dash) as a shorthand notation for the name of the <MAFBase> resource:

//{MAF-FQDN}/-/

Example: //maf123.mafprovider.org/-/

The MAF-FQDN represents a globally unique identifier of a MAF (i.e., MAF ID).

The **From** parameter of the <mafClientReg> create request primitive shall be left empty if the MAF client does not have a MAF client ID assigned yet. If the MAF client interfaces with the MAF on behalf of the node (clause 6.1.1), the Node-ID of the respective ADN, ASN, MN or IN shall serve as MAF client ID.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2, and with following differences:

In step Orig-6.0: "Process Response primitive", if the Originator used a symmetric key to authenticate to the MAF, and the <mafClientReg> resource in the response contained an *assignedSymmKeyID* attribute then the originator shall use the *assignedSymmKeyID* attribute to identify this symmetric key when it is subsequently used in authenticating to the MAF.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2, and with following differences:

The Receiver shall perform the following steps in order in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized to register with the administrating stakeholder (M2M SP or MTE) identified by *adminFQDN* attribute. This Recommendation does not specify how the Receiver makes this determination.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following steps in order as part of "Create the resource" (clause 7.3.3.5 of [ITU-T Y.4500.4]) during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) If the Originator authenticated using symmetric key with a key identifier which does not use the Receiver's FQDN, then:
 - a. The Receiver shall assign a symmetric key identifier with the Receiver's FQDN and with relative part which is unique within the scope of symmetric key identifiers issued by the Receiver. The Receiver shall associate this symmetric key identifier with the symmetric key used for authenticating the Originator;
 - b. The Receiver shall set the *assignedSymmKeyID* attribute to be the Credential-ID formed from the assigned symmetric key identifier as specified in clause 10.4 of TS-0003 [ETSI TS 118 103].

- 3) If the Originator authenticated using a symmetric key with a key identifier which does not use the Receiver's FQDN, or if the Originator authenticated using a certificate, then the Receiver shall not include an *assignedSymmKeyID* attribute in the created resource.
- 4) The Receiver shall assign the *creator* attribute to an AE-ID or CSE-ID or Node-ID on instructions from the administrating stakeholder. This Recommendation does not specify any details of how the AE-ID or CSE-ID or Node-ID is determined.

9.3.2.2 Retrieve

This procedure is denoted *MAF Client Configuration Retrieval* in clause 8.8.2.4 of TS-0003 [ETSI TS 118 103]. This procedure is used to retrieve the *<mafClientReg>* resource.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2, performing the following steps in order in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.3.2.3 Update

This procedure is denoted *MAF Client Configuration Update* in clause 8.8.2.5 of TS-0003 [ETSI TS 118 103]. This procedure is used to update attributes of the *<mafClientReg>* resource, such as e.g., labels, expiration time.

Originator:

The *<mafClientReg>* resource shall not be updated by a MAF client via API.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2, and with the following differences:

The Receiver shall perform the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following step as part of "Update the resource" (clause 7.3.3.7 of [ITU-T Y.4500.4] during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) If the Originator was the Creator of the resource, then the Receiver shall perform steps 2 and 3 in clause 9.3.2.1.

9.3.2.4 Delete

This procedure is denoted *MAF Client De-Registration* in clause 8.8.2.6 of TS-0003 [ETSI TS 118 103]. This procedure enables the MAF client to delete its own *<mafClientReg>* resource on a MAF.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2, performing the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.4 Resource type *<mefClientReg>*

9.4.1 Introduction

A *<mefClientReg>* resource shall represent a MEF client enrolled with the MEF on behalf of an M2M SP or M2M trust enabler. A *<mefClientReg>* resource shall be a child resource of the MEF's *<MEFBase>* resource.

Table 9.4.1-1 – Data type definition of *<mefClientReg>*

Data type ID	File name	Note
mefClientReg	SEC-mefClientReg-v2_0_0.xsd	available at [b-oneM2M.XML]

Table 9.4.1-2 – Universal/Common attributes of <mefClientReg> resource

Attribute name	Request optionality	
	Create	Update
@resourceName	NP	NP
resourceType	NP	NP
resourceID	NP	NP
parentID	NP	NP
creationTime	NP	NP
labels	O	O
expirationTime	M	M
creator	NP	NP

Table 9.4.1-3 – Resource specific attributes of <mefClientReg> resource

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
adminFQDN	M	NP	xs:anyURI	No default
assignedSymmKeyID	NP	NP	sec:credentialID	No default
sourceIDs	O	NP	List of m2m:ID	No default

Table 9.4.1-4 – Child resources of <mefClientReg> resource

Child resource type	Child resource name	Multiplicity	Ref. to resource type definition
<mefClientCmd>	"cmd"	1	Clause 8.7

9.4.2 <mefClientReg> resource specific procedures on CRUD operations

9.4.2.1 Create

This procedure is denoted *MEF Client Registration* in clause 8.8.2.3 of TS-0003 [ETSI TS 118 103]. The **To** parameter of the <mefClientReg> create request primitive includes the MEF-FQDN and the character "-" (dash) as a shorthand notation for the name of the <MEFBase> resource:

```
//{MEF-FQDN}/-/
```

Example: //mef123.mefprovider.org/-/

The MEF-FQDN represents a globally unique identifier of a MEF (i.e., MEF ID).

The **From** parameter of the <mefClientReg> create request primitive shall be left empty if the MEF client does not have a MEF client ID assigned yet. If the MEF client interfaces with the MEF on behalf of the node (clause 6.2.1), the Node-ID of the respective ADN, ASN, MN or IN shall serve as MEF client ID.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with following differences:

In step Orig-6.0: "Process Response primitive", if the Originator used a symmetric key to authenticate to the MEF, and the *<mefClientReg>* resource in the response contained an *assignedSymmKeyID* then the originator shall use the *assignedSymmKeyID* to identify this symmetric key when it is subsequently used in authenticating to the MEF.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with following differences:

The Receiver shall perform the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized to register with the administrating stakeholder (M2M SP or MTE) identified by *adminFQDN* attribute. This Recommendation does not specify how the Receiver makes this determination.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the ***Response Status Code*** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following steps in order as part of "Create the resource" (clause 7.3.3.5 of [ITU-T Y.4500.4]) during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) If the Originator authenticated using symmetric key with a key identifier which does not use the Receiver's FQDN, then
 - c. The Receiver shall assign a symmetric key identifier with the Receiver's FQDN and with relative part which is unique within the scope of symmetric key identifiers issued by the Receiver. The Receiver shall associate this symmetric key identifier with the symmetric key used for authenticating the Originator.
 - d. The Receiver shall set the *assignedSymmKeyID* attribute to be the Credential-ID formed from the assigned symmetric key identifier as specified in clause 10.4 of TS-0003 [ETSI TS 118 103].
- 3) If the Originator authenticated using a symmetric key with a key identifier which does not use the Receiver's FQDN, or if the Originator authenticated using a certificate, then the Receiver shall not include an *assignedSymmKeyID* attribute in the created resource.
- 4) The Receiver shall assign the *creator* attribute to an AE-ID or CSE-ID or Node-ID on instructions from the administrating stakeholder. This Recommendation does not specify any details of how the AE-ID or CSE-ID or Node-ID is determined.
- 5) The Receiver shall instantiate the *<mefClientCmd>* child resource.

9.4.2.2 Retrieve

This procedure is denoted *MEF Client Configuration Retrieval* in clause 8.8.2.4 of TS-0003 [ETSI TS 118 103]. This procedure is used to retrieve the *<mefClientReg>* resource.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, performing the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.4.2.3 Update

This procedure is denoted *MEF Client Configuration Update* in clause 8.3.5.2.5 of [ETSI TS 118 103]. This procedure is used to update attributes of the <mefClientReg> resource, such as e.g., labels, expiration time.

Originator:

The <mefClientReg> resource shall not be updated by a MEF client via API.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with the following differences:

The Receiver shall perform the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following step as part of "Update the resource" (clause 7.3.3.7 of [ITU-T Y.4500.4] during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) If the Originator was the Creator of the resource, then the Receiver shall perform steps 2 and 3 in clause 9.4.2.1.

9.4.2.4 Delete

This procedure is denoted *MEF Client De-Registration* in clause 8.8.2.6 of TS-0003 [ETSI TS 118 103]. This procedure enables the MEF client to delete its own <mefClientReg> resource on a MEF.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, performing the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the *Response Status Code* indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.5 Resource type <symmKeyReg>

9.5.1 Introduction

A <symmKeyReg> resource shall represent a symmetric key registered with a MAF or MEF and administrated by the identified administrating stakeholder. A <symmKeyReg> resource shall be a child resource of a <MAFBase> or a <MEFBase> resource.

Table 9.5.1-1 – Data type definition of <symmKeyReg>

Data type ID	File name	Note
symmKeyReg	SEC-symmKeyReg-v2_0_0.xsd	available at [b-oneM2M.XML]

Table 9.5.1-2 – Universal/Common attributes of <symmKeyReg> resource

Attribute name	Request optionality	
	Create	Update
@resourceName	NP	NP
resourceType	NP	NP
resourceID	NP	NP
parentID	NP	NP
creationTime	NP	NP
labels	O	O
creator	NP	NP
expirationTime	M	M

Table 9.5.1-3 – Resource specific attributes of <symmKeyReg> resource

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
adminFQDN	M	NP	xs:anyURI	No default
SUID	M	NP	m2m:suid	No default
targetIDs	O	O	m2m:listOfM2MID	No default
keyValue	O	NP	xs:base64Binary	No default

The *<symmKeyReg>* resource shall contain no child resources.

9.5.2 *<symmKeyReg>* resource specific procedures on CRUD operations

9.5.2.1 Create

This procedure is denoted *MAF Key Registration* in clause 8.8.2.7 of TS-0003 [ETSI TS 118 103] and *MEF Key Registration* in clause 8.8.2.7 of TS-0003. This procedure enables a source MAF client or a source MEF client to establish a symmetric key with the MAF or MEF, respectively, which can be retrieved for use by one or more target MAF clients or target MEF clients.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2 for Mmaf and in clauses 6.2.2 and 7.3 for Mmef, respectively, and with following differences:

In step Orig-1.0: "Compose of a Request primitive", the

- 1) Originator shall select to either use a key derived from the TLS handshake or use another key provided by the Originator.
 - a. If the Originator selects to use a key derived from the TLS handshake, then the Originator shall not include the *keyValue* attribute in the *<symmKeyReg>* resource of the request.
 - b. If the Originator selects to provide a key other than a key derived from the TLS handshake, the Originator shall include the value of this key in the *keyValue* attribute in the *<symmKeyReg>* resource of the request.

In step Orig-6.0: "Process Response primitive", the following steps shall be performed:

- 2) If the Originator selected to use a key derived from the TLS handshake (see difference to step Orig-1.0 above), then the Originator shall perform the following steps in order to generate the value for the *keyValue* attribute
 - a. The Originator shall apply the TLS export mechanism described in clause 10.3.1 of [ETSI TS 118 103] to generate a TLS-export-key. For MAF Key Registration the "TLS Key Export Details for M2M Secure Connection Key", for MEF Key Registration the "TLS Key Export Details for Enrolment Key" apply, respectively.
 - b. The Originator shall apply the usage-constrained key derivation algorithm in clause 10.3.7 of [ETSI TS 118 103] to derive the *keyValue* from TLS-export-key, *adminFQDN*, *SUID* and the *resourceName* assigned by the Receiver to the created resource.
- 3) The originator shall record the *resourceName* attribute of the created resource as the relative part of the key identifier for the symmetric key which is to be assigned to the value for the *keyValue* attribute.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and with following differences:

The Receiver shall perform the following steps in order in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall ensure that the following criteria are satisfied, with administrating stakeholder being the stakeholder matching the *adminFQDN* attribute of the *<symmKeyReg>* resource in the Create request:
 - a. The Originator is enrolled with the administrating stakeholder; that is, there is a non-expired *<mafClientReg>* resource whose *creator* attribute matches the Originator's

AE-ID or CSE-ID or Node-ID, and whose *adminFQDN* attribute identifies the administrating stakeholder.

- b. The Receiver determines that the administrating stakeholder allows the creation of the resource. This Recommendation does not specify how the Receiver makes this determination.
- 2) If these criteria are not met, then the Receiver shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - b. "Send the Response primitive".
- 3) Otherwise, then the Receiver shall allow the request.

The Receiver shall perform the following step as part of "Create the resource" (clause 7.3.3.5 of [ITU-T Y.4500.4]) during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 4) If the *keyValue* attribute is not present in the *<symmKeyReg>* resource in the request, then the Receiver shall perform the following steps in order to generate the value for the *keyValue* attribute:
 - a. The Receiver shall apply the TLS export mechanism described in clause 10.3.1 of [ETSI TS 118 103] to generate a TLS-export-key.
 - b. The Receiver shall apply the usage-constrained key derivation algorithm in clause 10.3.7 of [ETSI TS 118 103] to derive the value for the *keyValue* attribute from TLS-export-key, *adminFQDN*, *SUID* and the *resourceName* assigned by the Receiver to the created resource.

9.5.2.2 Retrieve

This procedure is denoted *MAF Key Retrieval* in clause 8.8.2.8 of TS-0003 [ETSI TS 118 103] and *MEF Key Retrieval* in clause 8.8.2.8 of TS-0003. It enables a target MAF client to retrieve the key value from a MAF corresponding to a RelativeKeyID available to the target MAF client.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2 for Mmaf and in clauses 6.2.2 and 7.3 for Mmef, respectively.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and with following differences:

The Receiver shall perform the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource or the Originator is identified in the *targetIDs*.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.5.2.3 Update

This procedure is denoted *MAF Key Registration Update* in clause 8.8.2.9 of TS-0003 [ETSI TS 118 103] and *MEF Key Registration Update* in clause 8.8.2.9 of TS-0003. It enables a source MAF client or source MEF client to update the metadata associated with a registered key.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2 for Mmaf and in clauses 6.2.2 and 7.3 for Mmef, respectively.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and performing the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.5.2.4 Delete

This procedure is denoted *MAF Key De-Registration* in clause 8.8.2.10 of TS-0003 [ETSI TS 118 103] and *MEF Key De-Registration* in clause 8.8.2.10 of TS-0003. It enables a source MAF client to request the MAF to stop distributing the registered key.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.1.2 and 7.2 for Mmaf and in clauses 6.2.2 and 7.3 for Mmef, respectively.

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2 and 7, and performing the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

9.6 Resource type <mefClientCmd>

9.6.1 Introduction

A <mefClientCmd> resource shall represent a command to be indicated to a MEF client by a MEF, and a status report on the attempted parsing and execution of that command to be indicated to the MEF by a MEF client. The retrieve procedure and update procedure are used for this purpose.

Table 9.6.1-1 – Data type definition of <mefClientCmd>

Data type ID	File name	Note
mefClientCmd	SEC-mefClientCmd-v2_0_0.xsd	available at [b-oneM2M.XML]

Table 9.6.1-2 – Universal/Common attributes of <mefClientCmd> resource

Attribute name	Request optionality
	Update
@resourceName	NP
resourceType	NP
resourceID	NP
parentID	NP
creationTime	NP
labels	O
expirationTime	NP

Table 9.6.1-3 – Resource specific attributes of <mefClientCmd> resource

Attribute name	Request optionality	Data type	Default value and constraints
	Update		
cmdID	M	m2m:requestID	No default
cmdDescription	NP	sec:cmdDescription	No default
cmdStatusCode	M	sec:cmdStatusCode	No default

The <mefClientCmd> resource shall contain no child resources.

9.6.2 <mefClientCmd> resource specific procedures on CRUD operations

9.6.2.1 Create

Originator:

The <mefClientCmd> resource shall not be created via API. It is instantiated by a MEF when the parent <mefClientReg> resource is created as described in clause 9.4.2.1.

Receiver:

The primitive specific operation on Recv-1.0 "Check the syntax of received message" defined in TS-0004 [ITU-T Y.4500.4] applies:

- 1) If the request is received, the Receiver CSE shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

9.6.2.2 Retrieve

This procedure is denoted *MEF Client Command Retrieval* in clause 8.3.9.2 of [ETSI TS 118 103]. This procedure is used to retrieve the <mefClientCmd> resource.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with following difference:

In step Orig-6.0: "Process Response primitive", the Originator shall extract the *cmdID*, *cmdDescription* and *cmdStatusCode* from the response and pass these to the MEF client command processing as specified in clause 8.3.9 in [ETSI TS 118 103].

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with following differences:

The Receiver shall perform the following in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the parent *<mefClientReg>* resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the ***Response Status Code*** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following step as part of "Create the resource" (clause 7.3.3.5 of [ITU-T Y.4500.4]) during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) If the Receiver has a pending MEF client command to be issued to the Originator, then the Receiver shall set the *cmdID*, *cmdDescription* and *cmdStatusCode* attributes as specified in clause 8.3.9 of [ETSI TS 118 103]. The values of these attributes should remain set to these values until the MEF client performs an Update on the resource (see clause 9.6.2.3). If the MEF client takes too long to perform an Update (for example, if the Response is not received by the Originator) then the MEF may choose to replace the attributes with a new MEF client command.

NOTE – The *cmdDescription* includes the *cmdClass* attribute which can be set to "NO_MORE_COMMANDS" by the MEF to indicate that there are no further commands to be issued.

9.6.2.3 Update

This procedure is denoted *MEF Client Command Update* in clause 8.3.9.3 of TS-0003 [ETSI TS 118 103]. This procedure is used by the MEF client to report on the status of an issued MEF client command, and for an MEF to issue another MEF client command.

Originator:

No change from the generic procedures in clause 7.2.2.1 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with following differences:

In step Orig-1.0: "Compose of a Request primitive", the Originator shall include the *cmdID* and *cmdStatusCode* attributes in the Content of the request, with attribute values assigned as described in clause 8.3.9.3 of [ETSI TS 118 103].

In step Orig-6.0: "Process Response primitive", the Originator shall extract the *cmdID*, *cmdDescription* and *cmdStatusCode* attributes from the response and pass these to the MEF client command processing specified in clause 8.3.9.3 in [ETSI TS 118 103].

Receiver:

Same as the generic procedures in clause 7.2.2.2 of [ITU-T Y.4500.4] with clarifications discussed in clauses 6.2.2 and 7.3, and with the following differences:

The Receiver shall perform the following step in the place of Recv-6.3: "Check authorization of the Originator":

- 1) The Receiver shall determine if the Originator is authorized by checking if the Originator is the creator of the parent *<mefClientReg>* resource.
 - a. If the Originator is not authorized, then the Receiver shall execute the following steps in order:
 - i. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "ACCESS_DENIED" error;
 - ii. "Send the Response primitive".
 - b. If the Originator is authorized, then the Receiver shall allow the request.

The Receiver shall perform the following steps in order as part of "Update the resource" (clause 7.3.3.7 of [ITU-T Y.4500.4]) during Step Recv-6.5: "Create/Update/Retrieve/Delete/Notify operation is performed":

- 2) The Receiver shall extract the *cmdID* and *cmdStatusCode* attributes and pass these to the MEF client command processing in the MEF described in clause 8.3.9.3 of [ETSI TS 118 103].
- 3) If the Receiver has a pending MEF client command to be issued to the Originator, then the Receiver shall set the *cmdID*, *cmdDescription* and *cmdStatusCode* attributes as specified in clause 8.3.9.3 of [ETSI TS 118 103]. The values of these attributes should remain set to these values until the MEF client performs a subsequent Update on the Resource. If the MEF client takes too long to perform an Update (for example, if the Response is not received by the Originator) then the MEF may choose to replace the attributes with a new MEF client command.

NOTE – The *cmdDescription* includes the *cmdClass* attribute which can be set to "NO_MORE_COMMANDS" to indicate that there are no further commands to be issued.

9.6.2.4 Delete

Originator:

The *<mefClientCmd>* resource shall not be deleted via API. It is deleted by a MEF when the parent *<mefClientReg>* resource is deleted.

Receiver:

The primitive specific operation on Recv-1.0 "Check the syntax of received message" defined in TS-0004 [ITU-T Y.4500.4] applies:

- 1) If the request is received, the Receiver CSE shall execute the following steps in order:
 - a. "Create an unsuccessful Response primitive" with the **Response Status Code** indicating "OPERATION_NOT_ALLOWED" error;
 - b. "Send the Response primitive".

10 Short names

10.1 Introduction

The short names are introduced in clause 8.2.1 of [ITU-T Y.4500.4]. The short names in [ITU-T Y.4500.4] shall apply in addition to the short names defined here.

10.2 Security-specific oneM2M resource attributes

In protocol bindings resource attributes names shall be translated into short names as shown in Table 10.2-1 below and in Table 8.2.3-1 of [ITU-T Y.4500.4].

Table 10.2-1 – Security-specific oneM2M attribute short names

Attribute name	Occurs in	Short name	Notes
<i>resourceType</i>	All	ty*	Defined in [ITU-T Y.4500.4]
<i>resourceID</i>	All	ri*	Defined in [ITU-T Y.4500.4]
<i>resourceName</i>	All	rn*	Defined in [ITU-T Y.4500.4]
<i>parentID</i>	mafClientReg, mefClientReg, symmKeyReg	pi*	Defined in [ITU-T Y.4500.4]
<i>.expirationTime</i>	All	et*	Defined in [ITU-T Y.4500.4]
<i>creationTime</i>	All	ct*	Defined in [ITU-T Y.4500.4]
<i>labels</i>	mafClientReg, mefClientReg, symmKeyReg	lbl*	Defined in [ITU-T Y.4500.4]
<i>creator</i>	mafClientReg, mefClientReg, symmKeyReg	cr*	Defined in [ITU-T Y.4500.4]
<i>adminFQDN</i>	mafClientReg, mefClientReg, symmKeyReg	adfq	
<i>SUID</i>	symmKeyReg	suid	
<i>assignedSymmKeyID</i>	mafClientReg, mefClientReg	aski	
<i>targetIDs</i>	symmKeyReg	tgis	
<i>keyValue</i>	symmKeyReg	kv	
<i>cmdID</i>	mefClientCmd	mcci	
<i>cmdDescription</i>	mefClientCmd	mccd	
<i>cmdStatusCode</i>	mefClientCmd	mccs	
NOTE – Marked short names have been already assigned for primitive parameters or resource attributes in [ITU-T Y.4500.4].			

10.3 Security-specific oneM2M resource types

In protocol bindings resource type names shall be translated into short names of Table 10.3-1.

Table 10.3-1 – Security-specific resource type short names

Attribute name	Short name
<i>MAFBase</i>	maf
<i>MEFBase</i>	mef
<i>mafClientReg</i>	macr
<i>mefClientReg</i>	mecr
<i>symmKeyReg</i>	mkr
<i>mefClientCmd</i>	mcc

10.4 Security-specific oneM2M complex data type members

In protocol bindings complex data types member names shall be translated into short names of Table 10.4-1.

NOTE – The member names of the security configuration parameters *mefClientRegCfg*, *mafClientRegCfg*, *mefKeyRegCfg* and *mafKeyRegCfg* are defined in clause 12.4 of TS-0003 [ETSI TS 118 103].

Table 10.4-1 – Security-specific oneM2M complex data type member short names

Member name	Occurs in	Short name	Notes
expirationTime	<i>mefClientRegCfg</i> , <i>mefKeyRegCfg</i> , <i>mafClientRegCfg</i> , <i>mafKeyRegCfg</i>	et*	Defined in [ITU-T Y.4500.4]
labels	<i>mefClientRegCfg</i> , <i>mefKeyRegCfg</i> , <i>mafClientRegCfg</i> , <i>mafKeyRegCfg</i>	lbl*	Defined in [ITU-T Y.4500.4]
fqdn	<i>mefClientRegCfg</i> , <i>mefKeyRegCfg</i> , <i>mafClientRegCfg</i> , <i>mafKeyRegCfg</i>	fq	
adminFQDN	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	adfq*	
httpPort	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	hpt	
coapPort	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	cpt	
websocketPort	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	wpt	
ppsk	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	pk	
rpsk	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	rk	
certAuth	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	cert	
credID	<i>mefClientRegCfg</i> , <i>mafClientRegCfg</i>	crdi	

Table 10.4-1 – Security-specific oneM2M complex data type member short names

Member name	Occurs in	Short name	Notes
caCerts	mefClientRegCfg, mafClientRegCfg	cact	
SUID	mefKeyRegCfg, mafClientRegCfg, authProfileMONodeArgs	suid*	
targetIDs	mefKeyRegCfg, mafClientRegCfg	tgis	
targetID	cmdDescription	tgi	
cmdClassID	cmdDescription	ccid	
cmdArgs	cmdDescription	cma	
certProvProtocolID	certProvCmdArgs	cppi	
URI	certProvCmdArgs	uri*	
certSubjectType	certProvCmdArgs	cst	
certSubjectID	certProvCmdArgs	csi	
deviceConfigURI	devCfgCmdArgs	dcu	
objectPath	MONodeCmdArgs	ajop*	
objectTypeID	MONodeCmdArgs	otyp	
objectTypeSpecificArgs	MONodeCmdArgs	otsa	
retryDuration	noMoreCmdArgs	rdu	
noMoreCmdArgs	cmdArgs	nmca	
certProvCmdArgs	cmdArgs	cpca	
devCfgCmdArgs	cmdArgs	dcca	
MONodeCmdArgs	cmdArgs	nnca	
NOTE – * marked short names have already been assigned to an attribute in Table 10.2-1.			

Annex A

oneM2M specification update and maintenance control procedure

(This annex forms an integral part of this Recommendation.)

The provisions of Annex L in [ITU-T Y.4500.1] regarding the oneM2M specification update and maintenance control procedure shall apply to this Recommendation.

Bibliography

- [b-ETSI TS 118 132] ETSI TS 118 132 V2.0.2 (2017), MAF and MEF Interface Specification (oneM2M TS-0032 version 2.0.2 Release 2A).
<https://www.etsi.org/deliver/etsi_ts/118100_118199/118132/02.00.02_60/ts_118132v020002p.pdf>
- [b-oneM2M.XML] oneM2M.XML, *oneM2M XML Schemas*.
<<http://www.onem2m.org/technical/xml-schemas>>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems