International Telecommunication Union

ITU-T Y.4500.22

(03/2018)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

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 – Field device configuration

Recommendation ITU-T Y.4500.22

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
Network control architectures and protocols	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	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
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.4500.22

oneM2M – Field device configuration

Summary

Recommendation ITU-T Y.4500.22 specifies the architectural options, resources and procedures needed to provision and maintain devices in the field domain in order to establish M2M service layer operation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4500.22	2018-03-01	20	11.1002/1000/13512

Keywords

Device management, device configuration, oneM2M.

* 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.

NOTE – This Recommendation departs slightly from the usual editorial style of ITU-T Recommendations to preserve existing cross-referencing from external documents.

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, 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/.

Table of Contents

Recommendation ITU-T Y.4500.22

oneM2M – Field device configuration

1 Scope

This Recommendation specifies the architectural options, resources and procedures needed to pre-provision and maintain devices in the field domain (e.g., ADN, ASN/MN) in order to establish M2M service layer operation between the device's application entity (AE) and/or common services entity (CSE) and a registrar and/or hosting CSE. The resources and procedures include information about the registrar CSE and/or hosting CSE needed by the AE or CSE to begin machine to machine (M2M) service layer operation.

This Recommendation contains oneM2M Release 2 specification – oneM2M Field Device Configuration V2.0.0 and is equivalent to standards of oneM2M partners including ARIB, ATIS, CCSA, ETSI [b-ETSI TS 118 122], TIA, TSDSI, TTA and 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.

The following referenced documents are necessary for the application of this 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*.

[ITU-T Y.4500.5] Recommendation ITU-T Y.4500.5 (2018), *oneM2M – Management enablement (OMA)*.

[ITU-T Y.4500.6] Recommendation ITU-T Y.4500.6 (2018), *oneM2M – Management enablement (BBF)*.

[ITU-T Y.4500.11] Recommendation ITU-T Y.4500.11 (2018), *oneM2M – Common terminology*.

[ETSI TS 118 103] ETSI TS 118 103 (2016), *oneM2M; Security solutions*.

[FIPS 180-4] NIST, FIPS 180-4 (2015), *Secure Hash Standard (SHS)*.

[IETF RFC 6920] IETF RFC 6920 (2013), *Naming Things with Hashes*.

3 Definitions

For the purposes of this Recommendation, the terms and definitions given in oneM2M TS-0011 [ITU-T Y.4500.11] apply.

3.1 Terms defined elsewhere

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

3.1.2 common services entity (CSE) [ITU-T Y.4500.11]: This represents an instantiation of a set of common service functions of the M2M environment. Such service functions are exposed to other entities through reference points.

3.1.3 (oneM2M) security principal [ITU-T Y.4500.11]: CSE or AE or node or M2M device which can be authenticated.

NOTE – When the security principal is a node or M2M device, then the node or M2M device is acting on behalf of the CSE and/or AE executing on the node or M2M device.

3.2 Terms defined in this Recommendation

3.2.1 application configuration: A procedure that configures an AE on an M2M node in the field domain for M2M service layer operation.

3.2.2 authentication profile: Security information that is needed to establish mutually-authenticated secure communications.

3.2.3 configuration AE: An AE whose role is to configure the M2M system, including the M2M node in the field domain.

3.2.4 configuration IPE: An IPE that provides the capability to configure the M2M node in the field domain by interworking the exchange of information between the M2M node and the M2M system.

3.2.5 service layer configuration: A procedure that configures a CSE on an M2M node in the field domain for M2M service layer operation.

4 Abbreviations and acronyms

For the purposes of this Recommendation, the abbreviations given in oneM2M TS-0011 [ITU-T Y.4500.11], oneM2M TS-0001 [ITU-T Y.4500.1] and the following apply:

AE	Application Entity
CSE	Common Services Entity
M2M	Machine to Machine
MAF	M2M Authentication Function
MEF	M2M Enrolment Function
MO	Managed Object (BBF specified management) or Management Object (OMA specified management)
NP	Not Present
RSPF	Remote Security Provisioning Framework
SAEF	Security Associated Establishment Framework
SUID	Security Usage Identifier
XML	extensible Markup Language
XSD	XML Schema Definition

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 to 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 Introduction

Devices in the field domain that host oneM2M AEs and CSEs require configuration that permits the AE or CSE to successfully operate in the M2M service layer. TS-0001 [ITU-T Y.4500.1] and TS-0003 [ETSI TS 118 103] specify much of what is needed to configure these devices in the field domain (i.e., ADN, ASN/MN). Specifically, TS-0001 [ITU-T Y.4500.1] provides:

- guidance on how a CSE is minimally provisioned in Annex E of the specification including how a user AE is established within a hosting CSE;
- specification of the general communication flows across the Mca and Mcc reference points in clause 8;
- specifications for how ASN/MN and ADN nodes and M2M applications are enrolled in the M2M system so that the node in the field domain can establish connectivity with a CSE. TS-0001 [ITU-T Y.4500.1] heavily relies on clause 6 and on the remote security provisioning framework (RSPF) of TS-0003 [ETSI TS 118 103] to specify how the security credentials of ASN/MN and ADN nodes and M2M applications are established in the M2M system for the enrolment of the node or M2M application in the M2M system;
- specifications for how the ADN and ASN/MN nodes in the field domain are managed using external management technologies in clause 6.2.4;
- guidance for how the ADN and ASN/MN nodes in the field domain can be configured without the support of external management technologies in clause 9.1.2.

The above clauses in TS-0001 [ITU-T Y.4500.1] assume that, for an M2M application to operate in the M2M system, all required information needed to establish M2M service operation between a

registrar or hosting CSE and the AE or CSE in the field domain is configured before registration of the AE or CSE to the M2M system.

This Recommendation specifies the additional architectural elements, resources and procedures necessary to configure ASN/MN and ADN nodes in the field domain in order for that device to establish M2M service layer operation. These architectural elements, resources and procedures are in addition to the architectural elements, resources and procedures already defined in TS-0001 [ITU-T Y.4500.1] and TS-0003 [ETSI TS 118 103].

7 Architectural aspects

7.1 Introduction

The information needed by the remote AE or CSE in the field domain to establish M2M service layer operation uses the architectural aspects of TS-0001 [ITU-T Y.4500.1] in order to convey the information elements to the ASN/MN or ADN nodes that host the AE or CSE prior to or during M2M service layer operation and to the AE or CSE during M2M service layer operation.

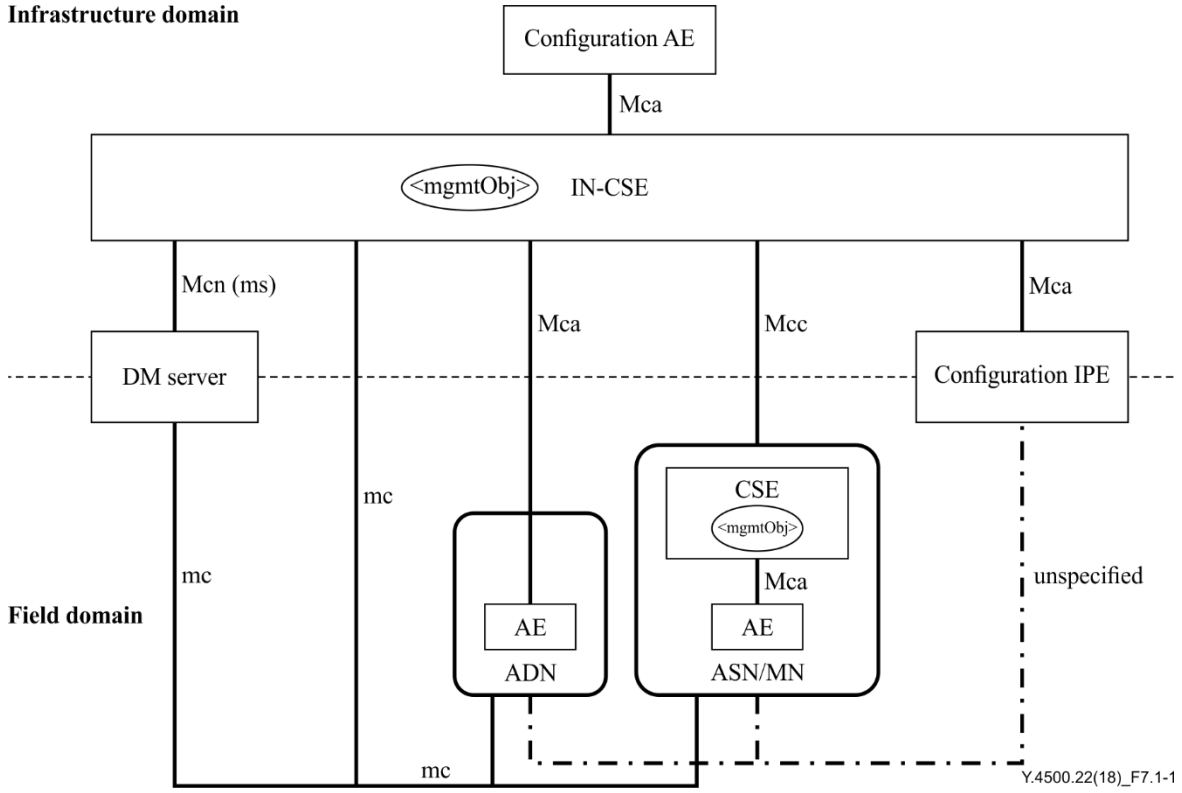

Figure 7.1-1 – Architectural aspects for configuration of ASN/MN and ADN nodes

Figure 7.1-1 depicts three (3) methods, in which ADN or ASN/MN nodes are configured using the following:

1) Device management technologies using the mc reference point defined in clause 6 of TS-0001 [ITU-T Y.4500.1]. Using this method, the information that is used to configure the ASN/MN or ADN is described as <*mgmtObj*> resource types that are hosted in the IN-CSE;

2) oneM2M Mcc and Mca reference point when M2M service layer operation has been established to the AE or CSE. Establishment of the M2M service layer operation includes actions such as setting up security associations and registration of the M2M entities as per TS-0003 [ETSI TS 118 103] and TS-0001 [ITU-T Y.4500.1];

3) oneM2M IPE technology where the IPE interworks the information exchange between the ADN and ASN/MN and the IN-CSE. This type of IPE is called a configuration IPE in order to depict the role and capabilities of the IPE related to this Recommendation.

NOTE – The reference point between the configuration IPE and the ADN and ASN/MN is unspecified in this Recommendation.

In addition, Figure 7.1-1 introduces an AE whose role is to configure the IN-CSE and nodes in the field domain with the information needed to establish M2M service layer operation. This type of AE is called a configuration AE in order to depict the role and capabilities of the AE related to this Recommendation.

The information that is used to configure the ASN/MN or ADN is described as <*mgmtObj*> resource types that are hosted in the IN-CSE.

7.2 Information needed for M2M service layer operation

7.2.1 Introduction

The configuration AE provisions the <*mgmtObj*> resource types in the IN-CSE and the IN-CSE then interacts with the DM Server, ADN or ASN/MN node or configuration IPE in order to configure the AE or CSE on the nodes.

7.2.2 Information elements required for M2M service layer operation

7.2.2.1 Introduction

The ASN/MN and ADN in the field domain should support the capability to be configured with the <*mgmtObj*> resource types defined in this Recommendation prior to initial registration with a registrar CSE (enrolment phase). When the AE or CSE has established M2M service layer operation with a registrar CSE (operational phase), the AE or CSE shall provide the capability to be configured with the <*mgmtObj*> resource types defined in this Recommendation.

7.2.2.2 M2M service layer registration information elements

The information elements used for CSE or AEs to register with a registrar CSE shall include the following information which depends on the M2M service provider:

- PoA information of registrar CSE;
- protocol binding to be used between the AE or CSE and the registrar CSE;
- CSE-ID of the CSE hosted on the ASN/MN;
- AE-ID of an AE hosted on an ASN/MN or ADN.

This set of information elements may be linked to a set of authentication profile information elements (see clause 7.2.2.4) providing the configuration for security association establishment with the registrar CSE.

7.2.2.3 Application configuration information elements

In order for an AE to operate, the AE may need to know the resource location within the hosting CSE to maintain its resource structure. In addition, for resources that are frequently provided by the AE to the hosting CSE, the AE may be configured with information that defines how frequently the AE collects or measures the data as well as the frequency at which that the data is transmitted to the hosting CSE.

When the hosting CSE is not the registrar CSE of the AE, then this set of information elements may be linked to a set of authentication profile information elements (see clause 7.2.2.4) providing the configuration for establishing end-to-end security of primitives (ESPrim) with the hosting CSE.

7.2.2.4 Authentication profile information elements

Authentication profile information elements may be required to establish mutually-authenticated secure communications.

The applicable security framework is identified via a security usage identifier (SUID). Where the security framework uses TLS or DTLS, a set of permitted TLS cipher suites may be provided. Then the applicable credentials are identified, with the allowed type of credentials dictated by the SUID.

A security framework can use a pre-provisioned or remotely provisioned symmetric key for establishing mutually-authenticated secure communications. In this cases, the identifier for the symmetric key is provided. If a symmetric key is remotely provisioned, then a remote security provisioning framework (RSPF) should be used as described in clause 8.3 of oneM2M TS-0003 [ETSI TS 118 103]. Alternatively, the value of the symmetric key may be configured as an information element of the authentication profile.

Certificate-based security frameworks may use one or more trust anchor certificates (also known as "root CA Certificates" or "root of trust certificates"). Information about trust anchor certificates is provided in the child trust anchor credential information elements (see clause 7.2.2.5) of the authentication profile.

M2M authentication function (MAF) based security frameworks use a MAF to facilitate establishing a symmetric key to be used for mutual authentication. The MAF client registration configuration credential information elements enable a MAF client to perform MAF procedures with the MAF.

7.2.2.5 My certificate file credential information elements

A security framework can use a certificate to authenticate the intended security principal in the managed entity to other security principals, as part of establishing mutually-authenticated secure communications. The certificate can be pre-provisioned or remotely provisioned, as discussed in oneM2M TS-0003 [ETSI TS 118 103]. If a certificate is remotely provisioned, then a remote security provisioning framework (RSPF) should be used as described in clause 8.3 of oneM2M TS-0003 [ETSI TS 118 103], or my certificate file credential information elements may be configured to the managed entity as described in this Recommendation.

My certificate file credential information elements include the media type of file containing the certificate, the file containing the certificate, and a list of security usage identifiers (SUID) for which the certificate may be used.

7.2.2.6 Trust anchor credential information elements

A security framework can use one or more trust anchor certificates (also known as "root Certificate Authority certificates" or "root of trust certificates"). These trust anchor certificates are used by a security principal on the managed entity for validating certificates of other security principals as part of establishing mutually-authenticated secure communications.

The trust anchor credential information elements include a hash-value-based identifier of the trust anchor certificate, along with a URL from which the trust anchor certificate can be retrieved. The managed entity can compute the hash value for the locally stored trust anchor certificates to determine if there is a match with the hash value in the information elements. If there is no match for the trust anchor certificates in local storage, then the managed entity retrieves the trust anchor certificate from the URL, and verifies that the hash value of the retrieved trust anchor certificate is a match for the hash value in the information elements.

7.2.2.7 MAF client registration configuration information elements

A security framework can use a MAF to establish symmetric key in a security principal in the managed entity and one or more other security principals, with the symmetric key used for establishing mutually-authenticated secure communications between the security principals. In this

case, the security principals are MAF clients. The security principal in the managed entity shall perform the MAF client registration procedure, described in clause 8.8.2.3 of oneM2M TS-0003 [ETSI TS 118 103] before the MAF facilitates establishing the symmetric keys.

The MAF client registration configuration information elements configure the security principal in the managed entity for the MAF client registration procedure, as described in clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103].

7.2.2.8 MEF client registration configuration information elements

A security framework can use a MEF to provision credentials to a security principal (an MEF client) in the managed entity for establishing mutually-authenticated secure communications between the security principal and another entity such as a security principal or MAF or MEF or device management server. The security principal in the managed entity shall perform the MEF client registration procedure described in clause 8.3.5.2.3 of oneM2M TS-0003 [ETSI TS 118 103] before the MEF provisions credentials.

The MEF client registration configuration information elements configure the security principal in the managed entity for the MEF client registration procedure, as described in clause 8.3.7.2 of oneM2M TS-0003 [ETSI TS 118 103].

8 Resource type and data format definitions

8.1 <mgmtObj> Resource type specializations

8.1.1 Introduction

The present clause specifies <*mgmtObj*> resource specializations used to configure AEs or CSEs on ADN or ASN/MN nodes in the field domain in order to establish M2M service layer operation.

Table 8.1.1-1 shows a summary of defined <*mgmtObj*> resource specializations in this Recommendation.

Table 8.1.1-1 – Summary of defined <*mgmtObj*> resources

mgmtDefinition	Intended use	Note
Registration	Service layer configuration information needed to register an AE or CSE with a registrar CSE.	This is M2M service provider dependent.
dataCollection	Application configuration information needed to establish a collection of data within the AE and transmit the data to the hosting CSE using <container> and <contentInstance> resource types.	This is M2M application dependent.
authenticationProfile	Security information needed to establish mutually-authenticated secure communications.	
myCertFileCred	Configuring a file containing a certificate and associated information.	
trustAnchorCred	Identifies a trust anchor certificate and provides a URL from which the certificate can be retrieved. The trust anchor certificate can be used to validate a certificate which the managed entity uses to authenticate another entity.	
MAFClientRegCfg	Instructions for performing the MAF client registration procedure with a MAF. Links to an authentication profile instance.	
MEFClientRegCfg	Instructions for performing the MEF client registration procedure with a MEF. Links to an authentication profile instance.	

8.1.2 Resource [registration]

This specialization of <*mgmtObj*> is used to convey the service layer configuration information needed to register an AE or CSE with a registrar CSE.

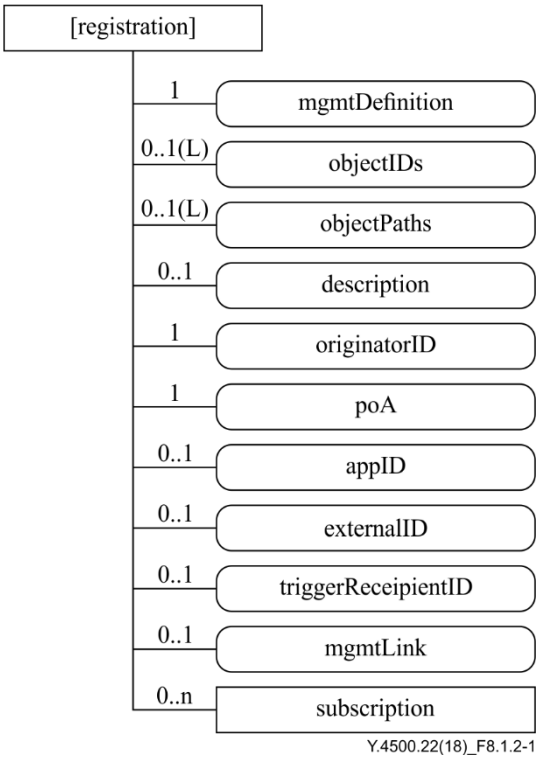

Figure 8.1.2-1 – Structure of [*registration*] resource

The [*registration*] resource shall contain the child resource specified in Table 8.1.2-1.

Table 8.1.2-1 – Child resources of *[registration]* resource

Child resources of *[registration]*	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*registration*] resource shall contain the attributes specified in Table 8.1.2-2.

Table 8.1.2-2 – Attributes of *[registration]* resource

Attributes of *[reboot]*	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "registration".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
originatorID	0..1	RW	CSE-ID of the CSE hosted on the ASN/MN or the AE-ID of an AE hosted on an ASN/MN or ADN node. If the setting is for a CSE, then this attribute shall be present.
poA	1	RW	The point of access URI of the registrar CSE. See note.
appID	0..1	RW	The App-ID of an AE. This attribute shall only be present when this resource is used for the registration of an AE.
externalID	0..1	RW	The M2M-Ext-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger recipient identifier of TS-0001 [ITU-T Y.4500.1].
triggerRecipientID	0..1	RW	The Trigger-Recipient-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger recipient identifier of TS-0001 [ITU-T Y.4500.1].
mgmtLink	0..1	RW	A link to a <mgmtObj> resource instance containing the information for establishing a security association with the registrar CSE.
NOTE – Protocol binding is determined from the protocol schema in this URI.			

8.1.3 Resource [dataCollection]

This specialization of <*mgmtObj*> is used to convey the application configuration information needed by an AE to collect data and then transmit the data to a hosting CSE.

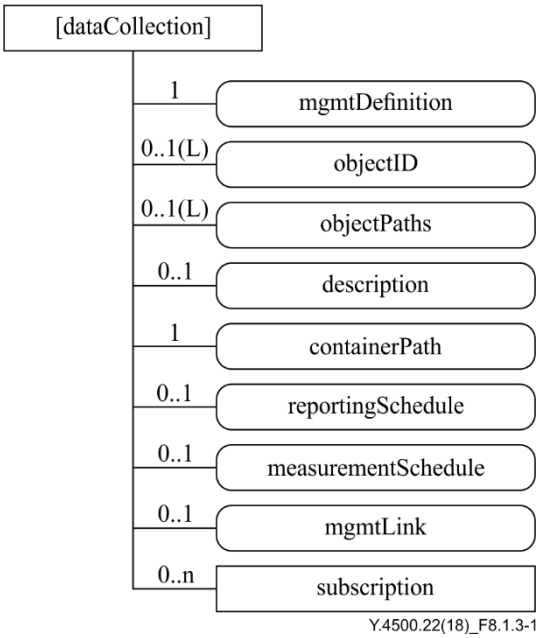

Figure 8.1.3-1 – Structure of [*dataCollection*] resource

The [*dataCollection*] resource shall contain the child resource specified in Table 8.1.3-1.

Table 8.1.3-1 – Child resources of *[dataCollection]* resource

Child resources of *[dataCollection]*	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*dataCollection*] resource shall contain the attributes specified in Table 8.1.3-2.

Table 8.1.3-2 – Attributes of *[dataCollection]* resource

Attributes of *[reboot]*	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].

Table 8.1.3-2 – Attributes of *[dataCollection]* resource

Attributes of *[reboot]*	Multiplicity	RW/ RO/ WO	Description
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "dataCollection".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
containerPath	1	RW	The URI of the <container> resource in the hosting CSE that stores the data transmitted by the device.
reportingSchedule	0..1	RW	The frequency interval, in seconds, used to transmit the data to the hosting CSE.
measurementSchedule	0..1	RW	The frequency interval, in seconds, that the device will use to collect or measure the data.
mgmtLink	0..1	RW	A link to a <mgmtObj> resource instance containing the information for establishing end-to-end security of primitives (ESPrim) between the AE and hosting CSE. ESPrim is specified in oneM2M TS-0003 [ETSI TS 118 103].
NOTE 1 – This Recommendation does not support configuration for end-to-end security of data (ESData) specified in oneM2M TS-0003 [ETSI TS 118 103]			

8.1.4 Resource [authenticationProfile]

The [*authenticationProfile*] specialization of the <*mgmtObj*> is used to convey the configuration information regarding establishing mutually-authenticated secure communications. The security principal using this configuration information can be a CSE or AE or the managed ADN/ASN/MN acting as security principal on behalf of AEs on the node.

An [*authenticationProfile*] instance identifies a security framework, TLS cipher suites, and credentials to be used. The applicable security framework is identified by the SUID attribute. The interpretation of SUID is specified in Table 8.1.4-3.

NOTE 1 – This Recommendation does not support using [authenticationProfile] for identifying ESData credentials.

The [*authenticationProfile*] resource does not include any credentials, but either identifies credentials which are stored locally on the managed entity or identifies an M2M authentication function (MAF) which is to be used to facilitate establishing symmetric keys. The intended security principal on the managed entity is the security principal which can use either all the credentials identified by the

[*authenticationProfile*] resource, or (in the case that a MAF is identified) all of the credentials required for mutual authentication with the MAF.

NOTE 2 – The other security principal can be any of the following: CSE; AE; a node terminating the security protocol on behalf of the AE on node; and an M2M authentication function (MAF).

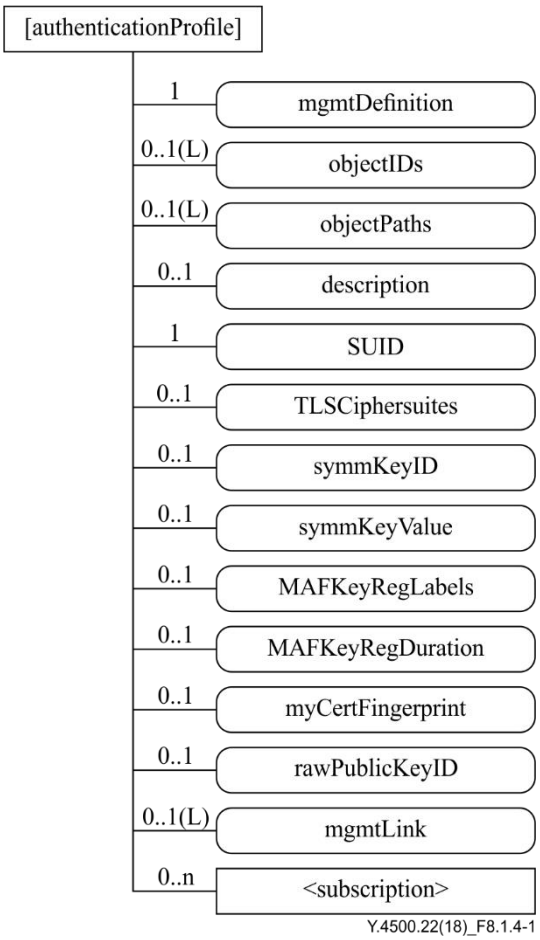

Figure 8.1.4-1 – Structure of [*authenticationProfile*]

The [*authenticationProfile*] resource shall contain the child resource specified in Table 8.1.4-1.

Table 8.1.4-1 – Child resources of *[authenticationProfile]* resource

Child resources of [authenticationProfile]	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*authenticationProfile*] resource shall contain the attributes specified in Table 8.1.4-2.

Table 8.1.4-2 – Attributes of *[authenticationProfile]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "authenticationProfile".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
SUID	1	WO	Describes how the authentication profile is to be used. Further details about interpretation of each SUID are specified in Table 8.1.4-3 of this Recommendation.
TLSCiphersuites	0..1	RW	If the security framework identified by SUID uses TLS, then this attribute provides a list of allowed TLS cipher suites.
symmKeyID	0..1	WO	Present when a symmetric key is to be used for mutual authentication. Identifier for a symmetric key already stored locally on the managed entity, or to be provisioned to the managed entity.
symmKeyValue	0..1	WO	Optionally present when a symmetric key is to be used for mutual authentication. Contains the value of the symmetric key to be used for mutual authentication.
MAFKeyRegLabels	0..1(L)	WO	Optionally present when a MAF is to be used to facilitate establishing a symmetric key for mutual authentication. Provides the content of the labels parameter in the MAF Key registration request; see Table 8.8.2.7-1, oneM2M TS-0003 [ETSI TS 118 103].

Table 8.1.4-2 – Attributes of *[authenticationProfile]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
MAFKeyRegDuration	0..1	WO	Present when a MAF is to be used to facilitate establishing one or more symmetric keys for mutual authentication. Provides the maximum duration for which an established symmetric key may be used.
mycertFingerprint	0..1	WO	Present when certificate-based authentication is to be used. Provides a hash value for identifying the certificate to be used by the intended security principal on the managed entity to authenticate itself to other security principals.
rawPubKeyID	0..1	WO	Present when certificate-based authentication is to be used and the other security principal will authenticate itself with a raw public key certificate.
mgmtLink	0..1(L)	RW	Present when a MAF is to be used to facilitate establishing one or more symmetric keys for mutual authentication or certificate-based authentication is to be used. In the former case, the list contains one reference to a [MAFClientRegCfg] resource. In the latter case, the list contains one or more references pointing to [trustAnchorCred] resources.

Table 8.1.4-3 – SUIDs which are currently supported in the [*authenticationProfile*] resource, along with reference to the authentication procedure in oneM2M TS-0003 [ETSI TS 118 103] and mapping to symmetric key

Value	Interpretation (see Note)	Authentication procedure in oneM2M TS-0003 [ETSI TS 118 103]	Derived symmetric key	DTLS/TLS Notes
10	A pre-provisioned symmetric key intended to be shared with a MEF	8.3.2.1	Kpm	See TLS-PSK profile in clause 10.2.2 of oneM2M TS-0003 [ETSI TS 118 103]
11	A pre-provisioned symmetric key intended to be shared with a MAF	8.8.2.2	Km	
12	A pre-provisioned symmetric key intended for use in a security associated establishment framework (SAEF)	8.2.2.1	Kpsa	
13	A pre-provisioned symmetric key intended for use in end-to-end security of primitives (ESPrim)	8.4.2	pairwiseESPrimKey	DTLS/TLS is not used

Table 8.1.4-3 – SUIDs which are currently supported in the [*authenticationProfile*] resource, along with reference to the authentication procedure in oneM2M TS-0003 [ETSI TS 118 103] and mapping to symmetric key

Value	Interpretation (see Note)	Authentication procedure in oneM2M TS-0003 [ETSI TS 118 103]	Derived symmetric key	DTLS/TLS Notes
21	A symmetric key, provisioned via a remote security provisioning framework (RSPF), and intended to be shared with a MAF	RSPF: 8.3.1.2 MAF: 8.8.2.2, 8.8.3.1	Km	See TLS-PSK profile in clause 10.2.2 of oneM2M TS-0003 [ETSI TS 118 103]
22	A symmetric key, provisioned via a RSPF, and intended for use in a SAEF	RSPF: 8.3.1.2 SAEF: 8.2.2.1, 9.1.1.1	Kpsa	
23	A symmetric key, provisioned via a RSPF, and intended for use in ESPrim	RSPF: 8.3.1.2 ESPRIM: 8.4.2	pairwiseESPrimKey	DTLS/TLS is not used
32	A MAF-distributed symmetric key intended for use in a SAEF	MAF: 8.8.2.7, 8.8.3.3 SAEF: 8.2.2.3, 9.1.1.1	Kpsa	See TLS-PSK profile in clause 10.2.2 of oneM2M TS-0003 [ETSI TS 118 103]
33	A MAF-distributed symmetric key intended for use in ESPrim	MAF: 8.8.2.7, 8.8.3.3 ESPRIM: 8.4.2	pairwiseESPrimKey	
40	A certificate intended to be shared with a MEF	8.3.2.2	NP	See certificate-based TLS profile in clause 10.2.3 of oneM2M TS-0003 [ETSI TS 118 103]
41	A certificate intended to be shared with a MAF	8.8.2.2	NP	
42	A certificate intended for use in a security associated establishment framework (SAEF)	8.2.2.2	NP	
43	A certificate intended for use in end-to-end security certificate-based key establishment (ESCertKE) to establish a pairwiseESPrimKey for end-to-end security of primitives (ESPrim)	ESCertKE: 8.7 ESPrim: 8.4.2	NP	For ESCertKE, see certificate-based TLS profile in clause 10.2.3 of oneM2M TS-0003 [ETSI TS 118 103]. For ESPrim, DTLS/TLS is not used
NOTE – The interpretation is copied from definition of m2m:suid in oneM2M TS-0004 [ITU-T Y.4500.4]. The oneM2M TS-0004 [ITU-T Y.4500.4] description takes precedence.				

The managed entity shall allow only TLS cipher suites identified in *TLSCiphersuites* in the TLS handshakes for a [*authenticationProfile*] instance. The final column of Table 8.1.4-3 provides references to clauses in oneM2M TS-0003 [ETSI TS 118 103] specifying the TLS profiles to be used with the SUID values. The *TLSCiphersuite* attribute shall be present only when the value of *SUID* identifies a security framework that uses TLS or DTLS.

If the value of *SUID* is 10, 11, 12, 21, 22 or 23, then the *symmKeyID* attribute shall be present. The *symmKeyID* provides the symmetric key identifier for a symmetric key which shall be retrieved from local storage on the managed entity for use in the TLS handshake. The symmetric key value may be configured in the *symmKeyValue*. Otherwise, the symmetric key, and associated symmetric key identifier, may be provisioned to the managed entity before or after the [*authenticationProfile*] is configured. Pre-provisioning or remote security provisioning frameworks (RSPFs), specified in oneM2M TS-0003 [ETSI TS 118 103], should be used whenever possible to establish symmetric keys. Special care is recommended to ensure the confidentiality and integrity of the credentials when using the *symmKeyValue* to configure symmetric keys.

If the value of *SUID* is 32 or 33, then the *MAFKeyRegDuration* attribute shall be present, the *MAFKeyRegLabels* attribute may be present, and a [*MAFClientRegCfg*] specialization shall be configured as a child of the [*authenticationProfile*] resource. These attributes provide the configuration controlling how the managed entity shall interact with a MAF to establish the symmetric key subsequently used for mutual authentication. The fqdn attribute of the [*MAFClientRegCfg*] specialization identifies the MAF.

- If the managed entity has not already performed MAF client registration procedure with the identified MAF, then the MAF shall perform MAF client registration procedure in clause 8.8.2.3 of oneM2M TS-0003 [ETSI TS 118 103] using the information in the [*MAFClientRegCfg*] specialization of the <*mgmtObj*> specified in clause 8.1.7.
- The managed entity shall perform the MAF Key registration procedure in clause 8.8.2.7 of oneM2M TS-0003 [ETSI TS 118 103] with the identified MAF, with the parameters of Table 8.8.2.7-1 of [ETSI TS 118 103] set as follows:
    - The *MAF-FQDN* parameter shall be set to the value of the *fqdn* attribute in the [*MAFClientRegCfg*] specialization which is the child of the [*authenticationProfile*] resource.
    - The *expirationTime* parameter shall be set to the time obtained by adding the *MAFKeyRegDuration* attribute to the present time.
    - If *MAFKeyRegLabels* attribute is present in the [*authenticationProfile*] resource, then the *labels* parameter shall be set to the value of the *MAFKeyRegLabels* attribute. Otherwise, the *labels* parameter shall not be present.
    - The *SUID* parameter shall be set to the *SUID* attribute.
    - The *targetIDs* parameter shall be set to the CSE-ID in the [*registration*] or [*dataCollection*] resource.

If the value of SUID is 40, 41, 42, or 43, then the *myCertFingerprint* attribute shall be present, and either the *rawPubKeyID* attribute shall be present or one or more [*trustAnchorCred*] specializations shall be configured as children of the [*authenticationProfile*] resource. The managed entity shall use the certificate matching *myCertFingerprint* to authenticate itself. The hash value portion of *myCertFingerprint* shall be computed over the X.509 ASN.1 DER encoded certificate.

- If the *rawPubKeyID* attribute is present, then the managed entity shall compare this value against the public key identifier (similar to a certificate fingerprint) generated from the raw public key certificate presented by the other entity, as specified in clause 10.1.2 of oneM2M TS-0003 [ETSI TS 118 103]. If the *rawPubKeyID* attribute is present, the managed entity shall ignore [*trustAnchorCred*] resource(s) configured as children of the [*authenticationProfile*].

- If the *rawPubKeyID* attribute is not present, then the managed entity shall use the one or more [*trustAnchorCred*] resource instance(s) configured as children of the [*authenticationProfile*] resource instance to retrieve certificate authority certificates to be used by the managed entity as a trust anchor certificate (also known as a "root CA certificate" or "trust root certificate") when validating the certificate chains provided by other entities. The managed entity shall allow the TLS handshake only if the other entity provides a certificate chaining to one of these trust anchors, using the process specified in clause 8.1.2.2 in oneM2M TS-0003 [ETSI TS 118 103].

[*authenticationProfile*] resources are expected to be protected by a secure environment on the managed entity, in order to preserve integrity of the attributes. Optimal protection is provided when the integrity protection of the management protocol message is verified in the secure environment.

8.1.5 Resource [myCertFileCred]

This <*mgmtObj*> specialization is used to configure a certificate or certificate chain which the managed entity knows the private key.

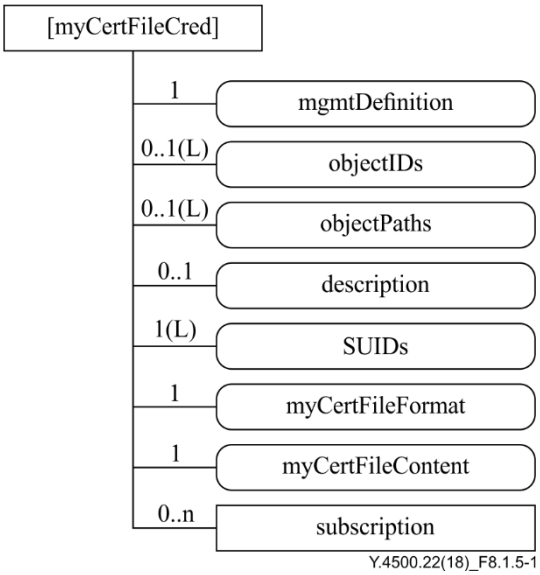

Figure 8.1.5-1 – Structure of [*myCertFileCred*] resource

The [*myCertFileCred*] resource shall contain the child resource specified in Table 8.1.5-1.

Table 8.1.5-1 – Child resources of *[myCertFileCred]* resource

Child resources of *[myCertFileCred]*	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*myCertFileCred*] resource shall contain the attributes specified in Table 8.1.5-2.

Table 8.1.5-2 – Attributes of *[myCertFileCred]* resource

Attributes of [myCertFileCred]	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "myCertFileCred".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
SUIDs	1 (L)	RW	Identifies the security framework(s) which may use this credential.
myCertFileFormat	1	WO	Media type of myCertFileContent attribute. Default is "application/pkcs7-mime".
myCertFileContent	1	WO	Certificate or certificate chain. Default media-type is "application/pkcs7-mime".

The *SUIDs* attribute lists the security usage identifiers (SUIDs) of the security frameworks which shall be allowed using this credential for establishing mutually-authenticated secure communication. Any SUID which is not in this list shall be prevented from using this credential for establishing mutually-authenticated secure communication. The SUID values allowed in this attribute are listed in Table 8.1.5-3. See Table 8.1.4-3 for references to the corresponding authentication procedure in oneM2M TS-0003 [ETSI TS 118 103] and DTLS/TLS notes.

Table 8.1.5-3 – SUID which are currently supported in the [*myCertFileCred*] resource

Value	Interpretation (see Note)
40	A certificate intended to be shared with a MEF
41	A certificate intended to be shared with a MAF
42	A certificate intended for use in a security associated establishment framework (SAEF)
43	A certificate intended for use in end-to-end security certificate-based key establishment (ESCertKE) to establish a pairwiseESPrimKey for end-to-end security of primitives (ESPrim)
NOTE – The interpretation is copied from definition of m2m:suid in oneM2M TS-0004 [ITU-T Y.4500.4]. The oneM2M TS-0004 [ITU-T Y.4500.4] description takes precedence.	

The certificate issuer should verify that the corresponding private key is known to the managed entity. This Recommendation does not provide a mechanism for such verification.

NOTE – In many scenarios, if the device management session takes place over a TLS connection in which the managed entity is authenticated using an existing certificate (e.g., a manufacturer certificate), then it would be acceptable to issue a certificate with SubjectPublicKeyInfo copied from the existing certificate.

managed entities shall support the default certificate-related media type.

If the *myCertFingerprint* attribute in an [*authenticationProfile*] resource matches the certificate in a [*myCertFileCred*] resource, then the authentication protocol based on that [*authenticationProfile*] shall provide the certificate or certificate chain in the *myCertFileContent*, and shall use the corresponding private key to authenticate the managed entity.

[*myCertFileCred*] instances are expected to be protected by a secure environment on the managed entity, in order to preserve confidentiality and integrity of the attributes. Optimal protection is provided when the decryption and integrity verification of the management protocol message occurs in the secure environment.

8.1.6 Resource [trustAnchorCred]

The [*trustAnchorCred*] <*mgmtObj*> specialization is read by AEs or CSEs on ADN or ASN/MN nodes in the field domain. A [*trustAnchorCred*] is configured as a child or children of [*authenticationProfile*] resources by means of a mgmtLink. A security principal acting on a [*authenticationProfile*] uses the information in the associated [*trustAnchorCred*] resources to identify a trust anchor certificate for validation of certificates.

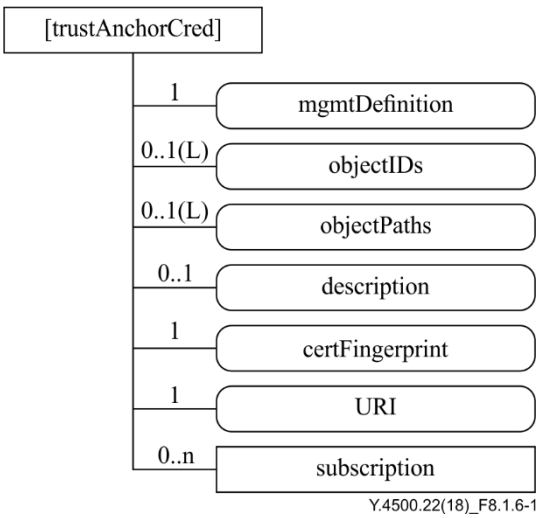

Figure 8.1.6-1 – Structure of [*trustAnchorCred*] resource

The [*trustAnchorCred*] resource shall contain the child resource specified in Table 8.1.6-1.

Table 8.1.6-1 – Child resources of *[trustAnchorCred]* resource

Child resources of [authenticationProfile]	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*trustAnchorCred*] resource shall contain the attributes specified in Table 8.1.6-2.

Table 8.1.6-2 – Attributes of *[trustAnchorCred]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "trustAnchorCred".

Table 8.1.6-2 – Attributes of *[trustAnchorCred]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
certFingerprint	1	WO	Provides a hash value for identifying a certificate authority certificate to be used for validating certificates presented by other entities
URI	1	RW	A URI from which the trust anchor certificate may be retrieved.

The *certFingerprint* attribute of the [*trustAnchorCred*] resource identifies a certificate authority certificate to be used by the managed entity as a trust anchor when validating the certificate chains provided by other entities. The hash value portion of the certFingerprint attribute shall be computed over the X.509 ASN.1 DER encoded certificate using the SHA-256 hash algorithm defined in FIPS 180-4 [FIPS 180-4]. The certFingerprint attribute shall be represented in the named Information (ni) URI format defined in IETF RFC 6920 [IETF RFC 6920], see Tables 7.2.6.1-2 and 7.3.2-1. Where the CA certificate identified in a [*trustAnchorCred*] resource is not already in local storage, then the managed entity shall retrieve the certificate using the *URI* attribute in the [*trustAnchorCred*] resources.

[*trustAnchorCred*] resources are expected to be protected by a secure environment on the managed entity, in order to preserve integrity of the attributes. Optimal protection is provided when the integrity protection of the management protocol message is verified in the secure environment.

8.1.7 Resource [MAFClientRegCfg]

This <*mgmtObj*> specialization is used to convey instructions regarding the MAF client registration procedure (clause 8.8.2.3 of oneM2M TS-0003 [ETSI TS 118 103]).

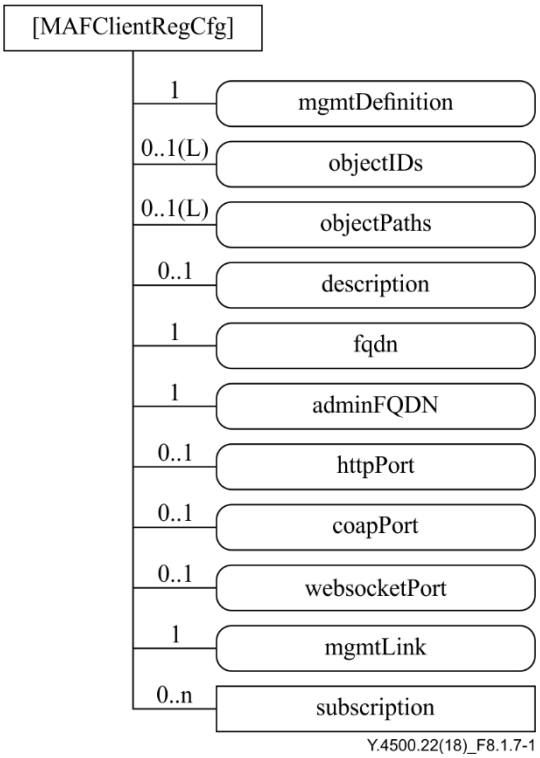

Figure 8.1.7-1 – Structure of [*MAFClientRegCfg*] resource

The [*MAFClientRegCfg*] resource shall contain the child resource specified in Table 8.1.7-1.

Table 8.1.7-1 – Child resources of *[MAFClientRegCfg]* resource

Child resources of [authenticationProfile]	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*MAFClientRegCfg*] resource shall contain the attributes specified in Table 8.1.7-2.

Table 8.1.7-2 – Attributes of *[MAFClientRegCfg]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].

Table 8.1.7-2 – Attributes of *[MAFClientRegCfg]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "MAFClientRegCfg".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
fqdn	1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103]
adminFQDN	1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103]
httpPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103]
coapPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103]
websocketPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [ETSI TS 118 103]
mgmtLink	1	RW	A link to a [authenticationProfile] resource containing the parameters for the MAF client to establish mutually-authenticated secure communications with the MAF.

The MAF client shall perform the MAF client registration procedure specified in clause 8.8.2.3 of oneM2M TS-0003 [ETSI TS 118 103], using the linked authentication profile for mutual authentication of the MAF client and MAF.

The MOs configured to the managed entity via [*MAFClientRegCfg*] resources are expected to be protected by a secure environment on the managed entity, in order to preserve integrity of the attributes. Optimal protection is provided when the integrity protection of the management protocol message is verified in the secure environment.

8.1.8 Resource [MEFClientRegCfg]

This <*mgmtObj*> specialization is used to convey instructions regarding the MEF client registration procedure (clause 8.3.5.2.3 of oneM2M TS-0003 [ETSI TS 118 103]).

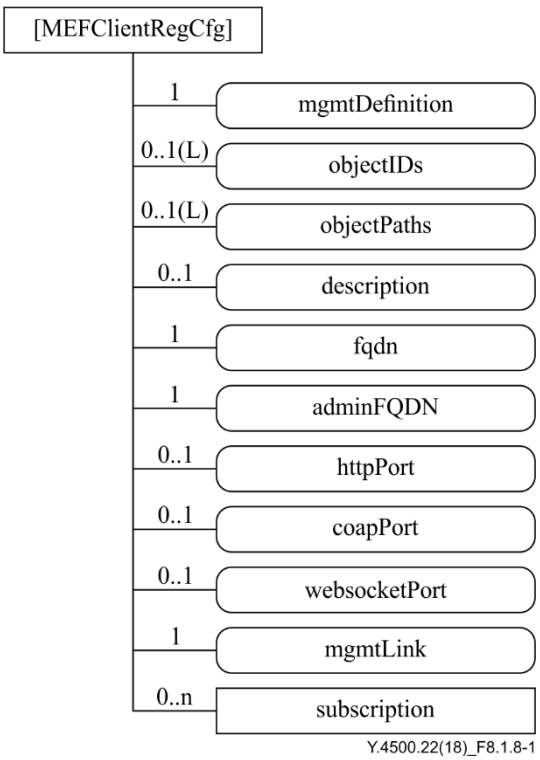

Figure 8.1.8-1 – Structure of [*MEFClientRegCfg*] resource

The [*MEFClientRegCfg*] resource shall contain the child resource specified in Table 8.1.8-1.

Table 8.1.8-1 – Child resources of *[MEFClientRegCfg]* resource

Child resources of [authenticationProfile]	Child resource type	Multiplicity	Description
[variable]	<*subscription*>	0..n	See clause 9.6.8 of oneM2M TS-0001 [ITU-T Y.4500.1]

The [*MEFClientRegCfg*] resource shall contain the attributes specified in Table 8.1.8-2.

Table 8.1.8-2 – Attributes of *[MEFClientRegCfg]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].

Table 8.1.8-2 – Attributes of *[MEFClientRegCfg]* resource

Attributes of [authenticationProfile]	Multiplicity	RW/ RO/ WO	Description
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [ITU-T Y.4500.1].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1]. This attribute shall have the fixed value "MEFClientRegCfg".
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [ITU-T Y.4500.1].
fqdn	1	WO	See clause 8.3.7 of oneM2M TS-0003 [ETSI TS 118 103]
adminFQDN	1	WO	See clause 8.3.7 of oneM2M TS-0003 [ETSI TS 118 103]
httpPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [ETSI TS 118 103]
coapPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [ETSI TS 118 103]
websocketPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [ETSI TS 118 103]
mgmtLink	1	RW	A link to a [authenticationProfile] resource containing the parameters for the MEF client to establish mutually-authenticated secure communications with the MEF.

The MEF client shall perform the MEF client registration procedure specified in clause 8.8.2.3 of oneM2M TS-0003 [ETSI TS 118 103], using the linked authentication profile for mutual authentication of the MEF client and MEF.

The MOs configured to the managed entity via [*MEFClientRegCfg*] resources are expected to be protected by a secure environment on the managed entity, in order to preserve integrity of the attributes. Optimal protection is provided when the integrity protection of the management protocol message is verified in the secure environment.

8.2 Resource-type specific procedures and definitions

8.2.1 Introduction

Clause 8.2 defines data types of the resource attributes specified in clause 7 and the resource-type specific procedures when performing operations on these resources types.

8.2.2 Resource [registration]

8.2.2.1 Introduction

This specialization of <*mgmtObj*> is used to convey the service layer configuration information needed to register an AE or CSE with a registrar CSE.

Table 8.2.2.1-1 – Data type definition of [*registration*]

Data type ID	File name	Note
registration	DCFG-registration-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.2.1-2 – Resource specific attributes of [*registration*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"registration"
objectIDs	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
originatorID	O	O	m2m:ID	CSE-ID of the CSE hosted on the ASN/MN or the AE-ID of an AE hosted on an ASN/MN or ADN node. If the setting is for a CSE, then this attribute shall be present.
poA	M	O	xs:anyURI	The point of access URI of the registrar CSE. Note; protocol binding is determined from the protocol schema in this URI.
appID	O	O	m2m:ID	The APP_ID of an AE. This attribute shall only be present when this resource is used for the registration of an AE.
externalID	O	O	m2m:externalID	The M2M-Ext-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger recipient identifier of TS-0001 [ITU-T Y.4500.1].

Table 8.2.2.1-2 – Resource specific attributes of [*registration*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
triggerRecipientID	O	O	m2m:triggerRecipientID	The Trigger-Recipient-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger recipient identifier of TS-0001 [ITU-T Y.4500.1].
mgmtLink	O	O	m2m:mgmtLinkRef	1 link to a [*authenticationProfile*] resource instance. See Note.
NOTE – The SUID in the linked [*authenticationProfile*] instance constrains the security framework to be used with the authentication profile. The security frameworks used with the [registration] resource are security association establishment frameworks (SAEFs). The entity composing a [*registration*] instance is expected to confirm that the linked authentication profile contains a SUID corresponding to an SAEF. The SAEF SUIDs are the values 12, 22, 32 or 42 as defined in oneM2M TS-0004 [ITU-T Y.4500.4].				

8.2.2.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004, '<*mgmtObj*> specific procedures' shall be used. There are no changes from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [ITU-T Y.4500.4] for operations on this resource.

8.2.3 Resource [dataCollection]

8.2.3.1 Introduction

Table 8.2.3.1-1 – Data type definition of [*dataCollection*]

Data type ID	File name	Note
dataCollection	DCFG-dataCollection-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.3.1-2 – Resource specific attributes of [*dataCollection*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"dataCollection"
objectIDs	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
containerPath	M	O	m2m:ID	The URI of the <container> resource in the hosting CSE that stores the data transmitted by the device.
reportingSchedule	O	O	m2m:scheduleEntries	The schedule, used to transmit the measured or collected data to the hosting CSE. If the entity that reports the data misses a reporting interval, the entity shall wait until the next interval to report the data.
measurementSchedule	O	O	m2m:scheduleEntries	The schedule, that the device will use to collect or measure the data. If the entity that measures or collects the data misses a measurement interval, the entity shall wait until the next interval to collect or measure the data.
mgmtLink	O	O	m2m:mgmtLinkRef	1 link to a [authenticationProfile]. See Note.
NOTE – The SUID in the linked [*authenticationProfile*] instance constrains the security framework to be used with the authentication profile. The security frameworks used with the [*dataCollection*] resource are end-to-end security of primitives (ESPrim). The entity composing a [*dataCollection*] instance is expected to confirm that the linked authentication profile contains a SUID corresponding to ESPrim. The SUIDs corresponding to ESPrim security frameworks are the values 13, 23, 33 or 43 as defined in oneM2M TS-0004 [ITU-T Y.4500.4].				

8.2.3.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.2.4 Resource [authenticationProfile]

8.2.4.1 Introduction

Table 8.2.4.1-1 – Data type definition of [*authenticationProfile*]

Data type ID	File name	Note
authenticationProfile	DCFG-authenticationProfile-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.4.1-2 – Resource specific attributes of [*authenticationProfile*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"authenticationProfile".
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
SUID	M	NP	m2m:suid	Allowed values are listed in Table 8.1.4-3.
TLSCiphersuites	M	O	dcfg:listOfTLSCiphersuite	
symmKeyID	O	NP	sec:credentialID	
symmKeyValue	O	NP	xs:base64Binary	The minimum key length is 256 bits.
MAFKeyRegLabels	O	NP	m2m:labels	
MAFKeyRegDuration	O	NP	xs:duration	
mycertFingerprint	O	NP	dcfg:niURI or dcfg:nihURI	
rawPubKeyID	O	NP	dcfg:niURI or dcfg:nihURI	
mgmtLink	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	

Table 8.2.4.1-3 – Child resources of [*authenticationProfile*] resource

Child resource type	Child resource name	Multiplicity	Ref. to in-resource type definition
<*subscription*>	*[variable]*	0..n	Clause 7.4.8 of oneM2M TS-0004 [ITU-T Y.4500.4]

8.2.4.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.2.5 Resource [myCertFileCred]

8.2.5.1 Introduction

Table 8.2.5.1-1 – Data type definition of [*myCertFileCred*]

Data type ID	File name	Note
myCertFileCred	DCFG-myCertFileCred-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.5.1-2 – Resource specific attributes of [*myCertFileCred*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"myCertFileCred"
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
SUIDs	M	O	xs:list of m2m:suid	Allowed values are listed in Table 8.1.5-3.
myCertFileFormat	M	NP	xs:anyURI	Media type of myCertFileContent attribute. Default is "application/pkcs7-mime".
myCertFileContent	M	NP	xs:string	Certificate or certificate chain. Default media-type is "application/pkcs7-mime".

Table 8.2.5.1-3 – Child resources of [*myCertFileCred*] resource

Child resource type	Child resource name	Multiplicity	Ref. to in-resource type definition
<*subscription*>	*[variable]*	0..n	Clause 7.4.8 of oneM2M TS-0004 [ITU-T Y.4500.4]

8.2.5.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.2.6 Resource [trustAnchorCred]

8.2.6.1 Introduction

Table 8.2.6.1-1 – Data type definition of [*trustAnchorCred*]

Data type ID	File name	Note
trustAnchorCred	DCFG-trustAnchorCred-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.6.1-2 – Resource specific attributes of [*trustAnchorCred*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"trustAnchorCred"
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	
certFingerprint	M	NP	dcfg:niURI	
URI	M	O	xs:anyURI	

Table 8.2.6.1-3 – Child resources of [*trustAnchorCred*] resource

Child resource type	Child resource name	Multiplicity	Ref. to in-resource type definition
<*subscription*>	*[variable]*	0..n	Clause 7.4.8 of oneM2M TS-0004 [ITU-T Y.4500.4]

8.2.6.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004

[ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.2.7 Resource [MAFClientRegCfg]

8.2.7.1 Introduction

Table 8.2.7.1-1 – Data type definition of [*MAFClientRegCfg*]

Data type ID	File name	Note
MAFClientRegCfg	DCFG-MAFClientRegCfg-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.7.1-2 – Resource specific attributes of [MAFClientRegCfg]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"MAFClientRegCfg"
fqdn	M	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
adminFQDN	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
httpPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	At least one of these attributes shall be present
coapPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
websocketPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
mgmtLink	M	O	m2m:mgmtLinkRef	1 link to a [*authenticationProfile*] resources instance
NOTE – For further details of these attributes, see clauses 8.8.3.2 and 12.4.2 of oneM2M TS-0003 [ETSI TS 118 103].				

Table 8.2.7.1-3 – Child resources of [MAFClientRegCfg] resource

Child resource type	Child resource name	Multiplicity	Ref. to in-resource type definition
<*subscription*>	*[variable]*	0..n	Clause 7.4.8 of oneM2M TS-0004 [ITU-T Y.4500.4]

8.2.7.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004

[ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.2.8 Resource [MEFClientRegCfg]

8.2.8.1 Introduction

Table 8.2.8.1-1 – Data type definition of [*MEFClientRegCfg*]

Data type ID	File name	Note
MEFClientRegCfg	DCFG-MEFClientRegCfg-v2_1_0.xsd	available at [b-oneM2M.XML]

Table 8.2.8.1-2 – Resource specific attributes of [*MEFClientRegCfg*]

Attribute name	Request optionality		Data type	Default value and constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15 of oneM2M TS-0004 [ITU-T Y.4500.4].	"MEFClientRegCfg"
fqdn	M	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
adminFQDN	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
httpPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	At least one of these attributes shall be present
coapPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
websocketPort	O	NP	See Table 12.4.2-1 of oneM2M TS-0003 [ETSI TS 118 103]	
mgmtLink	M	O	m2m:mgmtLinkRef	1 link to a [*authenticationProfile*] resources instance
NOTE – For further details of these attributes, see clauses 8.3.7.2 and 12.4.2 of oneM2M TS-0003 [ETSITS 118 103].				

Table 8.2.8.1-3 – Child resources of [*MEFClientRegCfg*] resource

Child resource type	Child resource name	Multiplicity	Ref. to in-resource type definition
<*subscription*>	*[variable]*	0..n	Clause 7.4.8 of oneM2M TS-0004 [ITU-T Y.4500.4]

8.2.8.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [ITU-T Y.4500.4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004

[ITU-T Y.4500.4] for operations on this resource. oneM2M TS-0005 [ITU-T Y.4500.5] and oneM2M TS-0006 [ITU-T Y.4500.6] provide the mapping of these resources into the technology specific protocol data model.

8.3 Data formats for device configuration

8.3.1 Introduction

This clause defines data formats of resource attributes and parameters used in this Recommendation.

Any data types of XML elements defined for use in this Recommendation shall be one of namespaces in Table 8.3.1-1.

Table 8.3.1-1 – Namespaces used in present document

Namespace	prefix	Namespace definition
oneM2M protocol CDT	m2m:	http://www.onem2m.org/xml/protocol
Device configuration	dcfg:	http://www.onem2m.org/xml/deviceConfig
oneM2M Security	sec:	http://www.onem2m.org/xml/securityProtocols

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

8.3.2 Simple oneM2M data types for device configuration

Table 8.3.2-1 describes simple data type definitions specific to security. The types in Table 8.3.2-1 are either:

- Atomic data types derived from XML schema data types by restrictions other than enumeration;
- list data types constructed from other XML schema or oneM2M-defined atomic data types.

Table 8.3.2-1 – oneM2M simple data types for device configuration

XSD type name	Used for	Examples	Description
dcfg:TLSCiphersuite	A TLS cipher suite identifier	C0A5	Four hexadecimal characters representing a TLS cipher suite identifier. The list of TLS cipher suites identifiers can be found at the IANA TLS Cipher Suite Registry http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml
dcfg:ListOfTLSCiphersuite	A list of TLS cipher suite identifiers		xs:list of elements of data type dcfg:TLSCiphersuite
dcfg:niURI	Identifying information with a hash value	ni:///sha-256;UyaQV... ni:///1;UyaQV... ("1" is a short identifier for sha-256)	An xs:anyURI conforming to the Named Information 'ni' URI scheme specified in IETF RFC 6920 [IETF RFC 6920], with no authority field.
dcfg:nihURI	Identifying information with a human speakable encoding of a hash value	nih:sha-256-32;53269057;b nih:sha-256-32;5326-9057;b nih:6;5326-9057 ("6" is a short identifier for sha-256-32)	An xs:anyURI conforming to the Human Speakable Named Information 'nih' URI scheme specified in IETF RFC 6920 [IETF RFC 6920], with no authority field. A check digit may be present.

9 Procedures

9.1 <mgmtObj> life cycle procedures

9.1.1 Introduction

The life cycle of the <*mgmtObj*> resource in the hosting CSE is established either through the:

- provisioning of the <*mgmtObj*> resource by the configuration AE;
- discovery of the <*mgmtObj*> resource by the hosting CSE using the methods described in clause 7.1 of this Recommendation.

9.1.2 Setting configuration information on <mgmtObj> resource

The configuration AE is able to configure the <*mgmtObj*> resources used for device configuration by either creating the <*mgmtObj*> resource or updating existing <*mgmtObj*> resources for the targeted AE or CSE. Likewise, the configuration AE can delete the <*mgmtObj*> resource as part of a decommissioning process.

In some scenarios the <*mgmtObj*> resource may already exist due to pre-provisioning or a previous discovery action by the IN-CSE's interaction with the configuration IPE, DM server or ASN/MN or ADN node. As such the configuration AE needs to first discover if the <*mgmtObj*> resource exists in the hosting CSE. As <*mgmtObj*> resources are represented under the <node> resource of the ASN/MN or ADN node, the discovery operation's scope can use the <node> resource within the discovery criteria. Based on the results of the discovery the configuration AE will either create or update the <*mgmtObj*> resource. Figure 9.1.2-1 depicts this flow.

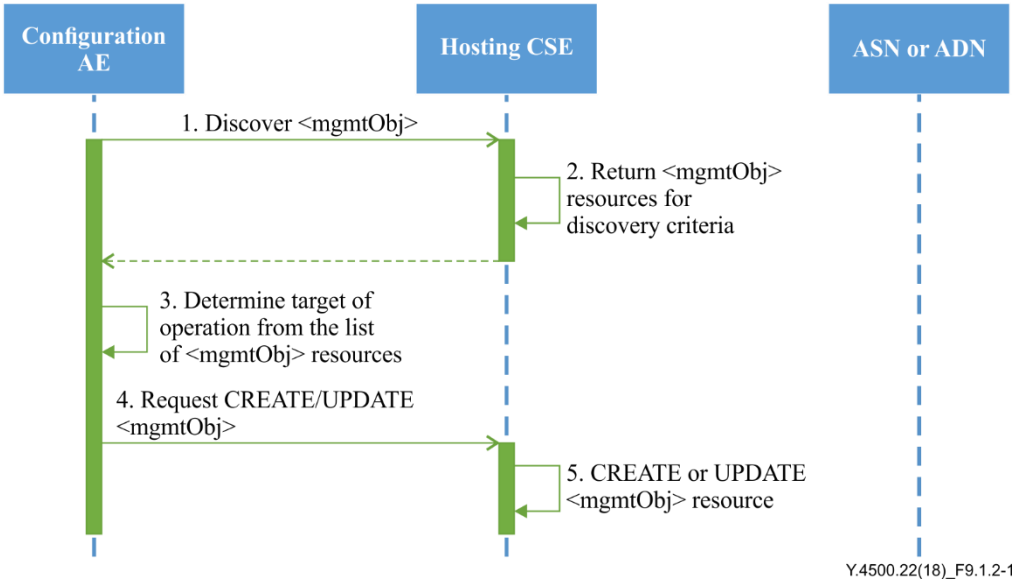

Figure 9.1.2-1 – Configuring attributes of a <*mgmtObj*> resource

Likewise, the configuration AE may use the same approach to discover when deleting the <*mgmtObj*> resource as part of a decommissioning process or retrieval of the <*mgmtObj*> resource.

NOTE – In order for the IN-CSE to forward the request onto the DM server, the <*mgmtObj*> resource is required to be configured with the path to the resource in the context of the technology specific protocol (e.g., LWM2M URI, OMA-DM path, BBF TR-069 path). The fully qualified domain name can also be used if the IN-CSE does not know the address of the DM server.

9.1.3 Management of <mgmtObj> resource on ASN/MN/ADN nodes

9.1.3.1 Introduction

Management of the <*mgmtObj*> object resources on ASN/MN or ADN nodes may be managed using one of the architectural methods described in clause 7.1 of this Recommendation.

9.1.3.2 Management using device management technologies

Clause 10.2.8 '<*mgmtObj*> Resource procedures' of TS-0001 [ITU-T Y.4500.1] describes the procedures for M2M nodes to represent their technology specific data as oneM2M resources within the IN-CSE.

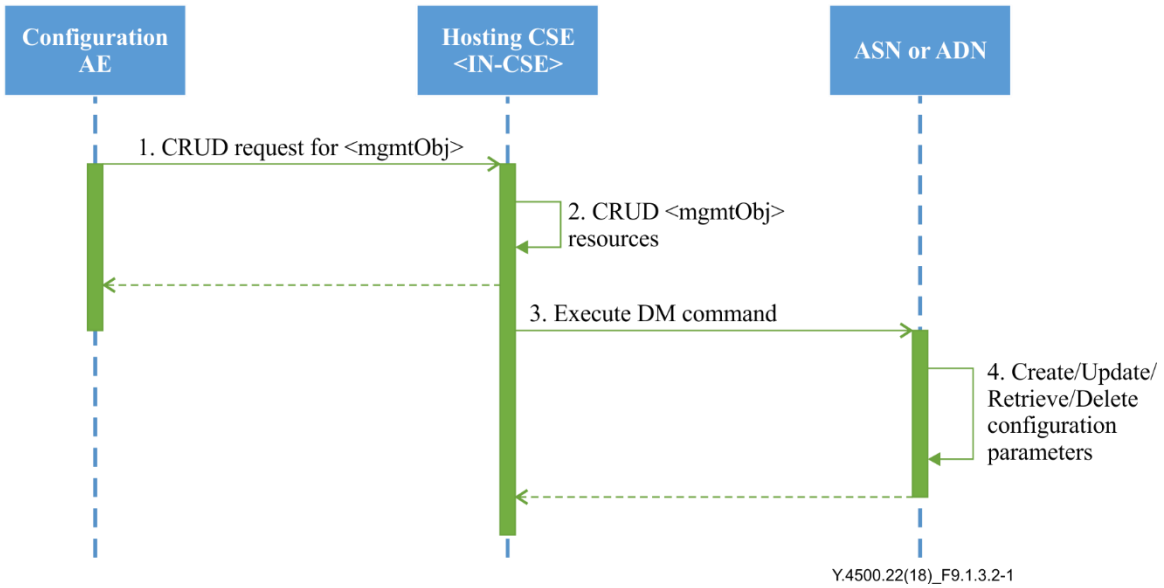

Figure 9.1.3.2-1 – Management using device management technologies

1) The configuration AE issues a request for <*mgmtObj*> resource for an ASN/MN/ADN node that is managed using device management technologies.
2) The IN- CSE processes the request issued by configuration AE.
3) The IN-CSE executes the device management command which is mapped from operation on <*mgmtObj*> resource to external management technologies.
4) The ASN/MN/ADN then creates, updates, deletes or retrieve the configuration parameters on the node, and returns the result of device management command.

9.1.3.3 Management using the Mcc reference point

Once M2M service layer operation is established between the AE or CSE and the registrar/hosting CSE, <*mgmtObj*> resources may be managed using the Mcc reference point by the AE or CSE subscribing to receive changes to the <*mgmtObj*> resource using the subscription procedures defined in clause 10.2.11 of oneM2M TS-0001 [ITU-T Y.4500.1]. Establishment of the M2M service layer operations includes actions such as establishing the appropriate security associations and registration of the CSEs and AEs.

While not mentioned in clause 7.1 of this Recommendation, <*mgmtObj*> specializations may be announced depending on the <*mgmtObj*> specialization type.

The following <*mgmtObj*> specializations specified in this document are announceable (i.e., announceable variants of this resource type are defined in the XSD of the respective <*mgmtObj*> specialization):

[*registration*], [*dataCollection*]

The following <*mgmtObj*> specializations specified in this document are not announceable (i.e., announceable variants of this resource type are not defined in the XSD of the respective <*mgmtObj*> specialization):

[*authenticationProfile*], [*myCertFileCred*], [*trustAnchorCred*], [*MAFClientRegCfg*], [*MEFClientRegCfg*]

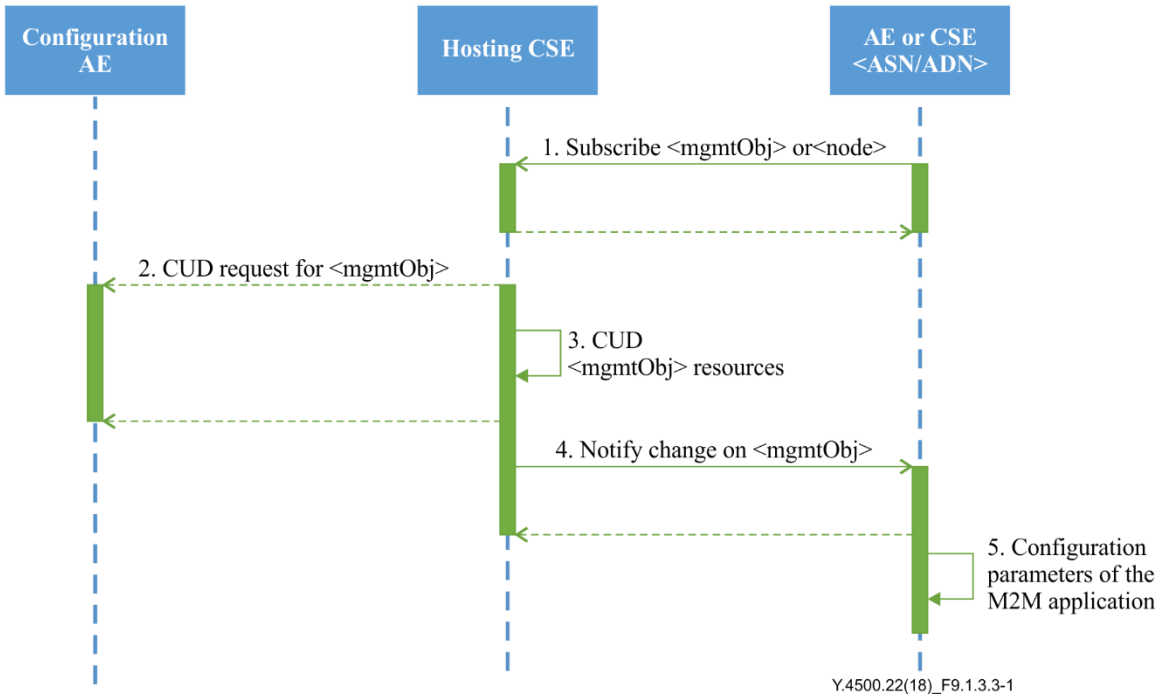

Figure 9.1.3.3-1 – Management using the Mcc reference point

1) Once M2M service layer operation is established, the AE or CSE on the ASN/MN/ADN node subscribes to the <*mgmtObj*> resource which is associated with the specific M2M application functionality creating <subscription> resource.
2) When the configurator AE creates, updates or delete the <*mgmtObj*> resource, the configuration AE issues a request on the <*mgmtObj*> resource.
3) The hosting CSE for the <*mgmtObj*> resource performs the operation on the resource as the receiver.
4) The hosting CSE notifies the subscribed AE or CSE as the subscribed event message.
5) The AE or CSE configures the M2M application on the ASN/MN or ADN node.

9.1.3.4 Management using the oneM2M IPE technology

When ASN/MN or ADN nodes are configured using a configuration IPE, the ASN/MN/ADN may periodically request the configuration IPE to configure the ASN/MN/ADN node. The method that the ASN/MN/ADN uses to periodically request to be configured is unspecified in this Recommendation. Once the configuration IPE receives the request from the ASN/MN/ADN node, the configuration IPE shall send a retrieve request to the hosting CSE to obtain the applicable specialization of <*mgmtObj*> resources for the ASN/MN/ADN node. How the configuration IPE maintains the mapping between the ASN/MN/ADN and the associated <*node*> and <*mgmtObj*> resources is unspecified in this Recommendation.

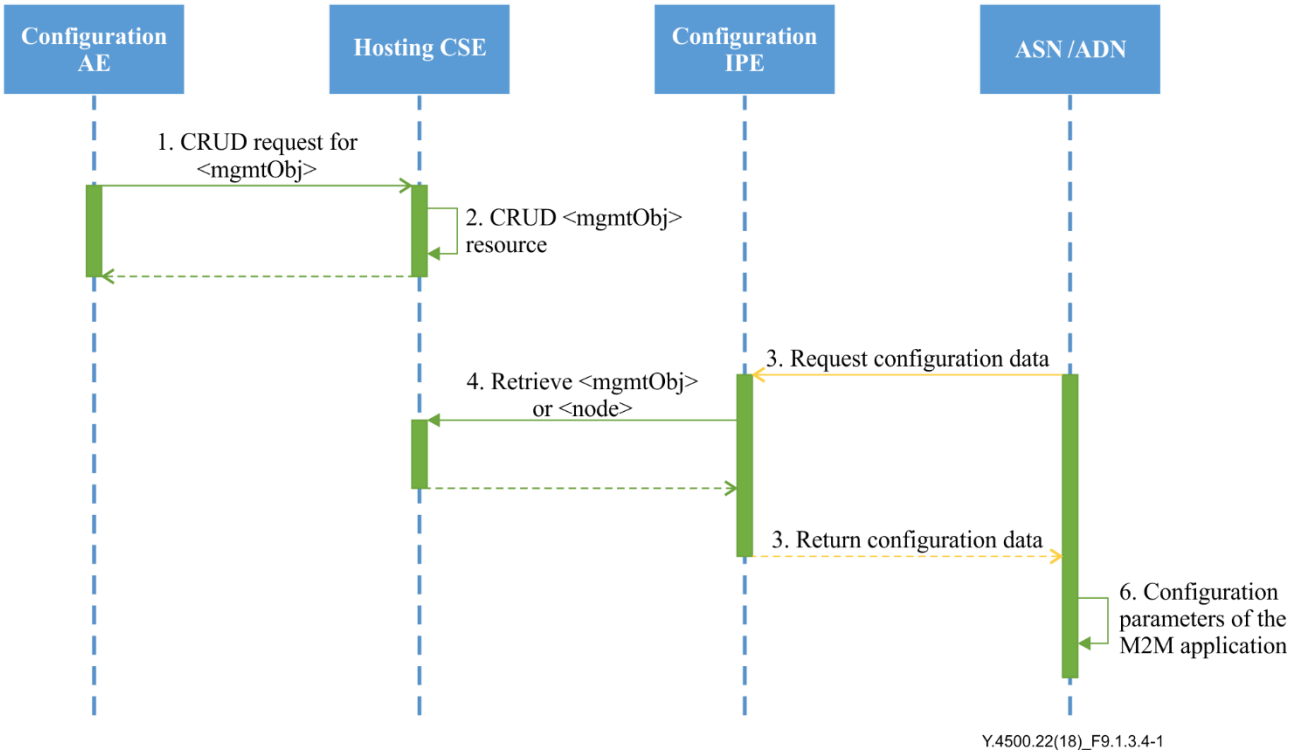

Figure 9.1.3.4-1 – Management using oneM2M IPE technology

1) The configuration AE issues a CRUD request to <mgmtObj> resource which is associated with the functionality of targeted field device.
2) The hosting CSE processes the CRUD request.
3) When the ASN/MN/ADN determines it needs to be configured, the ASN/MN/ADN issues a request to the configuration IPE.
4) The configuration IPE determines the <mgmtObj> resource to refer as the source of configuration parameter for the targeted field device, and issues an operation on the <mgmtObj> or <node> resource.
5) When the RETRIEVE request is successfully performed, the configuration IPE transforms the <mgmtObj> resource into a form understandable by ASN/MN/ADN node.
6) The ASN/MN/ADN configures setting parameters for the M2M application.

NOTE – One possible method of exchanging information between the configuration IPE and the ASN/MN/ADN is to simply serialize the <*mgmtObj*> resource using the MIME content types defined in clause 6.7 of TS-0004 [ITU-T Y.4500.4] 'oneM2M specific MIME media types'.

9.2 Obtaining authentication credential procedure

When an ASN/MN or ADN node is required to be authenticated, a mgmtLink 'authProfile' referring to the <*mgmtObj*> resource specialization for maintaining the authentication profiles shall be provided.

The authentication profile contains following information:

- choice of TLS options;
- mgmtLinkRef(s) to the <*mgmtObj*> which provides information required to obtain the credential(s).

When an ASN/MN or ADN node is establishing the appropriate security associations, the <*mgmtObj*> specialization for authentication profile shall be used to identify the security related settings.

The actual credential shall be obtained using the information on the <*mgmtObj*> specializations (authentication credential configuration) which is referred by mgmtLinkRef(s) from the authentication profile.

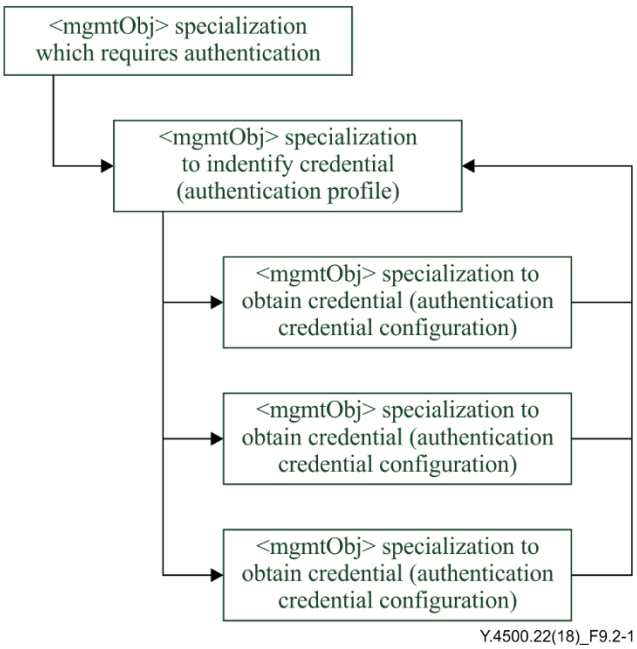

Figure 9.2-1 – Relationship between 'Authentication Profile' and 'Authentication Credential Configuration(s)'

9.3 AE and CSE registration procedure

When an ASN/MN or ADN node receives the information in the [*registration*] resource, the AE or CSE performs the registration procedure for that type of resource. If the resource is for CSE, then the CSE registration procedure which is defined in clause 10.1.1.2.1 of oneM2M TS-0001 [ITU-T Y.4500.1] is used. If the resource is for AE, the application entity registration procedure defined in clause 10.1.1.2.2 of oneM2M TS-0001 [ITU-T Y.4500.1] is used.

Required parameter for registration procedures are retrieved as attribute value of [registration] resource.

Table 9.3-1 – Required [registration] resource parameters for registration

attribute of [*registration*]	**parameter in TS-0001 [ITU-T Y.4500.1] / TS-0004 [ITU-T Y.4500.4]**
originatorID	From primitive parameter
PoA	CSE-PoA (Point of Access)
resourcePath	To primitive parameter

9.4 Enabling data collection by [dataCollection] resource

When an AE needs to measure or collect data to be later reported to a hosting CSE , report measured data to a CSE, the ASN/MN/ADN may be instructed when to measure/collect the data and then when to report the measured/collected data along with where to place the data within the hosting CSE.

Once the AE is configured with the [*dataCollection*] resource the AE performs the CREATE operation for new <*contentInstance*> resource as the child resource of <container> resource which is specified as the 'containerPath' attribute of [*dataCollection*] resource to report the measured/collected

data. The frequency of collection/measurement and reporting are accordingly specified as 'reportingSchedule' and 'measurementSchedule' attributes of the [*dataCollection*] resource.

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] as regard to oneM2M Specification update and maintenance control procedure shall apply to this Recommendation.

Bibliography

[b-ETSI TS 118 122] ETSI TS 118 122 V2.0.0 (2017), *oneM2M Field Device Configuration*.

[b-oneM2M.XML] oneM2M XML Schemas
http://www.onem2m.org/technical/developers-corner/tools/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

Printed in Switzerland
Geneva, 2018