ONEM2M
TECHNICAL SPECIFICATION

Document Number	TS-0022-V2_3_1
Document Name:	Field Device Configuration
Date:	2018-03-12
Abstract:	Field Device Configuration TS

Template Version: January 2017 (Do not modify)

About oneM2M

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

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

Contents

1 Scope

The present document 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 AE and/or CSE and a Registrar and/Hosting CSE. The resources and procedures includes information about the Registrar CSE and/or Hosting CSE needed by the AE or CSE to begin M2M Service Layer operation.

2 References

2.1 Normative references

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

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

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

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

[3] oneM2M TS-0003: "Security Solutions".

[4] oneM2M TS-0004: "Service Layer Core Protocol".

[5] oneM2M TS-0005: "Management Enablement (OMA)".

[6] oneM2M TS-0006: "Management Enablement (BBF)".

[7] IETF RFC 6920: "Naming Things with Hashes".

[8] IANA Transport Layer Security (TLS) Parameters.

NOTE: Available at http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml.

[9] oneM2M TS-0032: "MAF and MEF Interface Specification".

[10] FIPS PUB 180-4: "Secure Hash Standard (SHS)".

NOTE: Available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

2.2 Informative references

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

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

[i.1] oneM2M Drafting Rules .

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

3 Definitions and abbreviations

3.1 Definition

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

Application Configuration: procedure that configures an AE on an M2M Node in the Field Domain for M2M Service Layer operation.

Configuration AE: an AE whose role is to configure the M2M System, including the M2M Node in the Field Domain.

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.

Service Layer Configuration: procedure that configures a CSE on an M2M Node in the Field Domain for M2M Service Layer operation.

authentication profile: security information needed to establish mutually-authenticated secure communications

credential object: end-point of a security protocol

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in oneM2M TS-0011 [1], oneM2M TS-0001 [2] and the following apply:

NP	Not Present
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 Conventions

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

5 Introduction

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. oneM2M TS-0001 [2] and oneM2M TS-0003 [3] specifies much of what is needed to configure these devices in the Field Domain (i.e., ADN, ASN/MN). Specifically, oneM2M TS-0001 [2] 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 such that the node in the Field domain can establish connectivity with a CSE. TS-0001 heavily relies on Clause 6 and on the Remote Security Provisioning Framework (RSPF) of oneM2M TS-0003 [3] 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 8.1.2.

The above clauses in oneM2M TS-0001 [2] assume that, for a 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.

The present document 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 oneM2M TS-0001 [2] and oneM2M TS-0003 [3].

6 Architectural Aspects

6.1 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 oneM2M TS-0001 [2] 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.

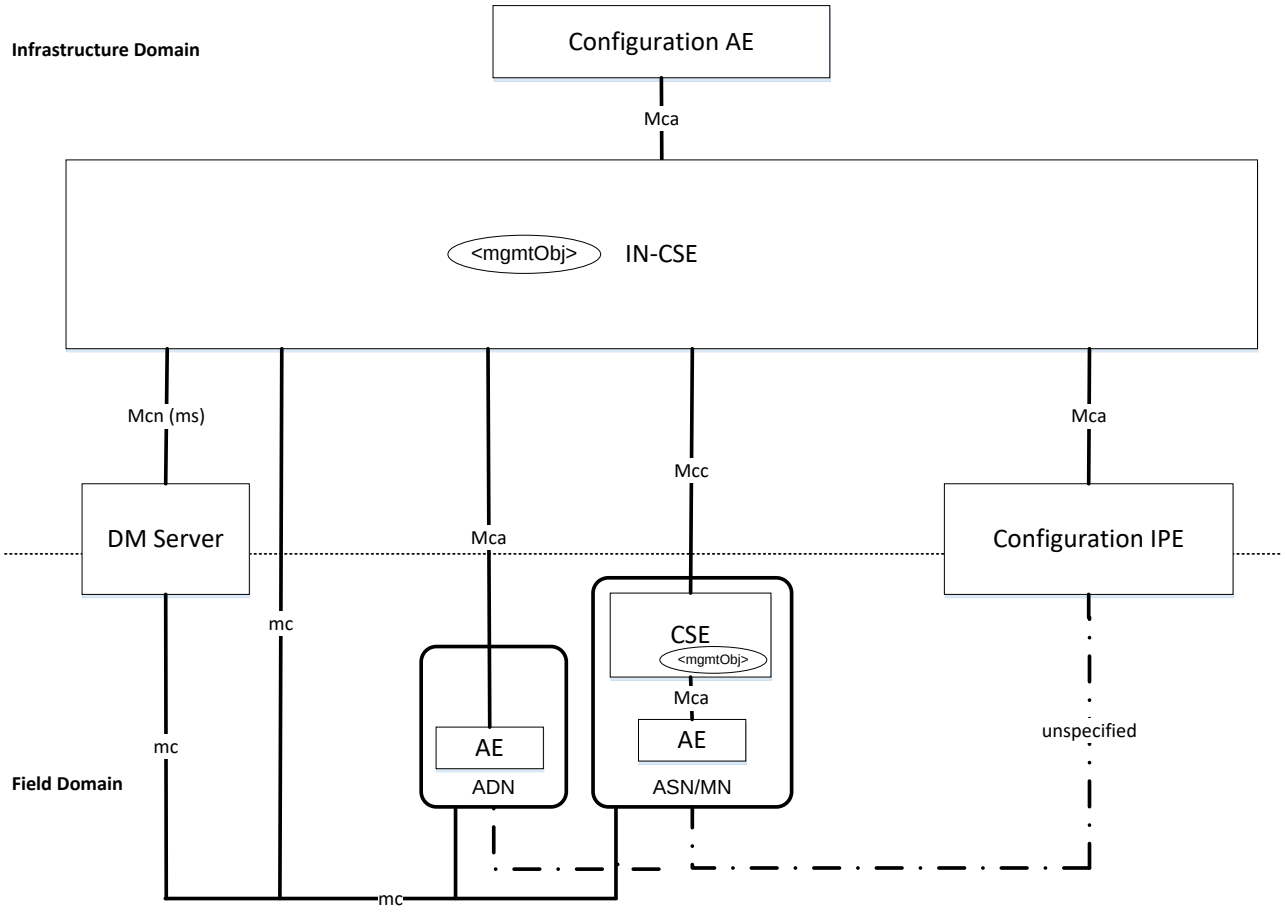

Figure 6.1-1: Architectural Aspects for Configuration of ASN/MN and ADN Nodes

Figure 6.1-1 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 oneM2M TS-0001 [2]. 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 oneM2M TS-0003 [3] and oneM2M TS-0001 [2].

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 the present document.

NOTE: The reference point between the Configuration IPE and the ADN and ASN/MN is unspecified in the present document.

In addition, Figure 6.1-1 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 the present document.

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.

6.2 Information needed for M2M Service Layer operation

6.2.1 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.

6.2.2 Information elements required for M2M Service Layer operation

6.2.2.1 Introduction

The ASN/MN and ADN in the Field Domain should support the capability to be configured with the <*mgmtObj*> resource types defined in the present document 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 the present document.

6.2.2.2 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 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 6.2.2.4) providing the configuration for security association establishment with the Registrar CSE.

6.2.2.3 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 6.2.2.4) providing the configuration for establishing End-to-End Security of Primitives (ESPrim) with the Hosting CSE.

6.2.2.4 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 both 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 [3]. 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 6.2.2.5) of the authentication profile.

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.

6.2.2.5 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 [3]. 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 [3], or my certificate file credential information elements may be configured to the Managed Entity as described in the present specification.

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.

6.2.2.6 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.

6.2.2.7 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 [3] 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 [3].

6.2.2.8 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 [3] 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 [3].

7 Resource type and data format definitions

7.1 <mgmtObj> Resource type specializations

7.1.1 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 7.1.1-1 shows a summary of <*mgmtObj*> resource specializations defined in the present document.

Table 7.1.1-1: Summary of defined <*mgmtObj*> resources

mgmtObj	mgmtDefinition	Intended use	Note
Registration	1020	Service Layer Configuration information needed to register an AE or CSE with a Registrar CSE.	This is M2M Service Provider dependent.
dataCollection	1021	Application Configuration information needed to establish 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	1022	Security information needed to establish mutually-authenticated secure communications	
myCertFileCred	1023	Configuring a file containing a certificate and associated information	
trustAnchorCred	1024	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.	

mgmtObj	mgmtDefinition	Intended use	Note
MAFClientRegCfg	1025	Instructions for performing the MAF Client Registration procedure with a MAF. Links to an Authentication Profile instance.	
MEFClientRegCfg	1026	Instructions for performing the MEF Client Registration procedure with a MEF. Links to an Authentication Profile instance.	

7.1.2 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.

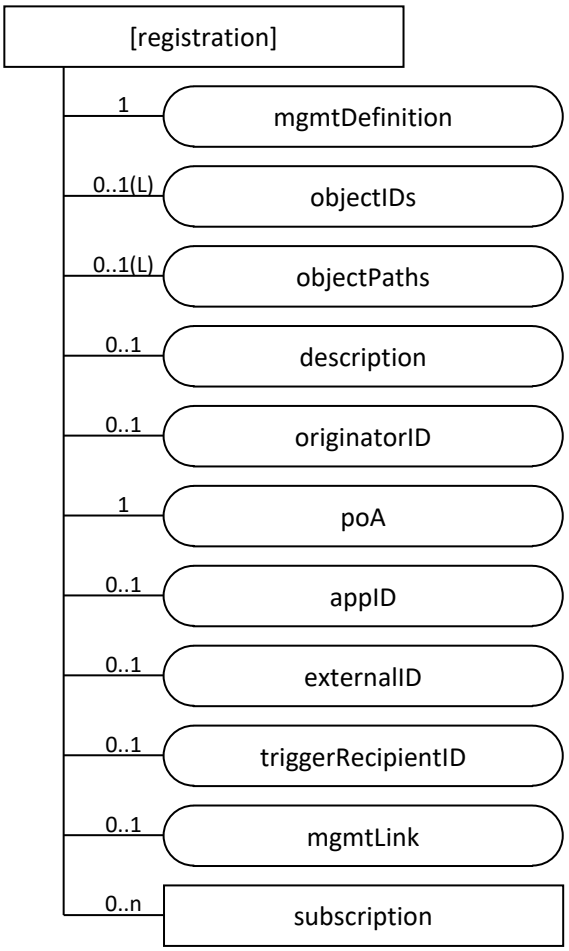

Figure 7.1.2-1: Structure of [*registration*] resource

The [*registration*] resource shall contain the child resource specified in table 7.1.2-1.

Table 7.1.2-1: 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 [2]

The [*registration*] resource shall contain the attributes specified in table 7.1.2-2.

Table 7.1.2-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1020 ("registration").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
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 oneM2M TS-0001 [2].
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 oneM2M TS-0001 [2].
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.			

7.1.3 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.

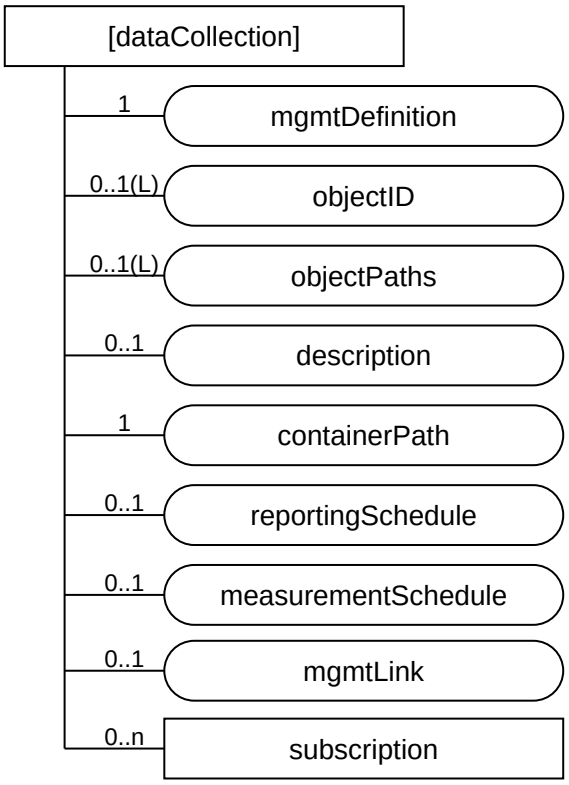

Figure 7.1.3-1: Structure of [*dataCollection*] resource

The [*dataCollection*] resource shall contain the child resource specified in table 7.1.3-1.

Table 7.1.3-1: 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 [2]

The [*dataCollection*] resource shall contain the attributes specified in table 7.1.3-2.

Table 7.1.3-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1021 ("dataCollection").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
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 AE and hosting CSE. ESPrim is specified in oneM2M TS-0003 [3].
NOTE: The present specification does not support configuration for End-to-End Security of Data (ESData) specified in oneM2M TS-0003 [3].			

7.1.4 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 7.1.4-3.

NOTE 1: The present document 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 AE on Node; and an M2M Authentication Function (MAF).

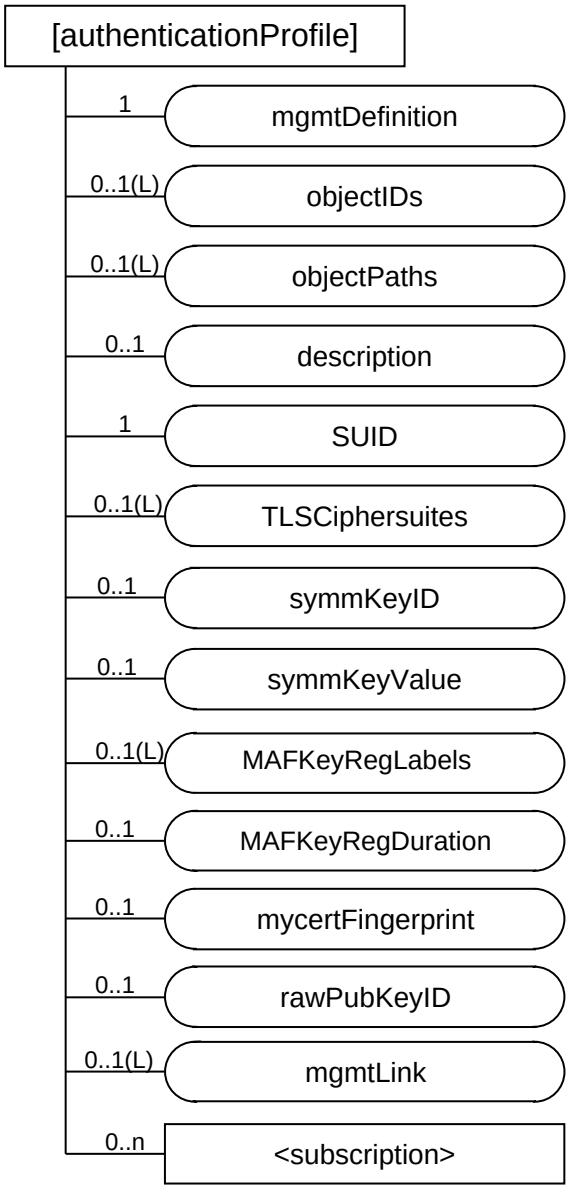

Figure 7.1.4-1: Structure of [*authenticationProfile*]

The [*authenticationProfile*] resource shall contain the child resource specified in table 7.1.4-1.

Table 7.1.4-1: 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 [2]

The [*authenticationProfile*] resource shall contain the attributes specified in table 7.1.4-2.

Table 7.1.4-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1022 ("authenticationProfile").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
SUID	1	WO	Describes how the authentication profile is to be used. Further details about interpretation of each SUID are specified in Table 7.1.4-3 of the present document.
TLSCiphersuites	0..1(L)	RW	If the security framework identified by *SUID* uses TLS, then this attributes 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 [3].
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 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 7.1.4-3: SUID which are currently supported in the [*authenticationProfile*] resource, along with reference to the authentication procedure in oneM2M TS-0003 [3] and mapping to symmetric key

Value	Interpretation (see note)	Authentication Procedure in oneM2M TS-0003 [3]	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 [3]
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
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 [3]
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 [3]
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 [3]
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 [3]. For ESPrim, DTLS/TLS is not used
NOTE: The interpretation is copied from definition of m2m:suid in oneM2M TS-0004 [4]. The oneM2M TS-0004 [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 7.1.4-3 provides references to clauses in oneM2M TS-0003 [3] 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 [3], 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 [3] using the information in the [*MAFClientRegCfg*] specialization of the <*mgmtObj*> specified in clause 7.1.7.

- The Managed Entity shall perform the MAF Key Registration Procedure in clause 8.8.2.7 of oneM2M TS-0003 [3] with the identified MAF, with the parameters of table 8.8.2.7-1 of oneM2M TS-0003 [3] 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 [3]. 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 [3].

[*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.

7.1.5 Resource [myCertFileCred]

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

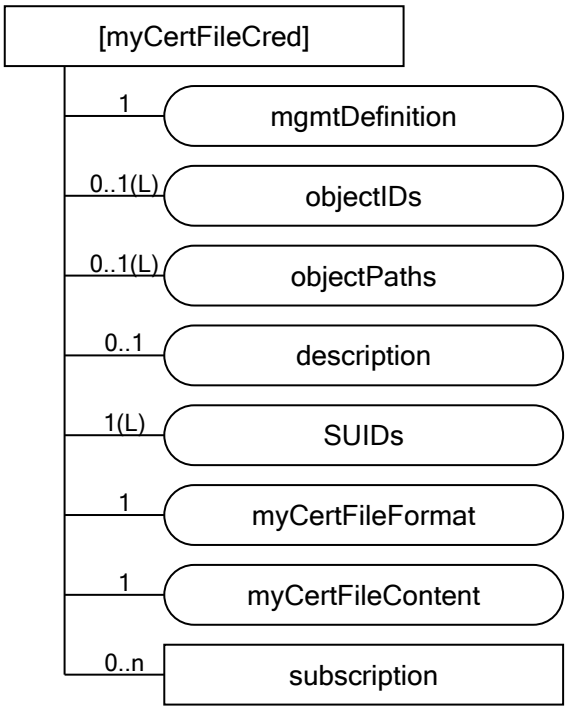

Figure 7.1.5-1: Structure of [*myCertFileCred*] resource

The [*myCertFileCred*] resource shall contain the child resource specified in table 7.1.5-1.

Table 7.1.5-1: 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 [2]

The [*myCertFileCred*] resource shall contain the attributes specified in table 7.1.5-2.

Table 7.1.5-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1023 ("myCertFileCred").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
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 7.1.5-3. See table 7.1.4-3 for references to the corresponding authentication procedure in oneM2M TS-0003 [3] and DTLS/TLS notes.

Table 7.1.5-3: 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 the definition of m2m:suid in oneM2M TS-0004 [4]. The oneM2M TS-0004 [4] description takes precedence.

The Certificate issuer should verify that the corresponding private key is known to the Managed Entity. The present specification 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.

7.1.6 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.

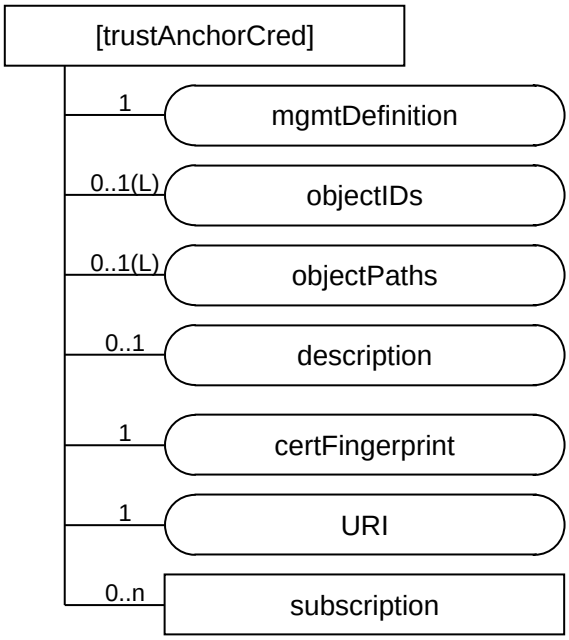

Figure 7.1.6-1: Structure of [*trustAnchorCred*] resource

The [*trustAnchorCred*] resource shall contain the child resource specified in table 7.1.6-1.

Table 7.1.6-1: 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 [2]

The [*trustAnchorCred*] resource shall contain the attributes specified in table 7.1.6-2.

Table 7.1.6-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
Labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1024 ("trustAnchorCred").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
Description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
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 1010[10101010101010101010]. The certFingerprint attribute shall be represented in the named information (ni) URI format defined in IETF RFC 6920 [7], 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.

7.1.7 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 [3]).

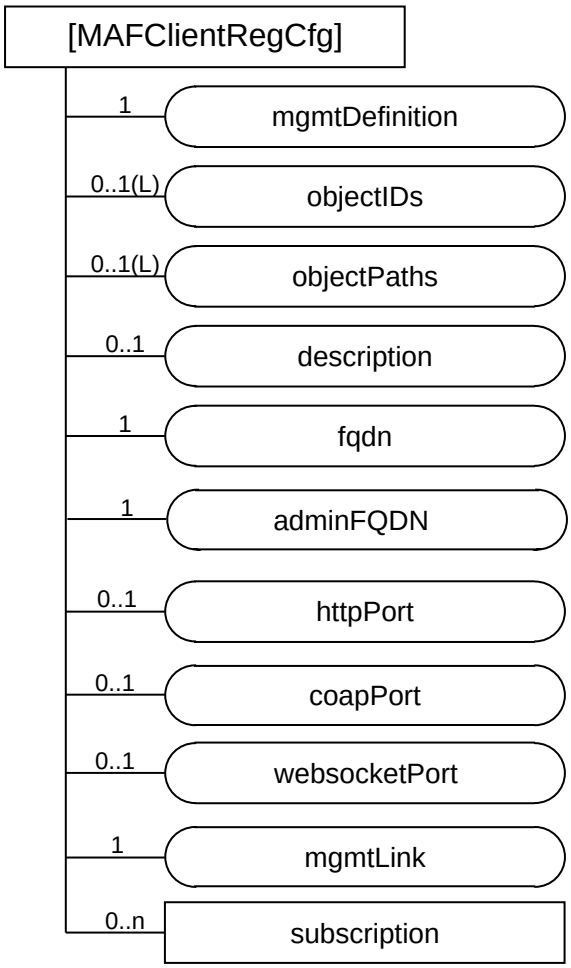

Figure 7.1.7-1: Structure of [*MAFClientRegCfg*] resource

The [*MAFClientRegCfg*] resource shall contain the child resource specified in table 7.1.7-1.

Table 7.1.7-1: 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 [2]

The [*MAFClientRegCfg*] resource shall contain the attributes specified in table 7.1.7-2.

Table 7.1.7-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1025 ("MAFClientRegCfg").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
fqdn	1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [3]
adminFQDN	1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [3]
httpPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [3]
coapPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [3]
websocketPort	0..1	WO	See clause 8.8.3.2 of oneM2M TS-0003 [3]
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 [3], 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.

7.1.8 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 [3]).

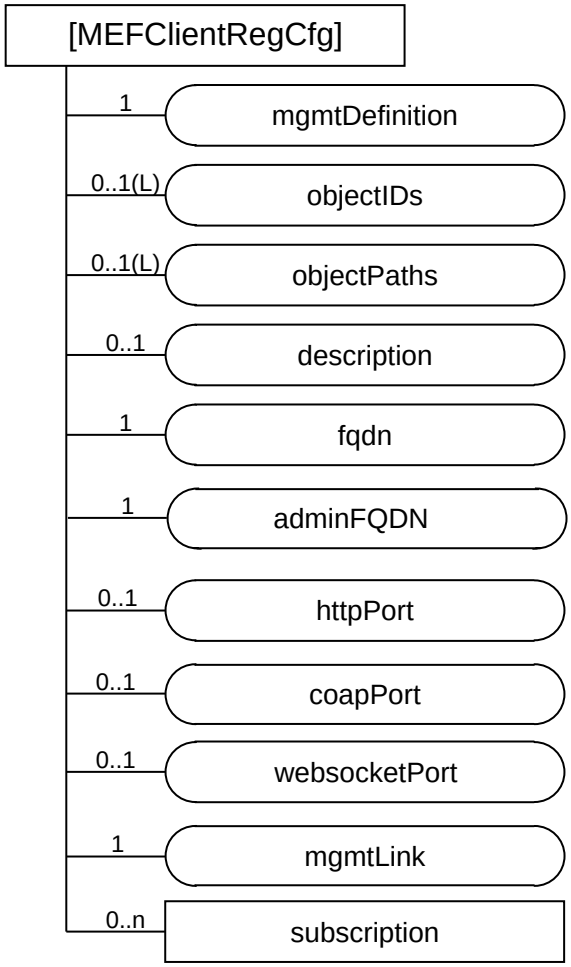

Figure 7.1.8-1: Structure of [*MEFClientRegCfg*] resource

The [*MEFClientRegCfg*] resource shall contain the child resource specified in table 7.1.8-1.

Table 7.1.8-1: 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 [2]

The [*MEFClientRegCfg*] resource shall contain the attributes specified in table 7.1.8-2.

Table 7.1.8-2: 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 [2].
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [2].
labels	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [2].
mgmtDefinition	1	WO	See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1026 ("MEFClientRegCfg").
objectIDs	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
objectPaths	0..1 (L)	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
description	0..1	RW	See clause 9.6.15 of oneM2M TS-0001 [2].
fqdn	1	WO	See clause 8.3.7 of oneM2M TS-0003 [3]
adminFQDN	1	WO	See clause 8.3.7 of oneM2M TS-0003 [3]
httpPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [3]
coapPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [3]
websocketPort	0..1	WO	See clause 8.3.7 of oneM2M TS-0003 [3]
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 [3], 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.

7.2 Resource-Type specific procedures and definitions

7.2.1 Introduction

The present clause defines the resource-type specific details of the resource representations and protocol procedures for each <*mgmtObj*> specialization defined in clause 7.1.

7.2.2 Resource [registration]

7.2.2.1 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 7.2.2.1-1: Data Type Definition of [*registration*]

Data Type ID	File Name	Note
registration	DCFG-registration-v2_3_0.xsd	

Table 7.2.2.1-2: Resource specific attributes of [*registration*]

Attribute Name	Request Optionality		Data Type	Default Value and Constraints
	Create	Update		
mgmtDefinition	M	NP	See clause 7.4.15of oneM2M TS-0004 [4].	"registration"
objectIDs	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [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 oneM2M TS-0001 [2].
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 oneM2M TS-0001 [2].
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 (SAEF). 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 [4].				

7.2.2.2 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 is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource.

7.2.3 Resource [dataCollection]

7.2.3.1 Introduction

Table 7.2.3.1-1: Data Type Definition of [*dataCollection*]

Data Type ID	File Name	Note
dataCollection	DCFG-dataCollection-v2_3_0.xsd	

Table 7.2.3.1-2: 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 [4].	"dataCollection"
objectIDs	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [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 [4].				

7.2.3.2 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.2.4 Resource [authenticationProfile]

7.2.4.1 Introduction

Table 7.2.4.1-1: Data Type Definition of [*authenticationProfile*]

Data Type ID	File Name	Note
authenticationProfile	DCFG-authenticationProfile-v2_3_0.xsd	

Table 7.2.4.1-2: 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 [4].	"authenticationProfile"
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [4].	
SUID	M	NP	m2m:suid	Allowed values are listed in table 7.1.4-3.
TLSCiphersuites	M	O	dcfg:listOfTLSCiphersuite	
symmKeyID	O	NP	sec:credentialID	
symmKeyValue	O	NP	xs:hexBinary	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 [4].	

Table 7.2.4.1-3: 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 [4]

1.1.1.1 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.2.5 Resource [myCertFileCred]

7.2.5.1 Introduction

Table 7.2.5.1-1: Data Type Definition of [*myCertFileCred*]

Data Type ID	File Name	Note
myCertFileCred	DCFG-myCertFileCred-v2_3_0.xsd	

Table 7.2.5.1-2: 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 [4].	"myCertFileCred"
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [4].	
SUIDs	M	O	xs:list of m2m:suid	Allowed values are listed in table 7.1.5-3.
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 7.2.5.1-3: 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 [4]

1.1.1.2 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.2.6 Resource [trustAnchorCred]

7.2.6.1 Introduction

Table 7.2.6.1-1: Data Type Definition of [*trustAnchorCred*]

Data Type ID	File Name	Note
trustAnchorCred	DCFG-trustAnchorCred-v2_3_0.xsd	

Table 7.2.6.1-2: 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 [4].	"trustAnchorCred"
objectID	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
objectPaths	O	NP	See clause 7.4.15 of oneM2M TS-0004 [4].	
description	O	O	See clause 7.4.15 of oneM2M TS-0004 [4].	
certFingerprint	M	NP	dcfg:niURI	
URI	M	O	xs:anyURI	

Table 7.2.6.1-3: 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 [4]

7.2.6.2 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.2.7 Resource [MAFClientRegCfg]

7.2.7.1 Introduction

Table 7.2.7.1-1: Data Type Definition of [*MAFClientRegCfg*]

Data Type ID	File Name	Note
MAFClientRegCfg	DCFG-MAFClientRegCfg-v2_3_0.xsd	

Table 7.2.7.1-2: 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 [4].	"MAFClientRegCfg"
fqdn	M	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
adminFQDN	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
httpPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	At least one of these attributes shall be present
coapPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
websocketPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
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 [3].				

Table 7.2.7.1-3: 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 [4]

7.2.7.2 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.2.8 Resource [MEFClientRegCfg]

7.2.8.1 Introduction

Table 7.2.8.1-1: Data Type Definition of [*MEFClientRegCfg*]

Data Type ID	File Name	Note
MEFClientRegCfg	DCFG-MEFClientRegCfg-v2_3_0.xsd	

Table 7.2.8.1-2: 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 [4].	"MEFClientRegCfg"
fqdn	M	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
adminFQDN	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
httpPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	At least one of these attributes shall be present
coapPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
websocketPort	O	NP	See table 12.4.2-1 of oneM2M TS-0003 [3]	
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 [3].				

Table 7.2.8.1-3: 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 [4]

7.2.8.2 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 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS-0006 [6] provide the mapping of these resources into the technology specific protocol data model.

7.3 Data formats for device configuration

7.3.1 Introduction

The clause 7.3 defines data formats of resource attributes and parameters used in present document.

Any data types of XML elements defined for use in present document shall be one of name spaces in table 7.3.1-1.

Table 7.3.1-1: Namespaces used in present document

Name space	prefix	Name space 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

7.3.2 Simple oneM2M data types for device configuration

Table 7.3.2-1 describes simple data type definitions specific to security. The types in table 7.3.2-1 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 7.3.2-1: oneM2M simple data types for device configuration

XSD type name	Used for	Examples	Description
dcfg:TLSCiphersuite	A TLS Ciphersuite 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 [8]
dcfg:ListOfTLSCiphersuite	A list of TLS Ciphersuite 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 [7], 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 [7], with no authority field. A checkdigit may be present.

8 Procedures

8.1 <mgmtObj> life cycle procedures

8.1.1 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 6.1.

8.1.2 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 8.1.2-1 depicts this flow.

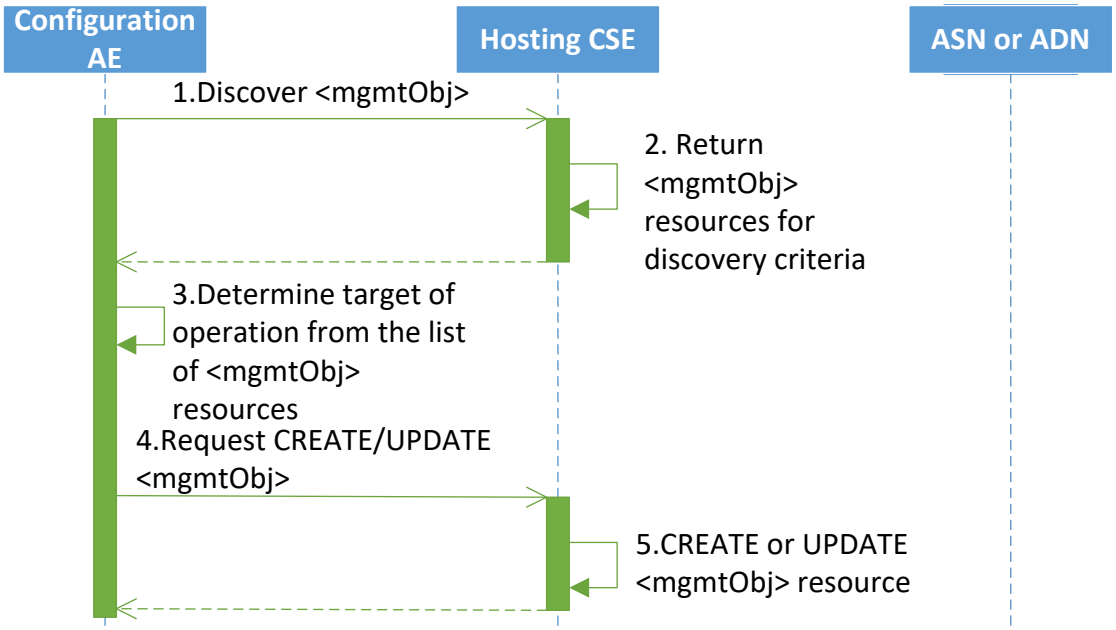

Figure 8.1.2-1: Configuring attributes of a <*mgmtObj*> resource

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.

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

8.1.3.1 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 6.1.

8.1.3.2 Management using device management technologies

Clause 10.2.8 '<*mgmtObj*> Resource Procedures' of oneM2M TS-0001 [2] describes the procedures for M2M Nodes to represent their technology specific data as oneM2M resources within the IN-CSE.

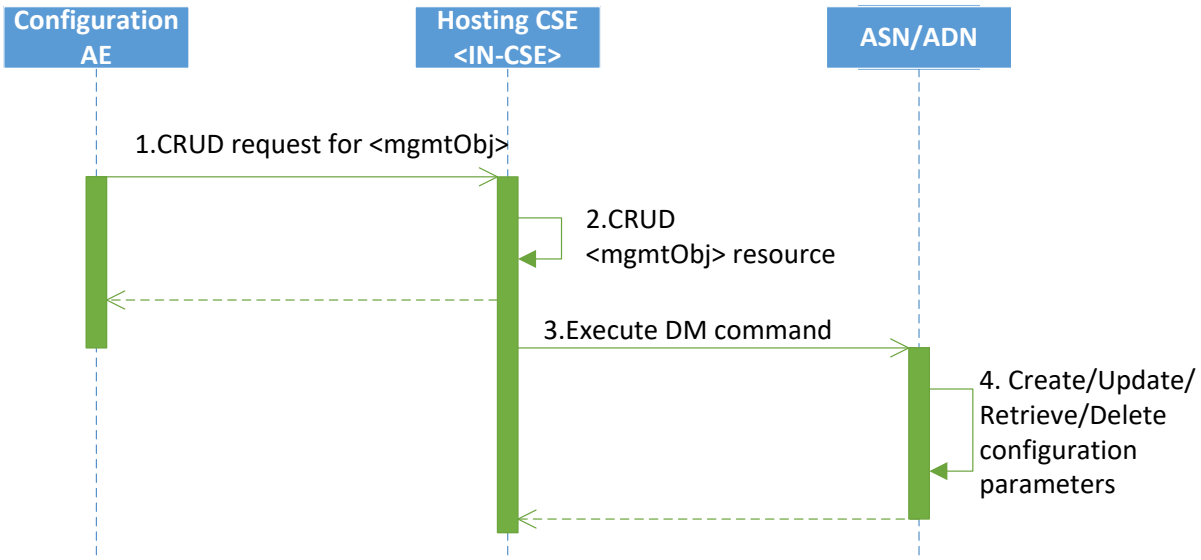

Figure 8.1.3.2-1: Management using Device Management technologies

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.

8.1.3.3 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 [2]. 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 6.1 of the present document, <*mgmtObj*> specializations may be announced depending on the <*mgmtObj*> specialization type.

The following <*mgmtObj*> specializations specified in the present 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 the present 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]

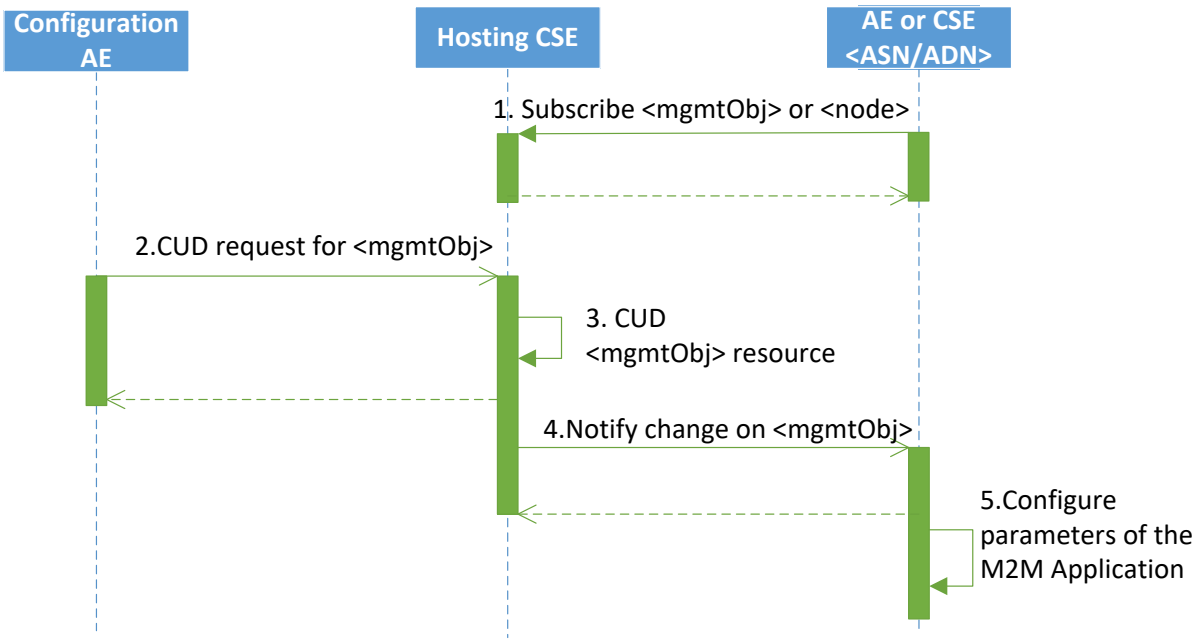

Figure 8.1.3.3-1: Management using the Mcc reference point

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 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.

8.1.3.4 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 the present document. 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 the present document.

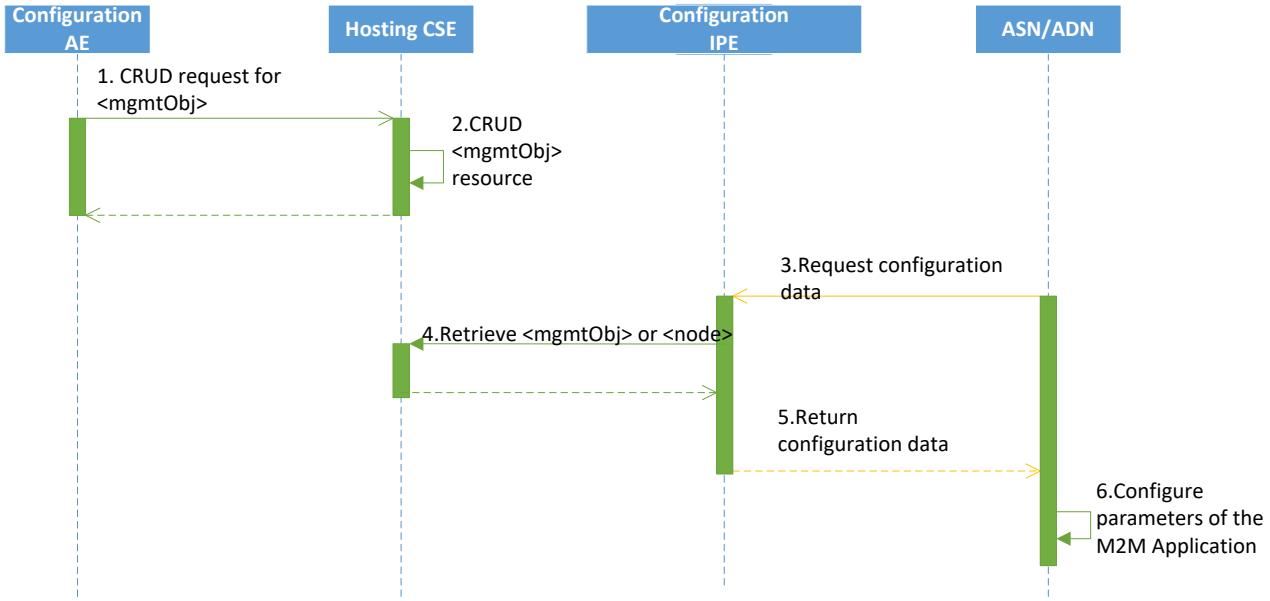

Figure 8.1.3.4-1: Management using oneM2M IPE technology

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 <*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 oneM2M TS-0004 [4] 'oneM2M specific MIME media types'.

8.2 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.

Actual credential shall be obtained using the information on the <*mgmtObj*> specializations (Authentication Credential Configuration) which is referred by mgmtLinkRef(s) from Authentication Profile.

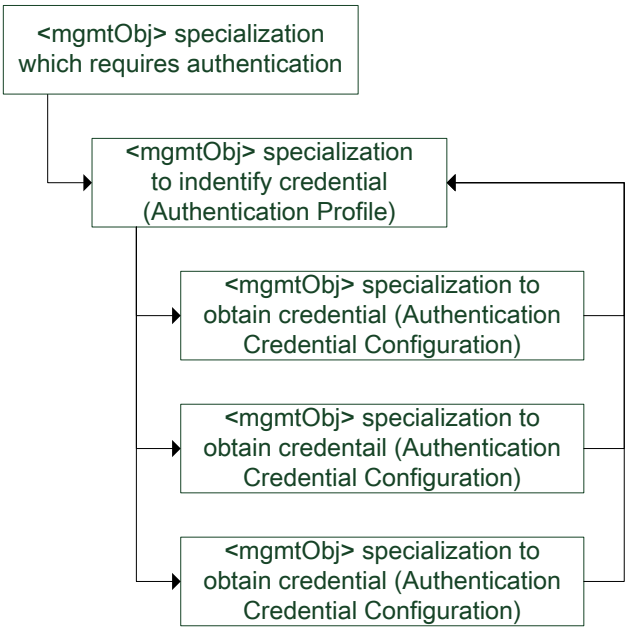

Figure 8.2-1: Relationship between 'Authentication Profile' and 'Authentication Credential Configuration(s)

8.3 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 [2] 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 [2] is used.

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

Table 8.3-1: Required [registration] resource parameters for registration

attribute of [*registration*]	parameter in TS-0001 [2]/TS-0004 [4]
originatorID	From primitive parameter
PoA	CSE-PoA (Point of Access)
resourcePath	To primitive parameter

8.4 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 AE is configured with the [*dataCollection*] resource AE performs CREATE operation for new <*contentInstance*> resource as the child resource of <container> resource which is specified as '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.

9 Short Names

9.1 Introduction

Short names are introduced in clause 8.2.1 of oneM2M TS-0004 [4]. The short names in oneM2M TS-0004 shall apply in addition to the short names defined in the present document.

9.2 Common and Field Device Configuration specific oneM2M Resource attributes

In protocol bindings, resource attribute names shall be translated into short names of table 9.2-1 and in table 8.2.3-1 of oneM2M TS-0004 [4].

Table 9.2-1: Common and Field Device Configuration specific oneM2M Attribute Short Names

Attribute Name	Occurs in	Short Name	Notes
resourceType	All	***ty***	Defined in oneM2M TS-0004 [4].
resourceID	All	***ri***	Defined in oneM2M TS-0004 [4].
resourceName	All	***rn***	Defined in oneM2M TS-0004 [4].
parentID	All	***pi***	Defined in oneM2M TS-0004 [4].
expirationTime	All	***et***	Defined in oneM2M TS-0004 [4].
creationTime	All	***ct***	Defined in oneM2M TS-0004 [4].
labels	All	***lbl***	Defined in oneM2M TS-0004 [4].
lastModifiedTime	All	***lt***	Defined in oneM2M TS-0004 [4].
description	All	***dc***	Defined in oneM2M TS-0004 [4].
mgmtDefinition	All	***mgd***	Defined in oneM2M TS-0004 [4].
objectIDs	All	***obis***	Defined in oneM2M TS-0004 [4].
objectPaths	All	***obps***	Defined in oneM2M TS-0004 [4].
mgmtLink	All	***cmlk***	Defined in oneM2M TS-0004 [4].
originatorID	registration	***oid***	
poA	registration	***poa***	
appID	registration	***apid***	
externalID	registration	***eid***	
triggerRecipientID	registration	***tri***	
containerPath	dataCollection	***cntp***	
reportingSchedule	dataCollection	***rpsc***	
measurementSchedule	dataCollection	***mesc***	
SUID	authenticationProfile	***suid***	
TLSCiphersuites	authenticationProfile	***tlcs***	
symmKeyID	authenticationProfile	***aski***	
symmKeyValue	authenticationProfile	***skv***	
MAFKeyRegLabels	authenticationProfile	***mkrl***	
MAFKeyRegDuration	authenticationProfile	***mkrd***	
mycertFingerprint	authenticationProfile	***mcfp***	
rawPubKeyID	authenticationProfile	***rpki***	
SUIDs	myCertFileCred	***suids***	
myCertFileFormat	myCertFileCred	***mcff***	
myCertFileContent	myCertFileCred	***mcfc***	
certFingerprint	trustAnchorCred	***cfp***	

Attribute Name	Occurs in	Short Name	Notes
URI	trustAnchorCred	***uri***	Defined in oneM2M TS-0004 [4].
fqdn	MEFClientRegCfg, MAFClientRegCfg	***fq***	Defined in oneM2M TS-0032 [9].
adminFQDN	MEFClientRegCfg, MAFClientRegCfg	***adfq***	Defined in oneM2M TS-0032 [9].
httpPort	MEFClientRegCfg, MAFClientRegCfg	***hpt***	Defined in oneM2M TS-0032 [9].
coapPort	MEFClientRegCfg, MAFClientRegCfg	***cpt***	Defined in oneM2M TS-0032 [9].
websocketPort	MEFClientRegCfg, MAFClientRegCfg	***wpt***	Defined in oneM2M TS-0032 [9].

9.3 Field Device Configuration specific oneM2M Resource types

In protocol bindings, resource type names of the <mgmtObj> specializations shall be translated into the short names of table 9.3-1.

Table 9.3-1: Field Device Configuration specific Resource Type Short Names

ResourceType Name	Short Name
registration	***reg***
registrationAnnc	***regA***
dataCollection	***datc***
dataCollectionAnnc	***datcA***
authenticationProfile	***autp***
MAFClientRegCfg	***macrc***
MEFClientRegCfg	***mecrc***
myCertFileCred	***nycfc***
trustAnchorCred	***tac***

9.4 oneM2M Complex data type members

In protocol bindings, complex data types member names shall be translated into the short names of table 9.4-1.

Table 9.4-1: oneM2M Complex data type member short names

Member Name	Occurs in	Short Name	Notes
childResource	All	***ch***	Defined in oneM2M TS-0004 [4].
name	All	***nm***	Defined in oneM2M TS-0004 [4].
value	All	***val***	Defined in oneM2M TS-0004 [4].
type	All	***typ***	Defined in oneM2M TS-0004 [4].

History

This clause shall be the last one in the document and list the main phases (all additional information will be removed at the publication stage).

Publication history		
V2.3.1	2018-Mar-12	Release 2A - Publication