ETSI TS 118 122 V2.0.0 (2017-05)

oneM2M Field Device Configuration
(oneM2M TS-0022 version 2.0.0 Release 2)

Reference

DTS/oneM2M-000022

Keywords

configuration, IoT, M2M

ETSI

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

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

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

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.

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

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

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

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

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

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

[4] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004)".

[5] ETSI TS 118 105: "oneM2M; Management Enablement (OMA) (oneM2M TS-0005)".

[6] ETSI TS 118 106: "oneM2M; Management Enablement (BBF) (oneM2M TS-0006)".

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

[8] IANA TLS Cipher Suite Registry.

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

2.2 Informative references

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

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

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

[i.1] oneM2M Drafting Rules.

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

3 Definitions and abbreviations

3.1 Definition

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

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

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

Configuration IPE: 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

credential object: end-point of a security protocol

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

3.2 Abbreviations

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

MO	Managed Object (BBF specified management) or Management Object (OMA specified management)
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. ETSI TS 118 101 [2] and ETSI TS 118 103 [3] specifies much of what is needed to configure these devices in the Field Domain (i.e. ADN, ASN/MN). Specifically, ETSI TS 118 101 [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. ETSI TS 118 101 [2] heavily relies on clause 6 and on the Remote Security Provisioning Framework (RSPF) of ETSI TS 118 103 [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 of ETSI TS 118 101 [2].
- 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 ETSI TS 118 101 [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 ETSI TS 118 101 [2] and ETSI TS 118 103 [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 ETSI TS 118 101 [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.

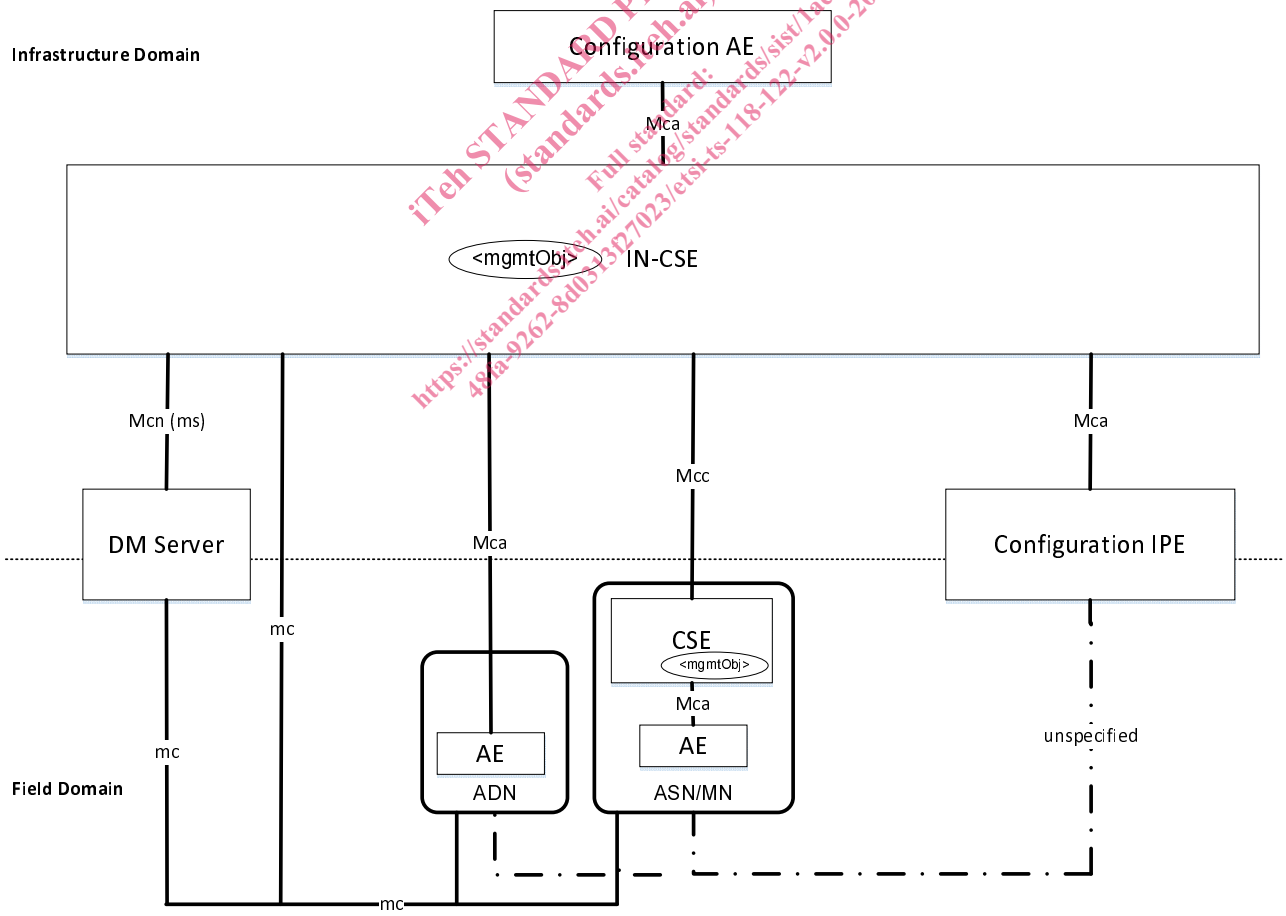

Figure 6.1-1: Architectural Aspects for Configuration of ASN/MN and ADN Nodes

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 ETSI TS 118 101 [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 ETSI TS 118 103 [3] and ETSI TS 118 101 [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 ciphersuites 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 ETSI TS 118 103 [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 ETSI TS 118 103 [3]. If a certificate is remotely provisioned, then a Remote Security Provisioning Framework (RSPF) should be used as described in clause 8.3 of ETSI TS 118 103 [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 ETSI TS 118 103 [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 ETSI TS 118 103 [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 summary of defined <*mgmtObj*> resource specializations in the present document.

Table 7.1.1-1: 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 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.	

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.