ETSI TS 118 111 V2.4.1 (2016-09)

oneM2M;
Common Terminology
(oneM2M TS-0011 version 2.4.1 Release 2)

Reference
RTS/oneM2M-000011v200

Keywords
IoT, M2M, terminology

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 contains a collection of specialist technical terms, definitions and abbreviations referenced within the oneM2M specifications.

Having a common collection of definitions and abbreviations related to oneM2M documents will:

- ensure that the terminology is used in a consistent manner across oneM2M documents;
- provide a reader with convenient reference for technical terms that are used across multiple documents.

The present document provides a tool for further work on oneM2M technical documentation and facilitates their understanding. The definitions and abbreviations as given in the present document are either externally created and included here, or created internally within oneM2M by the oneM2M TP or its working groups, whenever the need for precise vocabulary is identified or imported from existing documentation.

In addition in oneM2M Technical Specifications and Technical Reports there are also clauses dedicated for locally unique definitions and abbreviations.

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.

Not applicable.

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] Recommendation ITU-T X.800 (1991): "Security architecture for open system interconnection for CCIT applications".

[i.2] Recommendation ITU-T X.800/Amd.1 (1996): "Security architecture for open systems interconnection for CCITT applications. Amendment 1: Layer Two Security Service and Mechanisms for LANs".

[i.3] ISO/IEC 27001 (2005): "Information technology - Security techniques - Information security management systems - Requirements".

[i.4] ISO/IEC 27002 (2005): "Information technology - Security techniques - Code of practice for information security management".

[i.5] IETF RFC 4949 (2007): "Internet Security Glossary, Version 2".

[i.6] NIST SP800-57 Part 1 (07/2012): "Recommendation for Key Management - General, Rev3".

[i.7] NIST SP800-57 Part 1 (05/2011): "Recommendation for Key Management - General, Rev3".

[i.8] ISO/IEC 13888-1 (07/2009 - 3rd ed) Information technology - Security techniques - Non-repudiation - Part 1: General".

[i.9] ISO/IEC 24760-1 (12/2011 - 1st edition): "Information technology - Security techniques - A framework for identity management - Part 1: terminology and concepts".

[i.10] ISO/IEC 27004 (12/2009 - 1st edition): "Information technology - Security techniques - Information security management - Measurement".

[i.11] ISO/IEC 9798-1 (07/2010 - 3rd edition): "Information technology - Security techniques - Entity authentication -. Part 1: General".

[i.12] ISO/IEC TR 15443-1:2012: "Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts".

[i.13] IEEE 802.15.4™-2003: "IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)".

[i.14] OMA OMA-TS-LightweightM2M-V1_0-20141111-D: "Lightweight Machine to Machine Technical Specification".

3 Definitions

3.0 General Information

NOTE 1: Whenever in the present document a term "M2M Xyz" (e.g. M2M Application, M2M Solution, etc.) is used, then the prefix "M2M" should indicate that - unless otherwise indicated - the term identifies an entity Xyz that complies with oneM2M specifications.

NOTE 2: For better readability of the present document the prefix "M2M" is ignored when definitions are alphabetically ordered.

3.1 0-9

Void.

3.2 A

Abstract Information Model: Information Model of common functionalities abstracted from a set of Device Information Models

Abstraction: process of mapping between a set of Device Information Models and an Abstract Information Model according to a specified set of rules

Access Control Attributes: set of parameters of the originator, target resource, and environment against which there could be rules evaluated to control access

NOTE: An example of Access Control Attributes of originator is a role. Examples of Access Control Attributes of Environment are time, day and IP address. An example of Access Control Attributes of targeted resource is creation time.

Access Control Policy: set of privileges which represents access control rules defining allowed entities for certain operations within specified contexts that each entity has to comply with to grant access to an object

Access Control Role: security attribute associated to an entity defining the entity's access rights or limitations to allowed operations

NOTE: One or more operations can be associated to an Access Control Role. An Access Control Role can be associated to one or more entities and an entity can assume one or more Access Control Roles.

Access Decision: authorization reached when an entity's Privileges are evaluated

Analytics: processing which makes use of data to provide actions, insights and/or inference

M2M Application: applications that run the service logic and use M2M Common Services accessible via a set of oneM2M specified open interfaces

NOTE: Specification of M2M Applications is not subject of the current oneM2M specifications.

M2M Area Network: form of an Underlying Network that minimally provides data transport services among M2M Gateway(s), M2M Device(s), and Sensing&Actuation Equipment

NOTE 1: M2M Local Area Networks can use heterogeneous network technologies that may or may not support IP access.

NOTE 2: An M2M Area Network technology is characterized by its physical properties (e.g. IEEE 802.15.4-2003 [i.13] 2_4GHz), its communication protocol (e.g. ZigBee_1_0) and potentially a profile (e.g. ZigBee_HA).

Application Dedicated Node: contains at least one Application Entity and does not contain a Common Services Entity

NOTE: There may be zero or more ADNs in the Field Domain of the oneM2M System.

EXAMPLE: Physical mapping: an Application Dedicated Node could reside in a constrained M2M Device.

Application Entity: represents an instantiation of Application logic for end-to-end M2M solutions

M2M Application Infrastructure: equipment (e.g. a set of physical servers of the M2M Application Service Provider) that manages data and executes coordination functions of M2M Application Services

NOTE: The Application Infrastructure hosts one or more M2M Applications. Specification of Application Infrastructure is not subject of the current oneM2M specifications.

Application (App) Registrants: entities seeking to obtain a registered App-ID

M2M App-ID Registration Authority (ARA): legal entity that manages/administers the App-ID database used to issue unique global identifiers consistent with oneM2M specifications

M2M Application Service: realized through the service logic of an M2M Application and is operated by the User or an M2M Application Service Provider

Application Service Node (ASN): contains one Common Services Entity and contains at least one Application Entity

NOTE: There may be zero or more ASNs in the Field Domain of the oneM2M System.

EXAMPLE: Physical mapping: an Application Service Node could reside in an M2M Device.

M2M Application Service Provider: entity (e.g. a company) that provides M2M Application Services to the User

Authentication [i.7]: process that establishes the source of information, or determines an entity's identity

Authorization [i.1]: granting of rights, which includes the granting of access based on access rights

3.3 B

Void.

3.4 C

M2M Common Services: set of oneM2M specified functionalities that are widely applicable to different application domains made available through the set of oneM2M specified interfaces

Common Services Entity (CSE): represents an instantiation of a set of Common Service Functions of the M2M environments. Such service functions are exposed to other entities through reference points

Common Services Function (CSF): informative architectural construct which conceptually groups together a number of sub-functions

NOTE: Those sub-functions are implemented as normative resources and procedures. A set of CSFs is contained in the CSE.

Confidentiality [i.1]: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Content Sharing Resource: resource of specific type that contains application data to be shared across applications

Credentials: data objects which are used to uniquely identify an entity and which are used in security procedures

Credential-ID: globally unique identifier for a credential that was used to establish a Security Association between entities (CSEs and/or AEs)

NOTE: The Credential-ID can be used to determine the identifying information about the authenticated entity, such as the CSE-ID or AE-ID(s) or App-ID(s).

3.5 D

Data: in the context of oneM2M the term “Data” signifies digital representations of anything

NOTE: Data can or cannot be interpreted by the oneM2M System and/or by M2M Applications. See also Information.

M2M Device: physical equipment with communication capabilities, providing computing and/or sensing and/or actuation services

NOTE: An M2M Device hosts one or more M2M Applications or other applications and can contain implementations of CSE functionalities.

EXAMPLE: Physical mapping: A M2M Device contains an Application Service Node or an Application Dedicated Node.

Device Information Model: Information Model of the native protocol (e.g. ZigBee) for the physical device

Direct Dynamic Authorization: procedure in which a Hosting CSE interacts directly with a Dynamic Authorization System Server to obtain Dynamic Authorization

Dynamic Authorization: procedures for dynamically authorizing additional access to resources on a Hosting CSE without changing the <accessControlPolicy> resources configured to the Hosting CSE

Dynamic Authorization System (DAS): technology, external to oneM2M, which enables Dynamic Authorization

Dynamic Authorization System Server: server configured with policies for Dynamic Authorization, and provided with credentials for issuing Tokens

Dynamic Device/Gateway Context: dynamic metrics, which may impact the M2M operations of M2M Devices/Gateways

3.6 E

Encryption [i.6]: process of changing plaintext into ciphertext using a cryptographic algorithm and Key