ONEM2M
TECHNICAL SPECIFICATION

Document Number	oneM2M-TS-0011-Definitions and Acronyms-V1.0.0
Document Name:	Definitions and Acronyms
Date:	2014-August 01
Abstract:	This TS contains a collection of specific technical terms (definitions and acronyms) used within oneM2M .

This Specification is provided for future development work within oneM2M only. The Partners accept no liability for any use of this Specification.

The present document has not been subject to any approval process by the oneM2M Partners Type 1. Published oneM2M specifications and reports for implementation should be obtained via the oneM2M Partners' Publications Offices.

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

Copyright Notification

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. NO oneM2M PARTNER TYPE 1 SHALL BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY THAT PARTNER FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL oneM2M BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. oneM2M EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Contents

12Scope

The present document contains a collection of specialist technical terms, definitions and acronyms referenced within the oneM2M specifications.

Having a common collection of definitions and acronyms 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.

This document provides a tool for further work on oneM2M technical documentation and facilitates their understanding. The definitions and acronyms as given in this 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.

2 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.

2.1 Normative references

Not applicable.

2.2 Informative references

[i.1] oneM2M-TR-0005-Roles_and_Focus_Areas

[i.2] ITU-T Recommendation X.800 (1991), security architecture for open system interconnection for CCIT applications

[i.3] ITU-T Recommendation 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.4] ISO/IEC 27001 (2005), Information technology – Security techniques   Information security management systems   Requirements.

[i.5] ISO/IEC 27002 (2005), Information technology – Security techniques –Code of practice for information security management.

[i.6] IETF RFC 4949 (2007), Internet Security Glossary, Version 2

[i.7] NIST SP800-57 Part 1, 7/2012 – Recommendation for Key Management – General, Rev3

[i.8] NIST SP800-57 Part 1, 5/2011 – Recommendation for Key Management – General, Rev3

[i.9] ISO/IEC 13888-1: 2009-07-15 (3rd ed) Information technology — Security techniques — Non-repudiation — Part 1: General

[i.10] ISO/IEC 24760-1: 2011-12-15 (1st edition), Information technology – security techniques – a framework for identity management – part 1: terminology and concepts

[i.11] ISO/IEC 27004: 2009-12-15 (1st edition), Information technology — Security techniques — Information security management — Measurement.

[i.12] ISO/IEC 9798-1: 2010-07-01 (3rd edition), Information technology — Security techniques — Entity authentication —. Part 1: General.

[i.13] ISO/IEC TR 15443-1:2012, Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts

3 Definitions

3.0 General Information

NOTE 1: Whenever in this document a term "M2M Xyz" (e.g. M2M System, M2M Solution, …) 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

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 must 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.

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

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

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

Application Dedicated Node: is a Node that contains at least one Application Entity and does not contain a Common Services Entity. There may be zero or more ADNs in the Field Domain of the oneM2M System.
Example of 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. The Application Infrastructure hosts one or more M2M Applications. Specification of Application Infrastructure is not subject of the current oneM2M specifications.

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

Application Service Node: is a Node that contains one Common Services Entity and contains at least one Application Entity. There may be zero or more ASNs in the Field Domain of the oneM2M System.
Example of physical mapping: an Application Service Node could reside in an M2M Device.

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

M2M Area Network: Is a form of an Underlying Network that minimally provides data transport services among M2M Gateway(s), M2M Device(s), and Sensing&Actuation Equipment. M2M Local Area Networks can use heterogeneous network technologies that may or may not support IP access. An M2M Area Network technology is characterized by its physical properties (e.g. IEEE_802_15_4_2003_2_4GHz), its communication protocol (e.g. ZigBee_1_0) and potentially a profile (e.g. ZigBee_HA).

Authentication [i.8]: A process that establishes the source of information, or determines an entity’s identity.

Authorization [i.2]: The granting of rights, which includes the granting of access based on access rights.

3.3 B

<void>

3.4 C

M2M Common Services: is the 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: 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: is an informative architectural construct which conceptually groups together a number of sub-functions. Those sub-functions are implemented as normative resources and procedures. A set of CSFs is contained in the CSE.

Confidentiality [i.2]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

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

3.5 D

Data: In the context of oneM2M the term “Data” signifies digital representations of anything. Data can or cannot be interpreted by the M2M 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. An M2M Device hosts one or more M2M Applications or other applications and can contain implementations of CSE functionalities. Example of 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.

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

3.6 E

Encryption [i.7]: The process of changing plaintext into ciphertext using a cryptographic algorithm and key.

Event: An interaction or occurrence related to and detected by the M2M System.

Event Categories: The set of indicators that specify the treatment of Events for differentiated handling, based on policies.

3.7 F

Field Domain: consists of M2M Devices, M2M Gateways, Sensing and Actuation (S&A) Equipment and M2M Area Networks.

3.8 G

M2M Gateway: physical equipment that includes, at minimum, the entities and APIs of a Middle Node.

3.9 H

<void>

3.10 I

Identification [i.10]: Process of recognizing an entity in a particular domain as distinct from other entities.

NOTE 1 The process of identification applies verification to claimed or observed attributes.
NOTE 2 Identification typically is part of the interactions between an entity and the services in a domain and to access resources. Identification may occur multiple times while the entity is known in the domain.

Information: In the context of oneM2M "Information"signifies data that can be interpreted by the M2M System. Information has a defined syntax and semantic within the M2M System. See also Data.

Information Model: An abstract, formal representation of entities that may include their properties, relationships and the operations that can be performed on them.

Infrastructure Domain: consists of Application Infrastructure and M2M Service Infrastructure

Infrastructure Node: is a Node that contains one Common Services Entity and contains zero or more Application Entities. There is exactly one Infrastructure Node in the Infrastructure Domain per oneM2M Service Provider. Example of physical mapping: an Infrastructure Node could reside in an M2M Service Infrastructure.

Integrity [i.4], [i.5]: Safeguarding the accuracy and completeness of information and processing methods.

3.11 J

<void>

3.12 K

Key [i.7]: A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.

3.13 L

3.14 M

Middle Node: is a Node that contains one Common Services Entity and contains zero or more Application Entities. There may be zero or more Middle Nodes in the Field Domain of the oneM2M System. The CSE in a Middle Node communicates with one CSE residing in a Middle Node or in an Infrastructure Node and with one or more other CSEs residing in Middle Nodes or in Application Service Nodes. In addition, the CSE in the Middle Node can communicate with AEs residing in the same MN or residing in an ADN. Example of physical mapping: a Middle Node could reside in an M2M Gateway.

Mutual Authentication [i.12]: Entity authentication that provides both entities with assurance of each other's identity.

3.15 N

Network Operator: is an entity (e.g. a company) that operates an Underlying Network.

Node: logical entity that is identifiable in the M2M System.

3.16 O

oneM2M System: The oneM2M System is the system developed by the oneM2M global initiative that enables deployable M2M Solutions.

3.17 P

Privacy [i.3]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Privilege: Qualification given to an entity that allows a specific operation (e.g. Create/Retreive/Update/Delete, etc.) on a specific resource within a specified context.

3.18 Q

<void>

3.19 R

Repudiation: Denial by an entity of a claimed event or action.

NOTE: This definition applies to the security context only.

Role-Based Access Control [i.4]: permissions attributed to an Access Control Role granting access to an object.

3.20 S

Secure [i.13]: Not vulnerable to most attacks, are able to tolerate many of the attacks that they are vulnerable to, and that can recover quickly with a minimum of damage from the few attacks that successfully exploit their vulnerabilities.

Security [i.6]: A system condition that results from the establishment and maintenance of measures to protect the system.

Security Bootstrapping: The remote Security Provisioning for a service of a device deployed in the field.

Security Pre-Provisioning: The Security Provisioning performed prior to device deployment, e.g. during manufacturing.

Security Provisioning: The process of configuring a device to enable access to a service provided by a target entity, such as communication services or M2M Services. This involves putting in the device and target entity the security Credential that will be used for Mutual Authentication.

Sensing and Actuation (S&A) Equipment: equipment that provides functionality for sensing and/or influencing the physical environment by interacting with one or more M2M Application Services. Sensing and Actuation Equipment can interact with the M2M System, however does not host an M2M Application. The specification of S&A Equipment is not considered in the current oneM2M specifications. S&A Equipment may, but does not need to, be co-located with an M2M Device.

Sensitive Data: is a classification of stakeholder's data that is likely to cause its owner some adverse impact if either:
- It becomes known to others when not intended,
- It is modified without consent of the affected stakeholder

M2M Service: consists of one or more M2M Application Services and one or more M2M Common Services.

M2M Service Administrative State of a M2M Device: indicates whether the M2M Service is enabled by the M2M Service Provider to be run for this device.

M2M Service Infrastructure: physical equipment (e.g. a set of physical servers) that provides management of data and coordination capabilities for the M2M Service Provider and communicates with M2M Devices. An M2M Service Infrastructure may communicate with other M2M Service Infrastructures. An M2M Service Infrastructure contains a CSE. It can also contain M2M applications.

M2M Service Operational Status of a M2M Device: indicates whether the M2M Service is currently running for this device.

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

M2M Service Subscriber: One of the M2M Stakeholders that subscribes to M2M Service(s).

M2M Service Subscription: An agreement between a provider and a subscriber for consumption of M2M Services for a period of time. An M2M Service Subscription is typically a commercial agreement.

M2M Session: A service layer communication relationship between endpoints managed via M2M Common Services consisting of session authentication, connection establishment/termination, transmission of information and establishment/termination of Underlying Network services.

M2M Solution: A set of deployed systems satisfying all of the following criteria:

1. It satisfies the end-to-end M2M communication requirements of particular users; and
2. Some part of the M2M Solution is realized by including services compliant to oneM2M specifications.

M2M Stakeholder: entities who facilitate and/or participate in the legitimate operation of the M2M system. Examples of stakeholders, in alphabetical order, are: M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; Manufacturer of M2M system and its components; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator; User/Consumer of the M2M solution etc.

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

3.21 T

Thing: an element which is individually identifiable in the oneM2M system.

Trust [i.9]: A relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy.

3.22 U

Underlying Network: Functions, networks, busses and other technology assisting in data transportconnectivity services.

User: An entity which utilizes the services of the M2M Solution. The User may or may not be a subscriber to an M2M Application Service or an M2M Service. The User may or may not be identifiable in the M2M System.

3.23 V

Verification [i.11]: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Virtual Device: a logical device (implemented as software) that acts similar to physical M2M device and provides derived data. E.g. average temperature of a room, number of vehicles that passed during the last minute.

3.24 W

<void>

3.25 X

<void>

3.26 Y

<void>

3.27 Z

<void>

4 Acronyms

4.1 0-9

3GPP…3rd Generation Partnership Project

4.2 A

ACL… Access Control List

ADN…Application Dedicated Node

AE…Application Entity

API…Application Programming Interface

ASN…Application Service Node

4.3 B

BBF… Broad Band Forum

4.4 C

CHA…Continua Health Alliance

CPU… Centralized Processing Unit

CSE… Common Services Entity

CSF…Common Services Function

4.5 D

DM…Device Management

4.6 E

4.7 F

4.8 G

GBA… Generic Bootstrapping Architecture

GSM…Global System for Mobile communications

GSMA…GSM Association

4.9 H

4.10 I

IN…Infrastructure Node

IP…Internet Protocol

4.11 J

4.12 K

4.13 L

4.14 M

M2M … Machine to Machine

MN…Middle Node

MSISDN… Mobile Subscriber Integrated Services Digital Network-Number

MTC… Machine Type Communications

4.15 N

NSE… Network Service Entity

4.16 O

OMA… Open Mobile Alliance

4.17 P

4.18 Q

QoS… Quality of Service

4.19 R

RBAC…Role-Based Access Control

4.20 S

S&A … Sensing and Actuation

SDO… Standards Developing Organization

SMS… Short Message Service

4.21 T

TR…Technical Report

TS…Technical Specification

4.22 U

UICC… Universal Integrated Circuit Card

USIM… Universal Subscriber Identity Module

USSD… Unstructured Supplementary Service Data

4.23 V

4.24 W

WAN… Wide Area Network

4.25 X

4.26 Y

4.27 Z

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		
V.1.1.1	<dd Mmm yyyy>	<Milestone>

Draft history (to be removed on publication)		
V.0.0.1	26 Feb 2013	oneM2M-REQ-2013-0178R01 applied – initial skeleton TR
V.0.0.2	28 Feb 2013	oneM2M-REQ-2013-0139R05 applied – adds definitions and references
V.0.0.3	15 Apr 2013	Applied the following CRs: oneM2M-REQ-2013-0242R01 Subscription Term Update oneM2M-REQ-2013-0278-CR_change_text_of_section_1
V.0.0.4	10 June 2013	Applied the following CR: oneM2M-REQ-2013-0277R02-Security_Terminology_Update applied editorial changes
V.0.1.0	21 June 2013	Applied the following CR: oneM2M-TP-2013-0285R01-CR_to_TR_0004_Definitions_and_Acronyms_V0_0_3 applied editorial changes
V.0.2.0	09 Aug 2013	Applied the following CRs: oneM2M-REQ-2013-0335R03-Definition_of_Local_Context oneM2M-REQ-2013-0350R05-Clarify_OSR-019_and_OSR-021 – defines Data and Information) oneM2M-REQ-2013-0362-Update_to_Security_Terminology oneM2M-REQ-2013-0377R01-MAS_related_CR_to_TR_0004_Definitions_and_Acronyms_V0_0_3 oneM2M-REQ-2013-0383-Definition_of_stakeholder oneM2M-REQ-2013-0384R03-Input_Requirements_for_Correlation_of_Service_Statuses oneM2M-REQ-2013-0387R01-Definition_of_User oneM2M-REQ-2013-0388R02-CR_Definitions_from_REQ-2013-0351R03 oneM2M-ARC-2013-0314R01-Missing_definitions_for_WG1_work_progress_continued oneM2M-ARC-2013-0353R01-Definition_of_physical_objects applied editorial changes (upper case letters for definitions)
V.0.3.0	18 Oct 2013	Applied the CR oneM2M-TP-2013-0352-CR_to_TR_0004_Definitions_and_Acronyms.doc, aligned TR with latest template (copyright statement frontpage, new page 2)

V.0.4.0	13 Dec 2013	Applied the following CR oneM2M-TP-2013-0383-CR_to_TR_0004_Definitions_and_Acronyms and applied editorial changes to sections 2.2 (reference) and 3 (alphabetical order)
V.0.4.1	22 Feb 2014	According to TP decision at TP#9 (Mobile, AL) to change the WI-0003 in TP-2014-0028-CR_to_WI-0003-VocabPrinciples-V1_2 the TR was transformed into a TS.
V.0.5.0	11 Feb 2014	The following CR was applied after approval by MAS, review by TP and approval by REQ: MAS-2014-0333R01-CR_on_definition_of_M2M_Area_Network.doc. Additionally an Editor`s note was added highlighting the need for a definition for the term M2M Gateway.
V.0.6.0	12 Jun 2014	Applied the following CRs: REQ-2014-0443R02-Change_Privilege_Definition REQ-2014-0444R01-Terminology_change_of_M2M_System REQ-2014-0445R01-Definition_change_of_Subscriberr REQ-2014-0448-CR_to_TS-011_add_acronyms_to_section_4 REQ-2014-0454-Access_Control_Policy_Definition
V.0.7.0	29 Jul 2014	The following CR was applied: REQ-2014-0455R03-Proposed_resolution_for_Editors_notes_on_M2M_Gateway_and_node_relation