ONEM2M TECHNICAL SPECIFICATION

Document Number	TS-0011-V2.4.1
Document Name:	Common Terminology
Date:	2016-August-30
Abstract:	This TS contains a collection of specific technical terms (definitions and abbreviations) used within oneM2M .

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

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

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 reference document (including any amendments) applies.

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 reference 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] 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

End-to-End Certificate-based Key Establishment (E2EKey): interoperable framework for two end-points to use certificates for establishing symmetric keys for use in End-to-End Security of Data or End-to-End Security of Primitives

End-to-End Certificate-based Key Establishment Initiating End-Point: AE or CSE initiating the End-to-End Certificate-based Key Establishment procedure

End-to-End Certificate-based Key Establishment Terminating End-Point: AE or CSE with which an End-to-End Certificate-based Key Establishment Initiating End-Point intends to establish a symmetric key using End-to-End Certificate-based Key Establishment procedure

End-to-End Security of Data (ESData): interoperable framework for protecting data that ends up transported using oneM2M reference points, in order that so transited CSEs do not need to be trusted with that data

End-to-End Security of Primitives (ESPrim): interoperable framework for securing oneM2M primitives so CSEs (forwarding the primitive) do not need to be trusted with the confidentiality and integrity of the primitives

Event: interaction or occurrence related to and detected by the oneM2M System

Event Categories: 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

Geo-fence: virtual perimeter for real-time geographical area to detect whether an object is entering into or leaving from

3.9 H

Void.

3.10 I

Identification [i.9]: 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.

Indirect Dynamic Authorization: procedure in which an Originator obtains Dynamic Authorization from a Dynamic Authorization System Server, and provides the Hosting CSE with a Token or Token-ID representing that Dynamic Authorization

Information: in the context of oneM2M "Information"signifies data that can be interpreted by the oneM2M System

NOTE: Information has a defined syntax and semantic within the oneM2M System. See also Data.

Information Model: 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 (IN): contains one Common Services Entity and contains zero or more Application Entities

NOTE: There is exactly one Infrastructure Node in the Infrastructure Domain per oneM2M Service Provider.

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

Inner Primitive: oneM2M Primitive being secured by End-to-End Security for Primitives

Integrity [i.3], [i.4]: safeguarding the accuracy and completeness of information and processing methods

Interworking Proxy Application Entity (IPE): specialized AE that facititates interworking between Non-oneM2M Nodes (NoDN) and the oneM2M System. An IPE maps data of the NoDN into oneM2M resources

NOTE: It invokes operations in the NoDN when the related oneM2M resources are modified and modifies oneM2M resources based on the output of NoDN operations.

3.11 J

Void.

3.12 K

Key [i.6]: 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

LWM2M Client [i.14]: application that manages and controls things that are represented as LWM2M objects

LWM2M Client Endpoint Name [i.14]: identifier for a LWM2M Client

LWM2M Object [i.14]: LWM2M representation of a thing. LWM2M Objects are identified through a URI

LWM2M Server [i.14]: application that manages and controls LWM2M Clients

3.14 M

Management Authority (MA): legal entity that will supervise the issuance of unique global App-IDs under given Authority IDs, and potentially contract with an organization that will issue such unique global identifiers

Middle Node (MN): contains one Common Services Entity and contains zero or more Application Entities

NOTE 1: There may be zero or more Middle Nodes in the Field Domain of the oneM2M System.

NOTE 2: 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: Physical mapping: a Middle Node could reside in an M2M Gateway.

Mutual Authentication [i.11]: entity authentication that provides both entities with assurance of each other's identity

3.15 N

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

Node: logical entity that is identifiable in the oneM2M System

3.16 O

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

Outer Primitive: primitive used to transport an Inner Primitive secured using End-to-End Security of Primitives

3.17 P

Privacy [i.2]: 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

Registrar: legal entities that will directly interface with App Developers seeking App-IDs and can assign unique IDs

Remote Security Provisioning: process of providing a credential into a secure environment of a Node deployed in the field

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.3] (RBAC): permissions attributed to an Access Control Role granting access to an object

3.20 S

Secure [i.12]: 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.5]: system condition that results from the establishment and maintenance of measures to protect the system

Security Association: set of shared security attributes necessary to perform secure communication between two entities (CSEs and/or AEs) which have performed Mutual Authentication.

NOTE: The security attributes include a description of the algorithms to be applied, and derived keys which are applied for the lifetime of the security association.

Security Association Establishment: procedure for establishing a Security Association between two entities (CSEs and/or AEs)

Security Pre-Provisioning: process of providing a credential into a secure environment of the Node prior to device deployment, e.g. during manufacturing

Security Provisioning: process of configuring a credential into a secure environment of a Node to enable access to a service provided by a target entity, such as communication services or M2M Services

NOTE: This involves putting in the device and target entity the security Credentials 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

NOTE: Sensing and Actuation Equipment can interact with the oneM2M 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: 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

NOTE: 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: 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: agreement between a provider and a subscriber for consumption of M2M Services for a period of time

NOTE: An M2M Service Subscription is typically a commercial agreement.

M2M Session: 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: 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 oneM2M system

NOTE: Examples of stakeholders, in alphabetical order, are:

- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- Manufacturer of oneM2M 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

Time Series Data: sequence of data points which typically consist of successive measurements made over a time interval

Thing: element which is individually identifiable in the oneM2M system

Trust [i.8]: 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: entity which utilizes the services of the M2M Solution

NOTE: 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 oneM2M System.

3.23 V

Verification [i.10]: confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Virtual Device: logical device (implemented as software) that acts similar to physical M2M Device and provides derived data

EXAMPLE: 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 Abbreviations

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
AR Application Registrants
ARA M2M App-ID Registration Authority
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

DAS	Dynamic Authorization System
DM	Device Management

4.6 E

E2EKey	End-to-End Certificate-based Key Establishment
ESData	End-to-End Security of Data
ESPrim	End-to-End Security of Primitives

4.7 F

Void.

4.8 G

GBA	Generic Bootstrapping Architecture
GSM	Global System for Mobile communications
GSMA	GSM Association

4.9 H

Void.

4.10 I

IN	Infrastructure Node
IP	Internet Protocol
IPE	Interworking Proxy Application Entity

4.11 J

Void.

4.12 K

Void.

4.13 L

LWM2M	Lightweight M2M.

4.14 M

M2M	Machine to Machine
MA	Management Authority
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

Void.

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
URI	Universal Resource Identifier

4.23 V

Void.

4.24 W

WAN Wide Area Network

4.25 X

Void.

4.26 Y

Void.

4.27 Z

Void.

Annex A (informative): Bibliography

- TR-0005: "Roles and Focus Areas".

History

Publication history		
V1.2.1	30 Jan 2015	Release 1 - Publication
V2.4.1	30 August 2016	Release 2 - Publication