International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4500.11

(03/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Frameworks, architectures and protocols

---

oneM2M – Common terminology

Recommendation ITU-T Y.4500.11

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	**Y.4400–Y.4549**
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4500.11

oneM2M – Common terminology

Summary

Recommendation ITU-T Y.4500.11 contains a collection of specialist technical terms, definitions and abbreviations referenced within oneM2M specifications transposed as ITU-T Recommendations.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.4500.11	2018-03-01	20	11.1002/1000/13506

Keywords

Specialist technical terms, definitions, abbreviations

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

NOTE – This Recommendation departs slightly from the usual editorial style of ITU-T Recommendations to preserve existing cross-referencing from external documents.

Table of Contents

Page

Page

Recommendation ITU-T Y.4500.11

oneM2M - Common terminology

1 Scope

This Recommendation contains a collection of specialist technical terms, definitions and abbreviations referenced within oneM2M specifications transposed as ITU-T Recommendations.

Having a common collection of definitions and abbreviations related to these Recommendations will:

- ensure that the terminology is used in a consistent manner across the Recommendations;
- provide readers with a 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.

This Recommendation contains oneM2M Release 2 specification - oneM2M Common Terminology V2.4.1 and is equivalent to standards of oneM2M partners including ARIB, ATIS [ATIS.oneM2M.TS0011V241-2016], CCSA [CCSA M2M-TS-0011-V2.4.1], ETSI [ETSI TS 118 111 V2.4.1], TIA, TSDSI [TSDSI STD T1.oneM2M TS-0011-2.4.1 V1.0.0], TTA [TTAT.MM-TS.0011 v2.4.1] and TTC [TTC TS-M2M-0011v2.4.1].

2 References

None.

3 Definitions

This Recommendation lists the following terms defined in oneM2M related Recommendations:

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

3.2.1 abstract information model: Information model of common functionalities abstracted from a set of device information models.

3.2.2 abstraction: Process of mapping between a set of device information models and an abstract information model according to a specified set of rules.

3.2.3 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 an originator is a role. Examples of access control attributes of environment are time, day and IP address. An example of access control attributes of a targeted resource is creation time.

3.2.4 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.

3.2.5 access control role: Security attribute associated with an entity defining the entity's access rights or limitations to allowed operations.

NOTE – One or more operations can be associated with an access control role. An access control role can be associated with one or more entities and an entity can assume one or more access control roles.

3.2.6 access decision: Authorization reached when an entity's privileges are evaluated.

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

3.2.8 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.

3.2.9 M2M area network: Form of an underlying network that minimally provides data transport services among M2M gateway(s), M2M device(s) and sensing and actuation (S&A) 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 [b-IEEE 802.15.4] 2_4GHz), its communication protocol (e.g., ZigBee_1_0) and potentially a profile (e.g., ZigBee_HA).

3.2.10 application dedicated node: Contains at least one application entity and does not contain a common services entity.

NOTE – There may be zero or more application dedicated nodes (ADNs) in the field domain of the oneM2M system.

EXAMPLE – Physical mapping: an application dedicated node could reside in a constrained M2M device.

3.2.11 application entity: Represents an instantiation of application logic for end-to-end M2M solutions.

3.2.12 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.

3.2.13 application (App) registrants: Entities seeking to obtain a registered App-ID.

3.2.14 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.

3.2.15 M2M application service: Realized through the service logic of an M2M application and is operated by the user or an M2M application service provider.

3.2.16 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.

3.2.17 M2M application service provider: Entity (e.g., a company) that provides M2M application services to the user.

3.2.18 authentication [b-NIST SP800-57 Part 1]: Process that establishes the source of information, or determines an entity's identity.

3.2.19 authorization [b-ITU-T X.800]: Granting of rights, which includes the granting of access based on access rights.

3.3 B

Void.

3.4 C

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 confidentiality [b-ITU-T X.800]: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.4.5 content sharing resource: Resource of specific type that contains application data to be shared across applications.

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

3.4.7 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

3.5.1 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".

3.5.2 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.

3.5.3 device information model: Information model of the native protocol (e.g., ZigBee) for the physical device.

3.5.4 direct dynamic authorization: Procedure in which a hosting CSE interacts directly with a dynamic authorization system server to obtain dynamic authorization.

3.5.5 dynamic authorization: Procedures for dynamically authorizing additional access to resources on a hosting CSE without changing the <accessControlPolicy> resources configured to the hosting CSE.

3.5.6 dynamic authorization system (DAS): Technology, external to oneM2M, which enables dynamic authorization.

3.5.7 dynamic authorization system server: Server configured with policies for dynamic authorization and provided with credentials for issuing tokens.

3.5.8 dynamic device/gateway context: Dynamic metrics, which may impact the M2M operations of M2M devices/gateways.

3.6 E

3.6.1 encryption [b-NIST SP800-57 Part 1]: Process of changing plaintext into ciphertext using a cryptographic algorithm and key.

3.6.2 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.

3.6.3 end-to-end certificate-based key establishment initiating end-point: AE or CSE initiating the end-to-end certificate-based key establishment procedure.

3.6.4 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.

3.6.5 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.

3.6.6 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.

3.6.7 event: Interaction or occurrence related to and detected by the oneM2M system.

3.6.8 event categories: Set of indicators that specify the treatment of events for differentiated handling, based on policies.

3.7 F

3.7.1 field domain: Consists of M2M devices, M2M gateways, sensing and actuation (S&A) equipment and M2M area networks.

3.8 G

3.8.1 M2M gateway: Physical equipment that includes, at minimum, the entities and application programming interfaces (APIs) of a middle node.

3.8.2 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

3.10.1 identification [b-ISO/IEC 24760-1]: 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.

3.10.2 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.

3.10.3 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".

3.10.4 information model: Abstract, formal representation of entities that may include their properties, relationships and the operations that can be performed on them.

3.10.5 infrastructure domain: Consists of application infrastructure and M2M service infrastructure.

3.10.6 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.

3.10.7 inner primitive: oneM2M primitive being secured by end-to-end security for primitives.

3.10.8 integrity [b-ISO/IEC 27001], [b-ISO/IEC 27002]: Safeguarding the accuracy and completeness of information and processing methods.

3.10.9 interworking proxy application entity (IPE): Specialized AE that facilitates 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

3.12.1 key [b-NIST SP800-57 Part 1]: 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

3.13.1 LWM2M client [b-OMA OMA-TS-LightweightM2M]: Application that manages and controls things that are represented as LWM2M objects.

3.13.2 LWM2M client endpoint name [b-OMA OMA-TS-LightweightM2M]: Identifier for a LWM2M client.

3.13.3 LWM2M object [b-OMA OMA-TS-LightweightM2M]: LWM2M representation of a thing. LWM2M objects are identified through a universal resource identifier (URI).

3.13.4 LWM2M server [b-OMA OMA-TS-LightweightM2M]: Application that manages and controls LWM2M clients.

3.14 M

3.14.1 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.

3.14.2 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.

3.14.3 mutual authentication [b-ISO/IEC 9798-1]: Entity authentication that provides both entities with assurance of each other's identity.

3.15 N

3.15.1 network operator: Entity (e.g., a company) that operates an underlying network.

3.15.2 node: Logical entity that is identifiable in the oneM2M system.

3.16 O

3.16.1 oneM2M system: System developed by the oneM2M global initiative that enables deployable M2M solutions.

3.16.2 outer primitive: Primitive used to transport an inner primitive secured using end-to-end security of primitives.

3.17 P

3.17.1 privacy [b-ITU-T X.800]: 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.

3.17.2 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

3.19.1 registrar: Legal entities that will directly interface with App developers seeking App-IDs and can assign unique IDs.

3.19.2 remote security provisioning: Process of providing a credential into a secure environment of a node deployed in the field.

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

NOTE – This definition applies to the security context only.

3.19.4 role-based access control (RBAC) [b-ISO/IEC 27001]: Permissions attributed to an access control role granting access to an object.

3.20 S

3.20.1 secure [b-ISO/IEC TR 15443-1]: 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.

3.20.2 security [b-IETF RFC 4949]: System condition that results from the establishment and maintenance of measures to protect the system.

3.20.3 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.

3.20.4 security association establishment: Procedure for establishing a security association between two entities (CSEs and/or AEs).

3.20.5 security pre-provisioning: Process of providing a credential into a secure environment of the node prior to device deployment, e.g., during manufacturing.

3.20.6 (oneM2M) security principal: CSE or AE or node or M2M device which can be authenticated.

NOTE – When the security principal is a node or M2M device, then node or M2M device is acting on behalf of the CSE and/or AE executing on the node or M2M device.

3.20.7 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 into the device and target entity the security credentials that will be used for mutual authentication.

3.20.8 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.

3.20.9 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.

3.20.10 M2M service: Consists of one or more M2M application services and one or more M2M common services.

3.20.11 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.

3.20.12 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.

3.20.13 M2M service operational status of a M2M device: Indicates whether the M2M service is currently running for this device.

3.20.14 M2M service provider: Entity (e.g., a company) that provides M2M common services to a M2M application service provider or to the user.

3.20.15 M2M service subscriber: One of the M2M stakeholders that subscribes to M2M service(s).

3.20.16 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.

3.20.17 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.

3.20.18 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.

3.20.19 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.

3.20.20 static device/gateway context: Static metrics, which may impact the M2M operations of M2M devices/gateways.

3.21 T

3.21.1 time series data: Sequence of data points which typically consist of successive measurements made over a time interval.

3.21.2 thing: Element which is individually identifiable in the oneM2M system.

3.21.3 trust [b-ISO/IEC 13888-1]: 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

3.22.1 underlying network: Functions, networks, busses and other technology assisting in data transport connectivity services.

3.22.2 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

3.23.1 verification [b-ISO/IEC 27004]: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

3.23.2 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 and acronyms

This Recommendation lists the following abbreviations and acronyms:

4.1 0-9

Void.

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	BroadBand 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

oneM2M Specification update and maintenance control procedure

(This annex forms an integral part of this Recommendation.)

The provisions of Annex L in [ITU-T Y.4500.1] regarding the oneM2M specification update and maintenance control procedure shall apply to this Recommendation.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCIT applications*.

[b-ISO/IEC 9798-1] ISO/IEC 9798-1:2010, *Information technology – Security techniques – Entity authentication – Part 1: General*.
https://www.iso.org/standard/53634.html

[b-ISO/IEC 13888-1] ISO/IEC 13888-1:2009, *Information technology – Security techniques – Non-repudiation – Part 1: General*.
https://www.iso.org/standard/50432.html

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: terminology and concepts*.
https://www.iso.org/standard/57914.html

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology - Security techniques – Information security management systems - Requirements*.
https://www.iso.org/standard/42103.html

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.
https://www.iso.org/standard/50297.html

[b-ISO/IEC 27004] ISO/IEC 27004:2009, *Information technology – Security techniques – Information security management – Measurement*.
https://www.iso.org/standard/42106.html

[b-ISO/IEC TR 15443-1] ISO/IEC TR 15443-1:2012, *Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts*.
https://www.iso.org/standard/59138.html

[b-IEEE 802.15.4] IEEE 802.15.4-2003, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).*
https://standards.ieee.org/findstds/standard/802.15.4-2003.html

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet Security Glossary, Version 2*.
https://tools.ietf.org/html/rfc4949

[b-NIST SP800-57 Part 1] NIST SP800-57 Part 1 (2012), *Recommendation for Key Management – General, Rev3*.
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-3/archive/2012-07-10

[b-OMA OMA-TS-LightweightM2M] OMA OMA-TS-LightweightM2M-V1_0-20141111-D: *Lightweight Machine to Machine Technical Specification*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018