International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4500.2

(05/2018)

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 – Requirements

Recommendation ITU-T Y.4500.2

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.4500.2

oneM2M – Requirements

Summary

Recommendation ITU-T Y.4500.2 provides an informative functional role model and normative technical requirements for oneM2M.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4500.2	2018-05-06	20	11.1002/1000/13499

Keywords

Charging, communication, LWM2M interworking, oneM2M, operational, overall system, requirement, security, semantics.

* 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/.

Table of Contents

Recommendation ITU-T Y.4500.2

oneM2M – Requirements

1 Scope

The present Recommendation contains an informative functional role model and normative technical requirements for oneM2M.

The Recommendation contains oneM2M Release 2 specification – oneM2M Requirements V2.7.1 and is equivalent to standards of oneM2M partners including ARIB, ATIS [b-ATIS.oneM2M.TS0002V2.7.1], CCSA, ETSI [b-ETSI TS 118 102], TIA, TSDSI, TTA [b-TTA.oneM2M.TS0002V2.7.1] and TTC [b-TTC.oneM2M.TS0002V2.7.1].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4500.11] Recommendation ITU-T Y.4500.11 (2018), *oneM2M – Common terminology*.

[ETSI TS 122 368] ETSI TS 122 368, *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for Machine-Type Communications (MTC); Stage 1 (3GPP TS 22.368).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application entity (AE) [ITU-T Y.4500.11]: Represents an instantiation of application logic for end-to-end M2M solutions.

3.1.2 common services entity (CSE) [ITU-T Y.4500.11]: 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AE Application Entity

API Application Programming Interface

CMDH Communication Management and Delivery Handling

CPU	Central Processing Unit
DM	Device Management
GBA	Generic Bootstrapping Architecture
GSMA	Global System for Mobile communications Association
GW	Gateway
HGI	Home Gateway Initiative
HSM	Hardware Security Module
IP	Internet Protocol
LWM2M	Lightweight M2M
M2M	Machine to Machine
MTC	Machine Type Communications
OMA	Open Mobile Alliance
OSR	Overall System Requirements
OWL	Web Ontology Language
QoS	Quality of Service
RDF	Resource Description Framework
SMS	Short Message Service
UICC	Universal Integrated Circuit Card
USIM	UMTS Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WLAN	Wireless Local Area Network

5 Conventions

The keywords "shall", "shall not", "should", "should not", "may", "need not" in the present Recommendation are to be interpreted as described:

Shall/Shall not:

Requirements

1) effect on this Recommendation: The Recommendation needs to describe the required feature (i.e., specify a technical solution for the Requirement);
2) effect on products: every implementation (M2M solution that complies to this Standard) must support it;
3) effect on deployments: every deployment (M2M service based on this Standard) must use the Standardized feature where applicable – otherwise e.g., interoperability problems with other services could arise.

Should/Should not:

Recommendation

1) effect on this Recommendation: The Recommendation needs to describe a solution that allows the presence and the absence of the feature;

2) effect on products: an implementation may or may not support it, however support is recommended;

3) effect on deployments: a deployment may or may not use it, however usage is recommended.

May/Need not:

Permission/Option

1) effect on this Recommendation:The Recommendation needs to describe a solution that allows the presence and the absence of the required feature;

2) effect on products: an implementation may or may not support it;

3) effect on deployments: a deployment may or may not use it.

6 Introduction to the M2M ecosystem

6.1 Functional roles description

Figure 1 shows functional roles in the machine to machine (M2M) ecosystem.

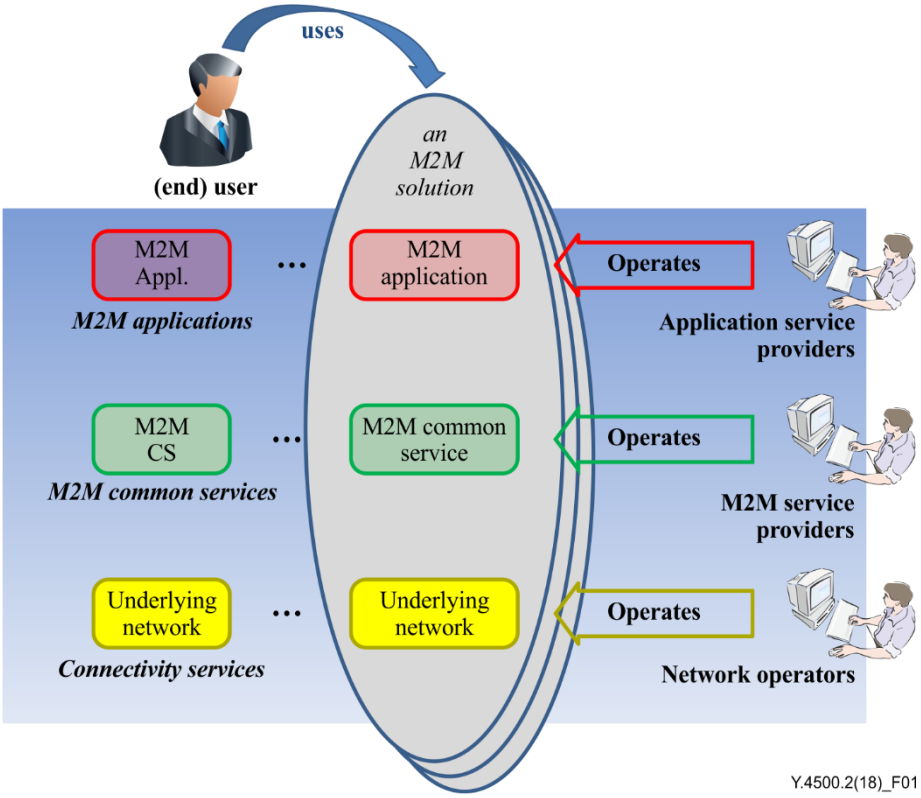

Figure 1 – Functional roles in the M2M ecosystem

1) The *user* (individual or company – aka: end-user) fulfils all of the following criteria:
   – Uses an M2M solution.

2) The *application service provider* fulfils all of the following criteria:
   – Provides an M2M application service.
   – Operates M2M applications.

3) The *M2M service provider* fulfils all of the following criteria:
   – Provides M2M services to application service providers.
   – Operates M2M common services.

4) The *network operator* fulfils all of the following criteria:

- Provides *connectivity* and related services for *M2M service providers.*
- Operates an *underlying network*. Such an underlying network could e.g., be a telecom network.

Any of the above functional roles may coincide with any of the other roles. These functional roles do not imply business roles or architectural assumptions.

7 Functional requirements (normative)

7.1 Overall system requirements

Table 1 – Overall system requirements

Requirement ID	Description
OSR-001	The oneM2M system shall allow communication between M2M applications by using multiple communication means based on Internet protocol (IP) access.
OSR-002a	The oneM2M system shall support communication means that can accommodate devices with constrained computing such as a small central processing unit (CPU), memory, battery, or communication capabilities such as 2G wireless modem or certain wireless local area network (WLAN) nodes.
OSR-002b	The oneM2M system shall support communication means that can accommodate devices with rich computing capabilities (e.g., large CPU, memory) or communication (e.g., 3/4G wireless modem, wireline).
OSR-003	The oneM2M system shall support the ability to maintain application-to-application communication in coordination with an application session for those M2M applications that require it.
OSR-004	The oneM2M system shall support session-less application communications for those M2M applications that require it.
OSR-005	The oneM2M system shall be able to expose the services offered by telecommunications networks to M2M applications such as short message service (SMS), unstructured supplementary service data (USSD), localization, subscription configuration, authentication (e.g., generic bootstrapping architecture), etc., subject to restrictions based on the network operator's policy.
OSR-006	The oneM2M system shall be able to reuse the services offered by underlying networks to M2M applications and/or M2M services by means of open access models such as Open Mobile Alliance (OMA), Global System for Mobile communications Association (GSMA) OneAPI framework).Examples of available services are: • IP multimedia communications. • Messaging. • Location. • Charging and billing services. • Device information and profiles. • Configuration and management of devices. • Triggering, monitoring of devices. • Small data transmission. • Group management. (see Note 1).
OSR-007	The oneM2M system shall provide a mechanism for M2M applications to interact with the applications and data/information managed by a different M2M service provider, subject to permissions as appropriate.

Table 1 – Overall system requirements

Requirement ID	Description
OSR-008	The oneM2M system shall provide the capability for M2M applications to communicate with an M2M device (i.e., application in the device) without the need for the M2M applications to be aware of the network technology and the specific communication protocol of the M2M device.
OSR-009	The oneM2M system shall support the ability for single or multiple M2M applications to interact with a single or multiple M2M devices/gateways (application in the device/gateway) (see Note 2).
OSR-010	The oneM2M system shall support mechanisms for confirmed delivery of a message to its addressee to those M2M applications requesting reliable delivery to dectect failure of message within a given time interval.
OSR-011a	The oneM2M system shall be able to request different communication paths, from the underlying network based on underlying network operator and/or M2M service provider policies, routing mechanisms for transmission failures.
OSR-011b	The oneM2M system shall be able to request different communication paths from the underlying network based on request from M2M applications.
OSR-012	The oneM2M system shall support communications between M2M applications and M2M devices supporting M2M services by means of continuous or non-continuous connectivity.
OSR-013	The oneM2M system shall be aware of the delay tolerance acceptable by the M2M application and shall schedule the communication accordingly or request the underlying network to do it, based on policies criteria.
OSR-014	The oneM2M system shall be able to communicate with M2M devices, behind an M2M gateway that supports heterogeneous M2M area networks.
OSR-015	The oneM2M system shall be able to assist underlying networks that support different communication patterns including infrequent communications, small data transfer, transfer of large file and streamed communication.
OSR-016	The oneM2M system shall provide the capability to notify M2M applications of the availability of, and changes to, available M2M application/management information on the M2M device/gateway, including changes to the M2M area network.
OSR-017	The oneM2M system shall be able to offer access to different sets of M2M services to M2M application providers. The minimum set of services are: • connectivity management; • device management (service level management); • application data management. In order to enable different deployment scenarios, these services shall be made available by the oneM2M system, individually, as a subset or as a complete set of services.
OSR-018	The oneM2M system shall be able to offer M2M services to M2M devices roaming across cellular underlying networks, subject to restriction based on network operator's policy (see Note 3).
OSR-019	The oneM2M system shall support the capabilities for data repository (i.e., to collect/store) and for data transfer from one or more M2M devices or M2M gateways, for delivery to one or more M2M gateways, M2M services infrastructure, or M2M application infrastructure, in ways requested by the M2M application infrastructure as listed below: • action initiated either by an M2M device, M2M gateway, M2M services infrastructure, or M2M application infrastructure; • when triggered by schedule or event;

Table 1 – Overall system requirements

Requirement ID	Description
	• for specified data.
OSR-020	The oneM2M system shall be able to support policies and their management regarding the aspects of storage and retrieval of data/information.
OSR-021	The oneM2M system shall be able to provide mechanisms to enable sharing of data among multiple M2M applications.
OSR-022	When some of the components of a M2M solution are not available (e.g., WAN connection lost), the oneM2M system shall be able to support the normal operation of components of the M2M solution that are available.
OSR-023	The oneM2M system shall be able to identify the M2M services to be used by M2M service subscriptions (see Note 4).
OSR-024	The oneM2M system shall be able to identify the M2M devices used by M2M service subscriptions.
OSR-025	The oneM2M system shall be able to identify the M2M applications used by M2M service subscriptions.
OSR-026	If provided by the underlying network, the oneM2M system shall be able to associate the M2M device used by M2M service subscriptions with the device identifiers offered by the underlying network and the device.
OSR-027	The oneM2M system shall provide a generic mechanism to support transparent exchange of information between the M2M application and the underlying network, subject to restriction based on M2M service provider's policy and/or network operator's policy (see Note 5).
OSR-028	The oneM2M system shall enable an M2M application to define trigger conditions in the oneM2M system such that the oneM2M system autonomously sends a series of commands to actuators on behalf of the M2M application when these contitions are met.
OSR-029	The oneM2M system shall be able to support sending common command(s) to each actuator or sensor via a group.
OSR-030	The oneM2M system shall be able to support the management (i.e., addition, removal, retrieval and update) of the membership of a group.
OSR-031	The oneM2M system shall be able to support a group as a member of another group.
OSR-032	The oneM2M system shall be able to support event categories (e.g., normal, urgency) associated with data for M2M applications when collecting, storing and reporting that data (see Note 6).
OSR-033	Based on the dynamic device/gateway context of the M2M gateway and/or device and the defined event categories, the oneM2M system shall provide the capability to dynamically adjust the scheduling of reporting and notification of the M2M device/gateway (see Note 17).
OSR-034	The oneM2M system shall support seamless replacement of M2M devices as well as M2M gateways (e.g., redirecting traffic, connection, recovery, etc.).
OSR-035	The oneM2M system shall support the exchange of non-M2M application related relevant information (e.g., device/gateway classes) between M2M device/gateway and M2M service infrastructure for the purpose of efficient communication facilitation. This includes the capability for an M2M device to report its device class to M2M service infrastructure and for the M2M service infrastructure to inform M2M device of the M2M service infrastruture capabilities.
OSR-036	The oneM2M system should provide mechanisms to accept requests from M2M application service providers for compute/analytics services.

Table 1 – Overall system requirements

Requirement ID	Description
OSR-037	The oneM2M system shall enable an M2M application to request to send data, in a manner independent of the underlying network, to the M2M applications of a group of M2M devices and M2M gateways in geographic areas that are specified by the M2M application.
OSR-038	The oneM2M system shall support the inclusion of M2M application's QoS preference in service requests to underlying networks.
OSR-039	The oneM2M system shall be able to authorize service requests with QoS preference at service level, but shall pass M2M application's QoS preference in service requests to underlying network for authorization and granting or negotiation of the service QoS requests.
OSR-040	The oneM2M system shall be able to leverage multiple communication mechanisms (such as USSD or SMS) when available in the underlying networks.
OSR-041	The oneM2M system shall provide a mechanism, which supports the addition of new M2M services to the oneM2M system as independent portable modules by means of the oneM2M interfaces.
OSR-042	The oneM2M system shall be able to support different QoS-levels specifying parameters, such as guaranteed bitrate, delay, delay variation, loss ratio and error rate, etc.
OSR-043	The oneM2M system shall be able to verify that members of a group support a common set of functions.
OSR-044	The oneM2M system shall support communication with M2M devices which are reachable based on defined time schedules (e.g., periodic) as well as M2M devices which are reachable in an unpredictable and spontaneous manner.
OSR-045a	The oneM2M system shall be able to receive and utilize information provided by the underlying network about when an M2M device can be reached.
OSR-045b	The oneM2M system shall be able to utilize reachability schedules generated by either the M2M device or the infrastructure domain.
OSR-046	The oneM2M system shall be able to support a capability for the M2M application to request/disallow acknowledgement for its communication.
OSR-047	The oneM2M system shall be able to support mechanism for the M2M devices and/or gateways to report their geographical location information to M2M applications (see Note 7).
OSR-048	The oneM2M system shall provide an M2M service that allows M2M devices and/or gateways to share their own or other M2M devices' geographical location information (see Note 7).
OSR-049	The oneM2M system shall be able to provide the capability for an M2M application to selectively share data (e.g., access control) among applications.
OSR-050	If communication over one communication channel provided by the underlying network can only be triggered by one side (infrastructure domain or field domain), and alternative channel(s) is (are) available in the other direction, the oneM2M system shall be able to use the alternative channel(s) to trigger bidirectional communication on the first channel.
OSR-051	Depending on availability of suitable interfaces provided by the underlying network the oneM2M system shall be able to request the underlying network to broadcast/multicast data to a group of M2M devices in a specified area.
OSR-052	The oneM2M system shall be able to select an appropriate underlying network to broadcast or multicast data depending on the network's broadcast/multicast support and

Table 1 – Overall system requirements

Requirement ID	Description
	the connectivity supported by the targeted group of M2M devices/gateways.
OSR-053	The oneM2M system shall provide a means that enables backward compatibility of interfaces among different releases (see Note 8).
OSR-054	The oneM2M system shall be able to support an M2M application, M2M device, or M2M gateway to obtain access to resources of another M2M application, M2M device, or M2M gateway.
OSR-055	The oneM2M system shall be able to provide the capability of M2M applications to exchange data with one or more authorized M2M applications which are not known in advance.
OSR-056	The oneM2M system shall enable discovery of usable M2M applications on an M2M gateway or at an M2M device.
OSR-057	The oneM2M system shall enable discovery of M2M gateways and M2M devices available to an M2M application for data exchange.
OSR-058	The oneM2M system shall be able to provide time stamps as needed by common service functions.
OSR-059	The oneM2M system shall be able to support role-based access control based on M2M service subscriptions.
OSR-060	The oneM2M system should support time synchronization with an external clock source.
OSR-061	M2M devices and M2M gateways may support time synchronization within the oneM2M system.
OSR-062	The oneM2M system shall enable means of testing the connectivity towards a set of M2M applications.
OSR-063	The oneM2M system shall be able to manage the scheduling of M2M service layer connectivity and messaging between the infrastracture domain and M2M devices/gateways.
OSR-064	The oneM2M system shall be able to aggregate messages depending on message delay tolerance and/or category.
OSR-065	The oneM2M system shall provide mechanisms that enable a M2M service provider to distribute processing functions to his M2M devices/gateways in the field domain
OSR-066	The oneM2M system shall be able to support the placement and operation of M2M applications in selected M2M nodes per criteria requested by M2M application service providers, subject to access rights.
OSR-067	The oneM2M system shall be able to take operational and management action as requested by M2M applications.
OSR-068	When available from an underlying network, the oneM2M system shall be able to provide the capability to retrieve and report the information regarding whether an M2M device is authorized to access underlying network services.
OSR-069	When available from the underlying network, the oneM2M system shall be able to maintain the M2M service operational status of a M2M device and update it when the underlying network connectivity service status changes.
OSR-070	The oneM2M system shall be able to provide the capability to notify an authorized M2M application when the M2M service administrative state or M2M service operational status of an M2M device changes, if that M2M application has subscribed for such notifications.

Table 1 – Overall system requirements

Requirement ID	Description
OSR-071	The oneM2M system shall be able to enable an authorized M2M application to set the M2M service administrative state of a M2M device.
OSR-072	The oneM2M system shall be able to initiate a set of well-defined actions (e.g., trigger upon a threshold, compare a value, etc.) to one or more M2M application(s) on behalf of another M2M application.
OSR-073	The oneM2M system shall support distributed transactions to multiple devices or applications where the transaction includes the characteristics of atomicity, consistency, isolation and durability.
OSR-074	The oneM2M system shall support the completion of distributed transactions to multiple devices or applications while maintaining the order of the operations and performing the transaction within a given time frame.
OSR-075	The oneM2M system shall be able to collect, store time series data.
OSR-076	The oneM2M system shall be able to detect and report the missing data in time series.
OSR-077	The oneM2M system shall be capable of collecting asynchronous responses pertaining to the broadcasted messages.
OSR-078	The oneM2M system shall support gateway-based capabilities for event management, e.g., capability for arbitration of the resulting processing.
OSR-079	The oneM2M system shall provide the capability to notify a device hosting a group of applications when alternative registration points for that group of applications are available (e.g., via different underlying networks) based on the service requirements of each of the applications hosted.
OSR-080	The oneM2M system shall provide the capability to register applications in group or independently, based on their service requirements.
OSR-081	The oneM2M system shall be able to collect data that is broadcast (e.g., in industrial bus systems) according to data collection policies.
OSR-082	The oneM2M system shall allow the update, modification, or deletion of data collection policies within an M2M application.
OSR-083	The oneM2M system shall be able to filter information from oneM2M devices for a given set of parameters.
OSR-084	The oneM2M system shall be able to handle an event notification from an authorized M2M application which triggers actions to be performed on the M2M device (example: Turn on or off the monitoring).
OSR-085	The oneM2M system shall support resource caching of registered M2M devices. Resource caching is a mechanism through which the oneM2M system retains resources of a registered M2M device in temporarily inactive state by moving the resources to a temporary storage e.g., cache bin.
OSR-086	The oneM2M system shall enable M2M gateways to discover M2M infrastructure nodes and M2M devices available for data exchange.
OSR-087	The oneM2M system shall enable M2M infrastructure nodes and M2M device to discover M2M gateways available for data exchange.
OSR-088	The oneM2M system shall be able to support the capabilities for data repository (i.e., to collect/store) and for data transfer among authorized M2M devices and M2M gateways via M2M area networks without involvement of the infrastructure domain.
OSR-089	The oneM2M system shall enable the cancellation of continuous data collection and/or the deletion of collected data when pre-defined conditions are met.

Table 1 – Overall system requirements

Requirement ID	Description
OSR-090	The oneM2M system shall be able to forward the M2M application data to M2M application without storing the data.
OSR-091	The oneM2M system shall be able to notify interested oneM2M entities when it detects forwarded M2M application data was not delivered within expected time duration.
OSR-092	The oneM2M system shall provide the capability for monitoring and describing data streams with associated attributes e.g., data freshness, accuracy, sampling rate, data integrity.
OSR-093	The oneM2M system shall support transaction management to multiple devices or applications providing policy based mechanism that should be invoked (e.g., keep status, re-schedule, rollback) depending on the outcome of the desired operation.
OSR-094	The oneM2M system shall provide Information Model(s) to support interoperability among different devices/applications.
OSR-095	The oneM2M system should provide mappings between different information models from non-oneM2M system(s).
OSR-096	The oneM2M system should be able to interwork with non-oneM2M system(s).
OSR-097	The oneM2M system shall be able to share data collection policies among multiple M2M devices/gateways within an M2M application service, or among different M2M application services.
OSR-098	The oneM2M system shall be able to support machine socialization functionalities (such as existence discovery, correlated task discovery, message interface discovery and process optimization for multiple machines with same tasks).
NOTE 1 – The set of features or application programming interfaces (APIs) to be supported depends on the M2M common services and access to available APIs. NOTE 2 – The relation M2M network application to M2M device/gateway may be 1:1, 1:n, n:1 and/or n:m. NOTE 3 – No roaming on M2M service level is assumed by this requirement. NOTE 4 – M2M service subscriptions are not application subscriptions (e.g., Home energy management). NOTE 5 – Transparent exchange of information implies information that is mainly interpreted by the M2M application and the underlying network provider. NOTE 6 – Based on the event categories and via interworking with underlying networks, the oneM2M system can support differentiated services (by providing quality-of-service) requested by M2M applications. NOTE 7 – Geographical location information can be more than simply longitude, latitude and geo-fence event. NOTE 8 – "means" above does not imply only technical mechanisms, e.g., there is no protocol version negociation. NOTE 9 – In Rel-1 only GBA and localization are available. NOTE 10 – Rel-1 covers: Location, charging and billing services, configuration and management of devices, device information and profiles, triggering. NOTE 11 – This requirement applies to M2M devices but not to devices interworked via M2M area networks. NOTE 12 – Based on device triggering. NOTE 13 – No support for streamed communication. NOTE 14 – Limitations to trigger (via Tsp interface) devices in a roamed-to network. NOTE 15 – Detail syntax to describe dynamic context is not specified. NOTE 16 – It is possible to deliver CoAP over SMS, but currently SMS message delivery interfaces are not expicitely defined.	

Table 1 – Overall system requirements

Requirement ID	Description
NOTE 17 – For example, if the battery of a gateway remains at only 10% or below, the gateway notifies the M2M service platform of the status. The M2M application in the infrastructure node will adjust the scheduling of reporting and notification based on the event categories associated with each message. Consequently, the M2M gateway operates longer. NOTE 18 – Void. NOTE 19 – Only the M2M service administrative state can be notified. M2M service operational status is not implemented. NOTE 20 – This can be implemented based on preconfigured access rights. NOTE 21 – In Rel-1 this is supported by means of the Mca interfaces, mapping the new service module to an AE. NOTE 22 – In Rel-2 data are stored in the common services entity (CSE) but never get retrieved by other entities except by subscribe/notify mechanism.	

7.2 Management requirements

Table 2 – Management requirements

Requirement ID	Description
MGR-001	The oneM2M system shall be able to support management and configuration of M2M gateways/devices including resource constrained M2M devices.
MGR-002	The oneM2M system shall provide the capability to discover the M2M area networks including information about devices on those networks and the parameters (e.g., topology, protocol) of those networks.
MGR-003	The oneM2M system shall be able to provide the capability to maintain and describe the management information model of devices and parameters (e.g., topology, protocol) of M2M area networks.
MGR-004	The oneM2M system shall support common means to manage devices enabled by different management technologies (e.g., OMA DM, BBF TR069).
MGR-005	The oneM2M system shall provide the capability to manage multiple devices in a grouped manner.
MGR-006	The oneM2M system shall provide the capability for provisioning and configuration of devices in M2M area networks.
MGR-007	The oneM2M system shall provide the capability for monitoring and diagnostics of M2M gateways/devices in M2M area networks.
MGR-008	The oneM2M system shall provide the capability for software management of devices in M2M area networks.
MGR-009	The oneM2M system shall provide the capability for rebooting and/or resetting of M2M gateways/devices and other devices in M2M area networks.
MGR-010	The oneM2M system shall provide the capability for authorizing devices to access M2M area networks.
MGR-011	The oneM2M system shall provide the capability for modifying the topology of devices in M2M area networks,subject to restriction based on M2M area network policies.
MGR-012	Upon detection of a new device the M2M gateway shall be able to be provisioned by the M2M service infrastructure with an appropriate configuration which is required to handle the detected device.
MGR-013	Void.

Table 2 – Management requirements

Requirement ID	Description
MGR-014	The oneM2M system shall be able to retrieve events and information logged by M2M gateways/devices and other devices in M2M area networks.
MGR-015	The oneM2M system shall be able to support firmware management (e.g., update) of M2M gateways/devices and other devices in M2M area networks.
MGR-016	The oneM2M system shall be able to retrieve information related to the static and dynamic device/gateway context for M2M gateways/devices as well as device context for other devices in M2M area networks.
MGR-017	The oneM2M system shall be capable of correlating access management elements provided by the technology specific device management protocols to access management elements used by the oneM2M system.
MGR-018	The M2M service infrastructure shall be able to accept standardized configuration settings from an external configuration server to allow the M2M devices to register.
MGR-019	The M2M device shall be able to accept standardized configuration settings from an external configuration server in order to register to the oneM2M system.
NOTE – In Rel-1 no detection mechanism exists, but once an M2M device is known at the gateway it can be configured via the GW through DM.	

7.3 Semantics requirements

7.3.1 Ontology related requirements

Table 3 – Ontology requirements

Requirement ID	Description
ONT-001	The M2M system shall support a standardized format for the rules/policies used to define service logic.
ONT-002	The M2M system shall support modelling semantic descriptions of things (including relationships among them) by using ontologies.
ONT-003	The M2M system shall support a common modeling language for ontologies (e.g., OWL).
ONT-004	The M2M system should be able to provide translation capabilities from different modeling languages for ontologies to the language adopted by oneM2M if the expressiveness of the imported ontology allows.
ONT-005	The M2M System shall provide the capability to retrieve semantic descriptions and ontologies stored outside of the M2M System.
ONT-006	The M2M system shall provide support for linking ontologies defined in the context of the M2M system with ontologies defined outside this context.
ONT-007	The M2M system shall be able to support extending ontologies in the M2M system.
ONT-008	The M2M system shall be able to use ontologies that contain concepts representing aspects (e.g., a room) that are not represented by resources of the M2M system.
ONT-009	The M2M system shall be able to re-use common ontologies (e.g., location, time ontologies, etc.) which are commonly used in M2M applications.
ONT-010	The M2M system shall be able to support simultaneous usage of multiple ontologies for the same M2M resource.
ONT-011	The M2M system shall provide the capability for making ontology available in the M2M system, e.g., through announcement.

Table 3 – Ontology requirements

Requirement ID	Description
ONT-012	The M2M system shall be able to support mechanisms to import external ontologies into the M2M system.
ONT-013	The M2M system shall be able to support update of ontologies.
ONT-014	The M2M system shall enable functions for data conversion based on ontologies.
ONT-015	The M2M system shall be able to model devices based on ontologies which may be available outside the M2M system (e.g., HGI device template).
ONT-016	The M2M system shall support storage, management and discovery of ontologies.
ONT-017	The oneM2M system shall support a semantic relation ("Is Paired To") between two M2M devices.

7.3.2 Semantics annotation requirements

Table 4 – Semantics annotation requirements

Requirement ID	Description
ANN-001	The oneM2M system shall provide capabilities to manage semantic information about the oneM2M resources, e.g., create, retrieve, update, delete, associate/link.
ANN-002	The oneM2M system shall support a common language for semantic description, e.g., resource description framework (RDF).
ANN-003	The oneM2M system shall support semantic annotation of oneM2M resources for example application related data contained in containers.
ANN-004	The oneM2M system shall support semantic annotation based on related ontologies.
ANN-005	The oneM2M system shall provide the capability for making semantic descriptions available in the M2M system, e.g., announcement.
ANN-006	The oneM2M system shall enable applications to retrieve an ontology representation related to semantic information used in the M2M system.
ANN-007	The oneM2M system shall provide capabilities to manage data quality descriptions of resource.

7.3.3 Semantics query requirements

Table 5 – Semantics query requirements

Requirement ID	Description
QRY-001	The oneM2M system shall provide capabilities to discover M2M resources based on semantic descriptions.

7.3.4 Semantics mashup requirements

Table 6 – Semantics mashup requirements

Requirement ID	Description
MSH-001	The oneM2M system shall provide the capability to host processing functions for mash-up.
MSH-002	The oneM2M system shall enable M2M applications to provide processing functions for mash-up.

Table 6 – Semantics mashup requirements

Requirement ID	Description
MSH-003	The oneM2M system itself may provide pre-provisioned or dynamically created processing functions for mash-up.
MSH-004	The oneM2M system shall be able to create and execute mash-ups based on processing functions.
MSH-005	The oneM2M system shall be able to expose mash-ups as resources e.g., virtual devices.

7.3.5 Semantics reasoning requirements

Table 7 – Semantics reasoning requirements

Requirement ID	Description
RES-001	The oneM2M system shall be able to update ontologies as a result of the ontology reasoning.
RES-002	The oneM2M system shall be able to support semantic reasoning e.g., ontology reasoning or semantic rule-based reasoning.
RES-003	The oneM2M system shall be able to support adding and updating semantic information based on semantic reasoning.

7.3.6 Data analytics requirements

Table 8 – Data analytics requirements

Requirement ID	Description
ANA-001	The oneM2M system shall be able to support capabilities (e.g., processing function) for performing M2M data analytics based on semantic descriptions from M2M applications and /or from the M2M system.
ANA-002	The oneM2M system shall provide the capability of interpreting and applying service logic (e.g., rules/policies of triggering operations upon other resources or attributes according to the change of the monitored resource) described with semantic annotation and ontology.
ANA-003	The oneM2M system shall support a standardized format for the rules/policies used to define service logic.

7.4 Security requirements

Table 9 – Security requirements

Requirement ID	Description
SER-001	The oneM2M system shall incorporate protection against threats to its availability such as denial of service attacks.
SER-002	The oneM2M system shall be able to ensure the confidentiality of data.
SER-003	The oneM2M system shall be able to ensure the integrity of data.

Table 9 – Security requirements

Requirement ID	Description
SER-004	In case where the M2M devices support UMTS subscriber identity module (USIM)/ universal integrated circuit card (UICC) and the underlying networks support network layer security, the oneM2M system shall be able to leverage device's USIM/UICC credentials and network's security capability e.g., 3GPP GBA for establishing the M2M services and M2M applications level security through interfaces to underlying network.
SER-005	In case where the M2M devices support USIM/UICC and the underlying networks support network layer security, and when the oneM2M system is aware of underlying network's bootstrapping capability e.g., 3GPP GBA, the oneM2M system shall be able to expose this capability to M2M services and M2M applications through API.
SER-006	In case where the M2M devices support USIM/UICC and the underlying networks support network layer security, the oneM2M system shall be able to leverage device's USIM/UICC credentials when available to bootstrap M2M security association.
SER-007	When some of the components of an M2M solution are not available (e.g., WAN connection lost), the oneM2M system shall be able to support the confidentiality and the integrity of data between authorized components of the M2M solution that are available.
SER-008	The oneM2M system shall support countermeasures against unauthorized access to M2M services and M2M application services.
SER-009	The oneM2M system shall be able to support mutual authentication for interaction with underlying networks, M2M services and M2M application services.
SER-010	The oneM2M system shall be able to support mechanisms for protection against misuse, cloning, substitution or theft of security credentials.
SER-011	The oneM2M system shall protect the use of the identity of an M2M stakeholder within the oneM2M system against discovery and misuse by other stakeholders.
SER-012	The oneM2M system shall be able to support countermeasures against impersonation attacks and replay attacks.
SER-013	The oneM2M system shall be able to provide the mechanism for integrity-checking on boot, periodically on run-time, and on software upgrades for software/hardware/firmware component(s) on M2M device(s).
SER-014	The oneM2M system shall be able to provide configuration data to an authenticated and authorized M2M application in the M2M gateway/device.
SER-015	The oneM2M system shall be able to support mechanisms to provide M2M service subscriber identity to authorized and authenticated M2M applications when the oneM2M system has the M2M service subscriber's consent.
SER-016	The oneM2M system shall be able to support non repudiation within the M2M service layer and in its authorized interactions with the network and application layers.
SER-017	The oneM2M system shall be able to mitigate threats. NOTE – Example of threats are identified in oneM2M TR-0008 [b-oneM2M TR-0008].
SER-018	The oneM2M system shall enable an M2M stakeholder to use a resource or service and be accountable for that use without exposing its identity to other stakeholders.
SER-019	The oneM2M system shall be able to use service-level credentials present inside the M2M device for establishing the M2M services and M2M applications level security.
SER-020	The oneM2M system shall enable legitimate M2M service providers to provision their own credentials into the M2M devices/gateways.
SER-021	The oneM2M system shall be able to remotely and securely provision M2M security credentials in M2M devices and/or M2M gateways.
SER-022	The oneM2M system shall enable M2M application service providers to authorize

Table 9 – Security requirements

Requirement ID	Description
	interactions involving their M2M applications on supporting entities (e.g., devices/ gateways/service infrastructure).
SER-023	Where a hardware security module (HSM) is supported, the oneM2M system shall be able to rely on the HSM to provide local security.
SER-024	The oneM2M system shall enable M2M applications to use different and segregated security environments.
SER-025	The oneM2M system shall be able to prevent unauthorized M2M stakeholders from identifying and/or observing the actions of other M2M stakeholders in the oneM2M system, e.g., access to resources and services (see Note 1).
SER-026	The oneM2M system shall be able to provide mechanism for the protection of confidentiality of the geographical location information (see Note 2).
SER-027	The M2M system shall support grouping of M2M applications that have the same access control rights towards one specific resources, together so that access control validation can be performed by validating if the M2M application is a member of certain group.
SER-028	The oneM2M system shall enable security protocol end-points to protect portions of individual application-generated data so that intermediate entities (whether trusted or untrusted) forwarding the data are unable to access the protected portions of the data in clear text.
SER-029	The oneM2M system shall enable security protocol end-points to protect portions of individual application-generated data so that security protocol end-points can detect modification, including modification by intermediate service layer entities (whether trusted or untrusted) forwarding the data.
SER-030	The oneM2M system shall enable security protocol end-points to protect portions of individual oneM2M messages so that intermediate entities (whether trusted or untrusted) forwarding the messages are unable to access the protected portions of the messages in clear text.
SER-031	The oneM2M system shall enable security protocol end-points to protect portions of individual oneM2M messages so that security protocol end-points can detect modification, including modification by intermediate service layer entities (whether trusted or untrusted) forwarding the messages.
SER-032	The oneM2M system shall enable security protocol end-points to establish security sessions which are used for protecting portions of one or more oneM2M messages so that intermediate entities (whether trusted or untrusted) forwarding the messages are unable to access the protected portions of the messages in clear text.
SER-033	The oneM2M system shall enable security protocol end-points to establish security sessions which are used for protecting portions of one or more oneM2M messages so that security protocol end-points can detect modification, including modification by intermediate service layer entities (whether trusted or untrusted) forwarding the messages.
SER-034	The oneM2M system shall enable security protocol end-points to protect portions of messages or data so that intermediate entities (whether trusted or untrusted) forwarding the messages or data are unable to access the protected portions of messages or data in clear text.
SER-035	The oneM2M system shall enable security protocol end-points to protect portions of messages or data so that security protocol end-points can detect modification, including modification by intermediate service layer entities (whether trusted or untrusted) forwarding the messages or data.

Table 9 – Security requirements

Requirement ID	Description
SER-036	The oneM2M system shall enable security protocol end-points to authenticate each other without relying on intermediate service layer entities (whether trusted or untrusted).
SER-037	The oneM2M system shall be able to support distributed authorization functions for making access control decisions, providing access control policies and providing authorization attributes (e.g., roles).
SER-038	The oneM2M system shall be able to expose an interoperable interface to provide access control policies by means of specified access control policy language.
SER-039	The oneM2M system shall enable individuals to establish policies for controlling access to their personal identifiable information even when it may have been collected without their knowledge.
SER-040	When the M2M devices are grouped and the M2M gateway is authorized as delegate of the group for accessing the M2M server, the M2M gateway shall be able to, on behalf of the M2M devices in the group, perform mutual authentication with the M2M server.
SER-041	When the M2M devices are grouped and the M2M gateway belongs to a third party, oneM2M System shall be able to protect security and privacy of communication between individual M2M device and M2M server from other M2M devices and the third party M2M gateway.
SER-042	A secured API shall enable application and service layer entities to make use of sensitive functions and data residing within the Secure Environment, independently of the technical implementation of the Secure Environment.
SER-043	The oneM2M system shall enable authorizing a oneM2M entity to temporarily delegate its access rights (or a subset thereof) to another authorized oneM2M entity, wherein the dynamically delegated access rights shall not enable the "delegated-to" oneM2M entity to delegate the same rights in turn to a third oneM2M entity.
SER-044	For M2M application service data, that are processed by an M2M application B in a M2M entity (e.g., M2M gateway) on its path from an originator A to the recipient M2M application C, the oneM2M system shall provide means that enable the recipient to verify both: • integrity of the data received by the M2M application B from the originator A; and, at the same time: • that the M2M application B that has processed the data has not been compromised.
SER-045	The oneM2M system shall support classification of application data by M2M applications into various security levels that are specified by oneM2M and support the mapping of these levels to applicable security capabilities.
SER-046	The oneM2M system shall enable to protect portions of individual application generated data that is at-rest (e.g., hosted data) for integrity protection and data creator authentication.
SER-047	The oneM2M system shall enable to protect portions of individual application data at-rest (e.g., hosted data) for confidentiality protection.
SER-048	The oneM2M system shall ensure that the end-to-end data credentials are protected for confidentiality, integrity and against tampering.
SER-049	The oneM2M system shall ensure that the end-to-end data credentials are protected from exposure to intermediate entities.
SER-050	The oneM2M system shall enable pre-defined conditions to be protected from unauthorized modification.
SER-051	The oneM2M system shall enable the deletion of M2M data produced/stored by the M2M devices/gateways based on request from an authorized entity.

Table 9 – Security requirements

Requirement ID	Description
SER-052	The oneM2M system shall store and process privacy preferences in an interoperable manner.
SER-053	The oneM2M system shall support privacy profiles at various levels to care for conditions of legal requirements, manufacturers, and data subjects.
SER-054	The oneM2M system shall be able to prioritize privacy profiles where there is a conflict between profiles (legal profile takes priority over data subject profile, for example).
SER-055	The oneM2M system shall be able to support configuration of security related settings of its infrastructure side components by a privileged user through standardized API.
SER-056	The oneM2M system shall allow overriding of security settings by a privileged user through standardized API.
SER-057	The oneM2M system shall support a mechanism enabling addition/deletion of information enabling authentication of oneM2M entities through standardized API.
SER-058	The oneM2M system shall enable delegation of security functions (e.g., message authentication/integrity protection) of an entity to a trust-worthy entity.
SER-059	The oneM2M system shall protect the authenticity, integrity and confidentiality of the representation of the delegated access rights.
SER-060	The oneM2M system shall be able to revoke the representation of the delegated access rights.
SER-061	The oneM2M system shall be able to verify the App-ID to support the detection of impersonation or to support revocation.
SER-062	The oneM2M system shall be able to reuse the privacy policy of the underlying network.
SER-063	The oneM2M system shall be able to share its privacy policy with the underlying network.
NOTE 1 – The above requirement does not cover items outside of the oneM2M system, e.g., underlying networks. NOTE 2 – Geographical location information can be more than simply longitude and latitude. NOTE 3 – Partly supported for impersonation attacks not supported for replay attacks. NOTE 4 – The oneM2M system has no means to verify a subscriber's consent. This requirement is only fulfillable at application level. NOTE 5 – Regarding remote provisioning, Release 1 supports remote provisioning of symmetric key credentials only.	

7.5 Charging requirements

Table 10 – Charging requirements

Requirement ID	Description
CHG-001	The oneM2M system shall support collection of charging specific information related to the individual services facilitated by the oneM2M system (e.g., data management, device management and/or connectivity management). Collection of charging specific information shall be possible concurrent with the resource usage.The format of the recorded information shall be fully specified including mandatory and optional elements.

Requirement ID	Description
CHG-002	The oneM2M system shall support mechanisms to facilitate correlation of charging information (e.g., of a User) collected for M2M services, M2M application services and services provided by underlying network operators.
CHG-003	The oneM2M system shall provide means to coordinate charging data records for data usages with differentiated QoS from the underlying network.
CHG-004	The oneM2M System shall be able to utilize existing charging mechanisms of Underlying Networks.
CHG-005	The oneM2M system shall support transfer of the charging information records to the billing domain of the M2M service provider, for the purpose of: • subscriber billing; • inter-provider billing; • provider-to-subscriber accounting including additional functions like statistics.
CHG-006	The oneM2M system should support generation of charging events for the purpose of requesting resource usage authorization from the real time credit control system where the subscriber account is located. The information contained in the charging events and the relevant chargeable events shall be fully specified including mandatory and optional elements (see Note 1).
NOTE 1 – A chargeable event is any activity, a provider may want to charge for that utilizes the resources and related M2M services offered by such provider. A charging event is the set of charging information needed by the credit control system for resource authorization. NOTE 2 – Information collected can be sent to the underlying networks which may used it for charging. NOTE 3 – The oneM2M service layer can pass info to underlying networks but cannot use Underlying Network mechanism. Charging can be done by underlying network. This is covered by CHG-002. NOTE 4 – Only supported in the Infrastructure Node.	

7.6 Operational requirements

Table 11 – Operational requirements

Requirement ID	Description
OPR-001	The oneM2M system shall provide the capability for monitoring and diagnostics of M2M applications.
OPR-002	The oneM2M system shall provide the capability for software management of M2M applications.
OPR-003	The oneM2M system shall be able to configure the execution state an M2M application (start, stop, restart).
OPR-004	When suitable interfaces are provided by the underlying network, the oneM2M system shall have the ability to schedule traffic via the underlying network based on instructions received from the underlying network.
OPR-005	The oneM2M system shall be able to exchange information with M2M applications related to usage and traffic characteristics of M2M devices or M2M gateways by the M2M application. This should include support for the 3GPP feature called: "Time controlled" [ETSI TS 122 368]. (see NOTE).
OPR-006	Depending on availability of suitable interfaces provided by the underlying network the oneM2M system shall be able to provide information related to usage and traffic characteristics of M2M devices or M2M gateways to the underlying network.
OPR-007	The oneM2M system shall be able to support receipt of the status information of the underlying network if supported by the underlying network.
OPR-008	The oneM2M system shall be able to provide the M2M applications with status information received from the underlying network.

Table 11 – Operational requirements

Requirement ID	Description
OPR-009	The format for registered App-IDs shall be able to support use by people and systems to readily determine whether the App-ID is registered and the registration authority which issued the App-ID, App developer and App name.
OPR-010	The oneM2M system registration authorities shall be able to collect and maintain supporting required information when assigning an App-ID.
NOTE – "Time controlled" is equivalent to the MTC features specified in clause 7.2 of 3GPP TS 22.368 [ETSI TS 122 368].	

7.7 Communication management requirements

Table 12 – Communication management requirements

Requirement ID	Description
CMR-001	The oneM2M system shall provide to M2M applications a communication service which provides buffering of messages to/from M2M gateway/device/ infrastructure domain.
CMR-002	The oneM2M system shall be able to support forwarding buffered messages depending on communication policies and based on service preference associated with the buffered messages.
CMR-003	The oneM2M system shall enable an M2M application to send a communication request with the following service preference: • QoS parameters, including delay tolerance, for initiating the delivery of data; • categorizing communication requests into different levels of priority or QoS classes.
CMR-004	The oneM2M system shall be able to support concurrent processing of messages within M2M gateways and/or M2M devices from different sources with awareness for the service preference associated with the messages while observing the provisioned communication policies.
CMR-005	The oneM2M system shall be able to maintain context associated with M2M sessions (e.g., security context or network connectivity context during the interruption of the session).
CMR-006	The oneM2M system shall support the ability for applications to categorize requested communications (priority, importance, etc.), so that the oneM2M system can adapt its actual communications (scheduling, aggregation, compression, etc.) by taking this categorization into account.
CMR-007	The oneM2M system shall support configurable communication policies that will define its communication patterns. Such policies shall take into account information received from the underlying network (such as information referred to in OPR-004) as well as information received from the applications (such as the information referred to in OPR-005 or categorization of communications requested by the applications).
CMR-008	The oneM2M system shall support data aggregation based on communication policies when exchanging data between the M2M gateway/device/infrastructure domain.
CMR-009	The oneM2M system should support data compression based on communication policies when exchanging data between the M2M gateway/device/infrastructure domain.
CMR-010	The oneM2M system shall support an additional randomized delay of communications, based on communication policies, when exchanging data between the M2M gateway/device/infrastructure domain.

Table 12 – Communication management requirements

Requirement ID	Description
CMR-011	The oneM2M system shall be able to monitor its own usage of the underlying networks over given periods of time: attempted communications, failed attempts and successful attempts.
CMR-012	The oneM2M system shall be able to restrict its own usage of the underlying networks, based on communication policies and on its monitored usage of them, when exchanging data between the M2M gateway/device/infrastructure domain.
CMR-013	The oneM2M system shall be able to refrain from using its own usage of the underlying networks, based on a time-based back-off procedure configurable in communication policies, when exchanging data between the M2M gateway/device/infrastructure domain.
CMR-014	The oneM2M system shall be able to restrict its own usage of the underlying networks, based on communication policies and on the date and time, when exchanging data between the M2M gateway/device/infrastructure domain.
CMR-015	The oneM2M system shall be able to identify a series of data (e.g., time series data) and indicate individual data belonging to this series.
NOTE 1 – Long lived security context and registration is covered, M2M sessions are not covered. NOTE 2 – Communication management and delivery handling (CMDH) policies (application side) is implemented, information from the underlying network can be utilized but the method for provisioning via Mcn is not covered.	

7.8 LWM2M interworking requirements

Table 13 – LWM2M interworking requirements

Requirement ID	Description
LWM2M-001	The oneM2M system shall provide the capability to transparently transport LWM2M objects between LWM2M clients and M2M applications.
LWM2M-002	The oneM2M system shall provide the capability to translate LWM2M objects into a semantic representation of the LWM2M object as oneM2M resources.
LWM2M-003	The oneM2M system shall provide the capabilities of the LWM2M server in order to interwork between LWM2M clients and M2M applications.
LWM2M-004	The oneM2M system shall provide the capability for M2M applications to discover LWM2M clients using the LWM2M client's endpoint name.
LWM2M-005	When transparently transporting LWM2M objects, the oneM2M system shall provide the capability for M2M applications to discover the definion of LWM2M objects transported by the oneM2M system.
LWM2M-006	When interworking with LWM2M objects, the oneM2M system shall provide the capability for M2M applications to discover a LWM2M object using the LWM2M object's identifier.
LWM2M-007	The oneM2M system shall provide capability to onboard devices that incorporate a LWM2M client.
LWM2M-008	The oneM2M system shall provide the capability to interoperate the underlying security mechanisms of the LWM2M client with the security capabililities provided by the oneM2M system.

8 Non-functional requirements (informative)

This clause is intended to gather high-level principles and guidelines that shall govern the design of the oneM2M system. Such principles and guidelines are fundamental to the design of the oneM2M system. But as they cannot necessarily be expressed as requirements per se, they shall be introduced and expressed in this clause.

Table 14 – Non-functional requirements

Requirement ID	Description
NFR-001	Continua Health Alliance (CHA) is incorporating a RESTful approach to its design. To support CHA, oneM2M should consider RESTful styles and approaches while designing the M2M architecture.
NFR-002	The oneM2M system should communicate using protocols that are efficient in terms of amount of exchanged information over amount of exchanged data measured in bytes.

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 oneM2M Specification update and maintenance control procedure shall apply to this Recommendation.

Bibliography

[b-oneM2M TR-0008] oneM2M Technical Report TR-0008, *Security*.

[b-ATIS.oneM2M.TS0002V2.7.1] ATIS oneM2M.TS0002V2.7.1(2016), *Requirements*.
https://www.atis.org/docstore/product.aspx?id=28325

[b-ETSI TS 118 102] ETSI TS 118 102 v2.7.1 (2016), *oneM2M Requirements*.
www.etsi.org/deliver/etsi_ts/118100_118199/118102/02.07.01_60/ts_118102v020701p.pdf

[b-TTA.oneM2M.TS0002V2.7.1] TTC oneM2M.TS0002V271(2016), *Requirements*.
http://www.tta.or.kr/data/ttas_view.jsp?rn=1&rn1=Y&rn2=&rn3=&nowpage=1&pk_num=TTAT.MMTS.0002+v2.7.1&standard_no=TTAT.MMTS.0002+v2.7.1&kor_standard=&publish_date=&section_code=&order=publish_date&by=desc&nowSu=1&totalSu=1&acode1=&acode2=&scode1=&scode2=

[b-TTC.oneM2M.TS0002V2.7.1] TTC oneM2M.TS0002V271(2016), *Requirements*.
www.ttc.or.jp/jp/document_list/pdf/j/TS/TS-M2M-0002v2.7.1.pdf

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