ETSI TS 118 102 V2.10.2 (2020-03)

oneM2M;
Requirements
(oneM2M TS-0002 version 2.10.2 Release 2A)

Reference
RTS/oneM2M-000002v2A

Keywords
IoT, M2M, requirements

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

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

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

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

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.2] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[i.3] oneM2M TR-0008: "Security".

[i.4] BBF TR-069 (November 2013): "CPE WAN Management Protocol" Issue: 1 Amendment 5.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 118 111 [i.2] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 118 111 [i.2] and the following apply:

AE	Application Entity
API	Application Program Interface
BBF	BroadBand Forum
CHA	Continua Health Alliance
CMDH	Communication Management and Delivery Handling
CPU	Central Processing Unit
CSE	Common Services Entity
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
MTC	Machine Type Communications
OEM	Original Equiment Manufacturer
OMA	Open Mobile Alliance
OSR	Overall System Requirements
OWL	Web Ontology Language
QoS	Quality of Service
RDF	Resource Description Framework
SIM	Subscriber Identity Module
SMS	Short Message Service
TPM	Trusted Platform Module
UICC	Universal Integrated Circuit Card
USIM	UMTS Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WLAN	Wireless Local Area Network

4 Conventions

The keywords "shall", "shall not", "should", "should not", "may", "need not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

NOTE: According to oneM2M Drafting Rules [i.1] in order to mandate a feature in the oneM2M System but allow freedom to the individual deployment whether to use it or not subsequently requirements are often formulated like:

- "The oneM2M System ***shall*** **support a mechanism** [function, capability...] **to** …"; or
- "…***shall*** **be able to** …".

This does not mandate usage of the required feature in a M2M Solution.

5 Introduction to the M2M ecosystem

5.1 Functional roles description

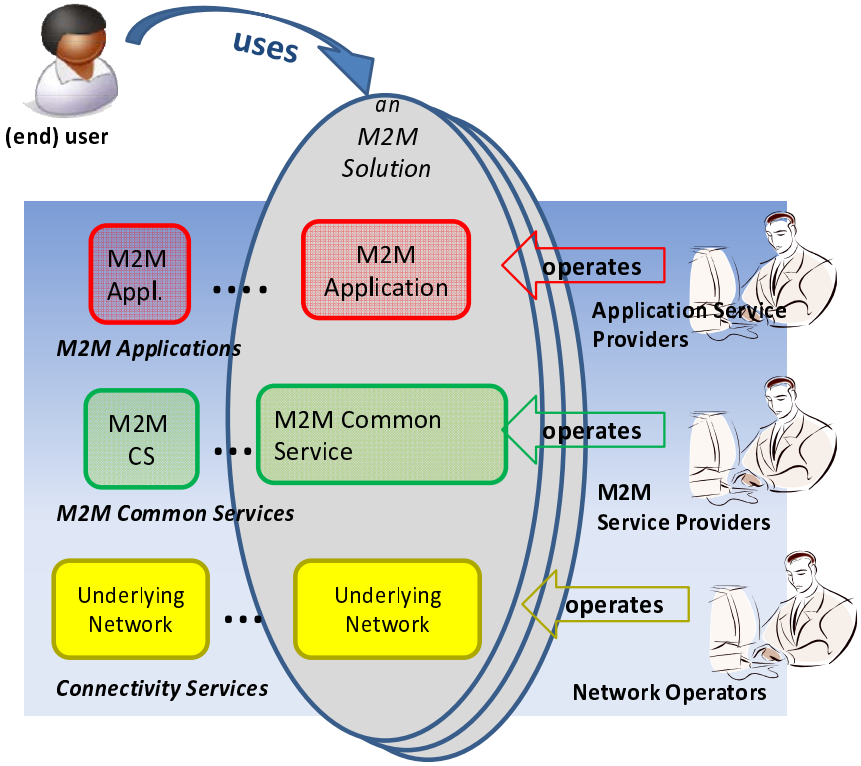

Figure 1: Functional Roles in the M2M Ecosystem

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.

6 Functional Requirements

6.1 Overall System Requirements

Table 1: Overall System Requirements

Requirement ID	Description	Release
OSR-001	The oneM2M System shall allow communication between M2M Applications by using multiple communication means based on IP access.	Implemented in Rel-1
OSR-002a	The oneM2M System shall support communication means that can accommodate devices with constrained computing (e.g. small CPU, memory, battery) or communication capabilities (e.g. 2G wireless modem, certain WLAN node).	Implemented in Rel-1
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).	Implemented in Rel-1
OSR-003 See REQ-2015-0626R01	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.	Not implemented
OSR-004	The oneM2M System shall support session-less application communications for those M2M Applications that require it.	Implemented in Rel-1
OSR-005	The oneM2M System shall be able to expose the services offered by telecommunications networks to M2M Applications (e.g. SMS, USSD, localization, subscription configuration, authentication (e.g. Generic Bootstrapping Architecture), etc.),subject to restriction based on Network Operator's policy.	Partially implemented (see note 9)
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 (e.g. OMA, 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).	Partially implemented (see note 10)
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.	Implemented in Rel-1
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.	Implemented in Rel-1 (see note 11)
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).	Implemented in Rel-1
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 detect failure of message within a given time interval.	Implemented in Rel-1
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.	Implemented in Rel-1 (see note 12)
OSR-011b	The oneM2M System shall be able to request different communication paths from the Underlying Network based on request from M2M Applications.	Not implemented
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.	Implemented in Rel-1

Requirement ID	Description	Release
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.	Implemented in Rel-1
OSR-014	The oneM2M System shall be able to communicate with M2M Devices, behind an M2M Gateway that supports heterogeneous M2M Area Networks.	Implemented in Rel-1
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.	Partially implemented (see note 13)
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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).	Implemented with some limitations (see note 14)
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; • for specified data.	Implemented in Rel-1
OSR-020	The oneM2M System shall be able to support policies and their management regarding the aspects of storage and retrieval of data/information.	Implemented in Rel-1
OSR-021	The oneM2M System shall be able to provide mechanisms to enable sharing of data among multiple M2M Applications.	Implemented in Rel-1
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.	Implemented in Rel-1
OSR-023	The oneM2M System shall be able to identify the M2M Services to be used by M2M Service Subscriptions (see note 4).	Implemented in Rel-1
OSR-024	The oneM2M System shall be able to identify the M2M Devices used by M2M Service Subscriptions.	Implemented in Rel-1
OSR-025	The oneM2M System shall be able to identify the M2M Applications used by M2M Service Subscriptions.	Implemented in Rel-1
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.	Implemented in Rel-1
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).	Not implemented
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 conditions are met.	Not implemented
OSR-029	The oneM2M System shall be able to support sending common command(s) to each actuator or sensor via a group.	Implemented in Rel-1
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.	Implemented in Rel-1
OSR-031	The oneM2M System shall be able to support a group as a member of another group.	Implemented in Rel-1
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).	Implemented in Rel-1

Requirement ID	Description	Release
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).	Partially implemented (see note 15)
OSR-034	The oneM2M System shall support seamless replacement of M2M Devices as well as M2M Gateways (e.g. redirecting traffic, connection, recovery, etc.).	Not implemented
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 Infrastructure capabilities.	Not implemented
OSR-036	The oneM2M System should provide mechanisms to accept requests from M2M Application Service Providers for compute/analytics services.	Not implemented
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.	Not implemented
OSR-038	The oneM2M System shall support the inclusion of M2M Application's QoS preference in service requests to Underlying Networks.	Not implemented
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.	Not implemented
OSR-040	The oneM2M System shall be able to leverage multiple communication mechanisms (such as USSD or SMS) when available in the Underlying Networks.	Not implemented (see note 16)
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.	Partially implemented (see note 21)
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.	Not implemented
OSR-043	The oneM2M System shall be able to verify that members of a group support a common set of functions.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Not implemented
OSR-045b	The oneM2M System shall be able to utilize reachability schedules generated by either the M2M Device or the Infrastructure Domain.	Implemented in Rel-2
OSR-046	The oneM2M System shall be able to support a capability for the M2M Application to request/disallow acknowledgement for its communication.	Not implemented
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).	Implemented in Rel-1
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).	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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 the connectivity supported by the targeted group of M2M Devices/Gateways.	Not implemented

Requirement ID	Description	Release
OSR-053	The oneM2M System shall provide a means that enables backward compatibility of interfaces among different releases (see note 8).	Not implemented
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.	Implemented in Rel-1
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.	Implemented in Rel-1 (see note 20)
OSR-056	The oneM2M System shall enable discovery of usable M2M Applications on an M2M Gateway or at an M2M Device.	Implemented in Rel-1
OSR-057	The oneM2M System shall enable discovery of M2M Gateways and M2M Devices available to an M2M Application for data exchange.	Implemented in Rel-1
OSR-058	The oneM2M System shall be able to provide time stamps as needed by Common Service Functions.	Implemented in Rel-1
OSR-059	The oneM2M System shall be able to support Role-Based Access Control based on M2M Service Subscriptions.	Implemented in Rel-1
OSR-060	The oneM2M System should support time synchronization with an external clock source.	Not implemented
OSR-061	M2M Devices and M2M Gateways may support time synchronization within the oneM2M System.	Not implemented
OSR-062	The oneM2M System shall enable means of testing the connectivity towards a set of M2M Applications.	Not implemented
OSR-063	The oneM2M System shall be able to manage the scheduling of M2M Service Layer connectivity and messaging between the Infrastructure Domain and M2M Devices/Gateways.	Implemented in Rel-1
OSR-064	The oneM2M System shall be able to aggregate messages depending on message delay tolerance and/or category.	Implemented in Rel-1
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.	Not implemented
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.	Implemented in Rel-1
OSR-067	The oneM2M System shall be able to take operational and management action as requested by M2M Applications.	Implemented in Rel-1
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.	Not implemented
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.	Not implemented
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.	Partially implemented (see note 19)
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.	Implemented in Rel-1
OSR-072	The oneM2M System shall be able to initiate a set of actions defined by a M2M Application (e.g. trigger upon a threshold, compare a value) that impacts another Application.	Not implemented
OSR-073 See REQ-2015-0529R03	The oneM2M System shall support distributed transactions to multiple devices or applications where the transaction includes the characteristics of atomicity, consistency, isolation and durability.	Not implemented
OSR-074 See REQ-2015-0529R03	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.	Not implemented
OSR-75 See REQ-2015-0546R01	The oneM2M System shall be able to collect, store Time Series Data.	Implemented in Rel-2
OSR-76 See REQ-2015-0546R01	The oneM2M System shall be able to detect and report the missing data in time series.	Implemented in Rel-2

Requirement ID	Description	Release
OSR-077 See REQ-2015-0558R01	The oneM2M System shall be capable of collecting asynchronous responses pertaining to the broadcasted messages.	Not implemented
OSR-078 See REQ-2015-573R01	The oneM2M System shall support gateway-based capabilities for Event management, e.g. capability for arbitration of the resulting processing.	Not implemented
OSR-079 See REQ-2015-574R01	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.	Not implemented
OSR-080 See REQ-2015-574R01	The oneM2M System shall provide the capability to register applications in group or independently, based on their service requirements.	Not implemented
OSR-081 See REQ-2015-0553R02	The oneM2M System shall be able to collect data that is broadcast (e.g. in industrial bus systems) according to data collection policies.	Not implemented
OSR-082 See REQ-2015-0553R02	The oneM2M System shall allow the update, modification, or deletion of data collection policies within an M2M Application.	Not implemented
OSR-083 See REQ-2015-0593R02	The oneM2M System shall be able to filter information from oneM2M Devices for a given set of parameters.	Not implemented
OSR-084 See REQ-2015-0595R04	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).	Not implemented
OSR-085 See REQ-2015-0608	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.	Not implemented
OSR-086 See REQ-2015-0611R02	The oneM2M System shall enable M2M Gateways to discover M2M Infrastructure Nodes and M2M Devices available for data exchange.	Implemented in Rel-1
OSR-087 See REQ-2015-0611R02	The oneM2M System shall enable M2M Infrastructure Nodes and M2M Device to discover M2M Gateways available for data exchange.	Implemented in Rel-1
OSR-088 See REQ-2015-0611R02	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 by only involving the field domain.	Implemented in Rel-1
OSR-089 See REQ-2015-0620	The oneM2M System shall enable the cancellation of continuous data collection and/or the deletion of collected data when pre-defined conditions are met.	Not implemented
OSR-090 See REQ-2015-0622R02	The oneM2M System shall be able to forward the M2M Application Data to M2M Application without storing the Data.	Partially implemented (see note 22)
OSR-091 See REQ-2015-0622R02	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.	Not implemented
OSR-092 See REQ-2015-0629	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.	Not implemented
OSR-093 See REQ-2015-0630	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.	Not implemented
OSR-094 See REQ-2015-0631R02	The oneM2M System shall provide Information Model(s) to support interoperability among different devices/applications.	Implemented in Rel-2
OSR-095 See REQ-2015-0631R02	The oneM2M System should provide mappings between different Information Models from non-oneM2M System(s).	Not implemented
OSR-096 See REQ-2015-0631R02	The oneM2M System should be able to interwork with non-oneM2M System(s).	Implemented in Rel-2

Requirement ID	Description	Release
OSR-097 See REQ-2015-0583R01	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.	Not implemented
OSR-098 See REQ-2016-0055R02	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).	Not implemented
OSR-099 See REQ-2016-0066R01	The oneM2M system shall enable continuity of services to M2M devices as they move across various geographic points in the oneM2M System(s).	Implemented in Rel-3
OSR-100 See REQ-2017-0006R02	The oneM2M system shall allow use of multiple communication methods (protocol bindings, serializations, and versions) between M2M Devices/Gateways and M2M application services.	
OSR-101 See REQ-2017-0008R02	The oneM2M System shall enable discovery of M2M Application Servers, M2M Management Servers and M2M Devices available to an M2M Gateway for data exchange.	
OSR -102 See REQ-2017-0008R02	The oneM2M System shall enable discovery of M2M Gateways available to a M2M Management Server and an M2M Device for data exchange.	
OSR-103 See REQ-2017-0008R02	The oneM2M System shall be able to 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 via M2M Area Network without any assistance or instruction of M2M Management Servers and M2M Application Serve.	
OSR-104 See REQ-2017-0008R02	Upon request from M2M Application Server, an M2M Gateway shall enable functions that pre-process (e.g. average) M2M data before providing them to the recipient.	Not Implemented
OSR -105 See REQ-2017-0008R02	Upon request, an M2M Gateway shall enable functions that erase M2M data (e.g. that have been sent or could not be sent to the recipient within a certain time) based on criteria from an M2M Application Server.	Not Implemented
OSR-106 See REQ-2017-0008R02	An M2M Gateway and/or an M2M Device shall be able to broadcast the need to receive/deliver specific data.to otherM2M Devices and/or M2M Gateways.	Not Implemented
OSR -107 See REQ-2017-0008R02	The oneM2M system shall enable M2M Gateways and/or M2M Devices to establish a connection to each other if able to receive/deliver the specific data.	Not Implemented
OSR-108 See REQ-2017-0008R02	The oneM2M System shall enable M2M Gateways to set conditions used for processing jointly group/aggregate data subscriptions to reduce the number of messages to M2M Devices and distribute the resulting notifications according to the set conditions.	Implemented in Rel-3
OSR -109 See REQ-2017-0008R02	The oneM2M System shall enable M2M Gateways to distribute notifications according to how data subscriptions have been grouped/aggregated.	Implemented in Rel-3
OSR-110 See REQ-2017-0008R02	The oneM2M System shall enable subscriptions to changes to multiple data sources (e.g. oneM2M resources) which aim to generate data publication (i.e. automatic notifications) if and only if the expected changes to each of those multiple resources occur concurrently.	Implemented in Rel-3
OSR-111 See REQ-2017-0018R01	The oneM2M system shall be able to support heterogeneous identification services, the recognition of external identification systems and converting an object identifier to a compatible identifier recognized by the oneM2M system.	
OSR-112 See REQ-2017-0030R05	The oneM2M System shall enable the M2M Application to configure the notification interval in the M2M Devices.	Implemented in Rel-1
OSR-113 See REQ-2017-0030R05	The oneM2M System shall support communication between the Infrastructure Domainand M2M devices either directly or via a gateway.	Implemented in Rel-1
OSR-114 See REQ-2017-0030R05	The oneM2M System shall enable exchange of information between M2M applications via the Infrastructure Domain.	Implemented in Rel-1
OSR-115 See REQ-2017-0030R05	The oneM2M system shall be able to support service requests from M2M applications for communication with QoS requirement e.g. higher delivery priority, reliable delivery.	Partially Implemented
OSR-116 See REQ-2017-0030R05	The oneM2M system shall be able to support requests with time expiration or geography restriction.	Implemented in Rel-2

Requirement ID	Description	Release
OSR-117 See REQ-2017-0030R05	The oneM2M System shall support setting the configuration for Geo-Fence based location services by a M2M Application.	Implemented in Rel-2
OSR-118 See REQ-2017-0031R05	The oneM2M System shall enable exchanges of diagnostic data periodically between M2M Devices and the Infrastructure Domain.	Rel-3/future releases
OSR-119 See REQ-2017-0031R05	The oneM2M system shall support a mechanism to describe the syntax and semantics format of the diagnostics data exchanged between the M2M Devices and the InfrastructureDomain.	Rel-3/future releases?
OSR-120 See REQ-2017-0031R05	The oneM2M System shall be able to provide the service capability for location based services.	Implemented
OSR-121 See REQ-2017-0031R05	The oneM2M System shall be able to provide the service capability supporting Over The Air management.	Implemented
OSR-122 See REQ-2017-0031R05	The oneM2M system shall provide the capability for an M2M Device to maintain registration with multiple entities simultaneously.	Rel-3/future releases?
OSR-123 See REQ-2017-0031R05	The oneM2M System shall enable exchange of information with the intended vehicles by unicast, multicast and/or broadcast.	Partially Implemented (see note 23)
OSR-124 See REQ-2017-0031R05	The oneM2M System shall be able to transfer time critical information. For example for feeding back current road states to automatic driving control, the feedback time should be less than a few seconds (the distance between vehicles normally corresponds to a few seconds) to avoid unnecessary speed down/stop of following vehicles (see note 24).	Rel-3/future releases?
OSR-125 See REQ-2017-0031R05	The oneM2M System shall be able to guarantee its reliability in order to receive/feedback messages from/to related M2M Devices (e.g. for Vehicular Domain) (see note 24).	Rel-3/future releases?
OSR-126 See REQ-2017-0031R05	The oneM2M System shall enable sharing of service information between devices/GWs based on proximity (see note 24).	Rel-3/future releases?
OSR-127 See REQ-2017-0031R05	The oneM2M System shall enable sending and receiving of service information between devices/GWs with minimized interruption (see note 24).	Rel-3/future releases?
OSR-128 See REQ-2017-0031R05	The oneM2M System shall support mobile/portable M2M Gateway and/or Device.	Rel-3/future releases?
OSR-129 See REQ-2017-0031R05	The oneM2M System shall support triggering M2M Devices for on-demand reporting regarding collected data.	Rel-3/future releases?
OSR-130 See REQ-2017-0031R05	The oneM2M System shall enable the M2M Infrastructure to facilitate direct communication between two or more different M2M devices without having registered with one another.	Rel-3/future releases?
OSR-131 See REQ-2017-0031R05	The oneM2M System shall be able to verify geographical location information from moving objects regardless of information accuracy.	Rel-3/future releases?
OSR-132 See REQ-2017-0031R05	The oneM2M System shall be able to verify time synchronization.	Rel-3/future releases?
OSR-133 See REQ-2017-0031R05	The oneM2M System shall be able to coordinate end-to-end reliable communications for applications that can have safety impacts.	Rel-3/future releases?

Requirement ID	Description	Release
NOTE 1: The set of features or 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 negotiation.		
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 explicitly defined.		
NOTE 17: For example, if the battery of Gateway is remained 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 CSE but never get retrieved by other entities except by subscribe/notify mechanism.		
NOTE 23: Unicast communications have been implemented in Release 1.		
NOTE 24: Definition of “real time” and how to specify timing and reliability requirements is TBD.		

6.2 Management Requirements

Table 2: Management Requirements

Requirement ID	Description	Release
MGR-001	The oneM2M System shall be able to support management and configuration of M2M Gateways/ Devices including resource constrained M2M Devices.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
MGR-004	The oneM2M System shall support common means to manage devices enabled by different management technologies (e.g. OMA DM, BBF TR-069 [i.4]).	Implemented in Rel-1
MGR-005	The oneM2M System shall provide the capability to manage multiple devices in a grouped manner.	Implemented in Rel-1
MGR-006	The oneM2M System shall provide the capability for provisioning and configuration of devices in M2M Area Networks.	Implemented in Rel-1
MGR-007	The oneM2M System shall provide the capability for monitoring and diagnostics of M2M Gateways/Devices in M2M Area Networks.	Implemented in Rel-1
MGR-008	The oneM2M System shall provide the capability for software management of devices in M2M Area Networks.	Implemented in Rel-1
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.	Implemented in Rel-1
MGR-010	The oneM2M System shall provide the capability for authorizing devices to access M2M Area Networks.	Implemented in Rel-1

Requirement ID	Description	Release
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.	Implemented in Rel-1
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.	Partially implemented (see note)
MGR-013	Void.	
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
MGR-018 See REQ-2015-0555R02	The M2M Service Infrastructure shall be able to accept standardized configuration settings from an external configuration server to allow the M2M Devices to register.	Not implemented
MGR-019 See REQ-2015-0555R02	The M2M Device shall be able to accept standardized configuration settings from an external configuration server in order to register to the oneM2M System.	Not implemented
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.		

6.3 Semantics Requirements

6.3.1 Ontology Related Requirements

Table 3: Ontology Requirements

Requirement ID	Description	Release
ONT-001 See REQ-2015-0521R01	The M2M System shall support a standardized format for the rules/policies used to define service logic.	Not implemented
ONT-002 See REQ-2015-0521R01	The M2M System shall support modelling semantic descriptions of Things (including relationships among them) by using ontologies.	Implemented in Rel-2
ONT-003 See REQ-2015-0521R01	The M2M System shall support a common modelling language for ontologies (e.g. OWL).	Implemented in Rel-2
ONT-004 See REQ-2015-0521R01	The M2M System should be able to provide translation capabilities from different modelling languages for ontologies to the language adopted by oneM2M if the expressiveness of the imported ontology allows.	Not implemented
ONT-005 See REQ-2015-0521R01	The M2M System shall provide the capability to retrieve semantic descriptions and ontologies stored outside of the M2M System.	Not implemented
ONT-006 See REQ-2015-0521R01	The M2M System shall provide support for linking ontologies defined in the context of the M2M System with ontologies defined outside this context.	Not implemented
ONT-007 See REQ-2015-0521R01	The M2M System shall be able to support extending ontologies in the M2M System.	Not implemented
ONT-008 See REQ-2015-0521R01	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.	Implemented in Rel-2
ONT-009 See REQ-2015-0521R01	The M2M System shall be able to re-use common ontologies (e.g. location, time ontologies, etc.) which are commonly used in M2M Applications.	Not implemented

Requirement ID	Description	Release
ONT-010 See REQ-2015-0521R01	The M2M System shall be able to support simultaneous usage of multiple ontologies for the same M2M resource.	Implemented in Rel-2
ONT-011 See REQ-2015-0521R01	The M2M System shall provide the capability for making ontology available in the M2M System, e.g. through announcement.	Not implemented
ONT-012 See REQ-2015-0521R01	The M2M System shall be able to support mechanisms to import external ontologies into the M2M System.	Not implemented
ONT-013 See REQ-2015-0521R01	The M2M System shall be able to support update of ontologies.	Not implemented
ONT-014 See REQ-2015-0521R01	The M2M System shall enable functions for data conversion based on ontologies.	Not implemented
ONT-015 See REQ-2015-0521R01	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).	Implemented in Rel-2
ONT-016 See REQ-2015-0521R01	The M2M System shall support storage, management and discovery of ontologies.	Not implemented
ONT-017 See REQ-2015-0609	The oneM2M System shall support a semantic relation ("Is Paired To") between two M2M Devices.	Not implemented

6.3.2 Semantics Annotation Requirements

Table 4: Semantics Annotation Requirements

Requirement ID	Description	Release
ANN-001 See REQ-2015-0521R01	The oneM2M System shall provide capabilities to manage semantic information about the oneM2M resources, e.g. create, retrieve, update, delete, associate/link.	Implemented in Rel-2
ANN-002 See REQ-2015-0521R01	The oneM2M System shall support a common language for semantic description, e.g. RDF.	Implemented in Rel-2
ANN-003 See REQ-2015-0521R01	The oneM2M System shall support semantic annotation of oneM2M resources for example application related data contained in containers.	Implemented in Rel-2
ANN-004 See REQ-2015-0521R01	The oneM2M System shall support semantic annotation based on related ontologies.	Implemented in Rel-2
ANN-005 See REQ-2015-0521R01	The oneM2M System shall provide the capability for making semantic descriptions available in the M2M System, e.g. announcement.	Implemented in Rel-2
ANN-006 See REQ-2015-0521R01	The oneM2M System shall enable applications to retrieve an ontology representation related to semantic information used in the M2M System.	Not implemented
ANN-007 See REQ-2015-0521R01	The oneM2M system shall provide capabilities to manage data quality descriptions of resource.	Not implemented

6.3.3 Semantics Query Requirements

Table 5: Semantics Query Requirements

Requirement ID	Description	Release
QRY-001 See REQ-2015-0521R01	The oneM2M System shall provide capabilities to discover M2M Resources based on semantic descriptions.	Implemented in Rel-2

6.3.4 Semantics Mashup Requirements

Table 6: Semantics Mashup Requirements

Requirement ID	Description	Release
MSH-001 See REQ-2015-0521R01	The oneM2M System shall provide the capability to host processing functions for mash-up.	Not implemented
MSH-002 See REQ-2015-0521R01	The oneM2M System shall enable M2M Applications to provide processing functions for mash-up.	Not implemented
MSH-003 See REQ-2015-0521R01	The oneM2M System itself may provide pre-provisioned or dynamically created processing functions for mash-up.	Not implemented
MSH-004 See REQ-2015-0521R01	The oneM2M System shall be able to create and execute mash-ups based on processing functions.	Not implemented
MSH-005 See REQ-2015-0521R01	The oneM2M System shall be able to expose mash-ups as resources e.g. virtual devices.	Not implemented

6.3.5 Semantics Reasoning Requirements

Table 7: Semantics Reasoning Requirements

Requirement ID	Description	Release
RES-001 See REQ-2015-0521R01	The oneM2M System shall be able to update ontologies as a result of the ontology reasoning.	Not implemented
RES-002 See REQ-2015-0521R01	The oneM2M System shall be able to support semantic reasoning e.g. ontology reasoning or semantic rule-based reasoning.	Not implemented
RES-003 See REQ-2015-0521R01	The oneM2M System shall be able to support adding and updating semantic information based on semantic reasoning.	Not implemented

6.3.6 Data Analytics Requirements

Table 8: Data Analytics Requirements

Requirement ID	Description	Release
ANA-001 See REQ-2015-0521R01	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.	Not implemented
ANA-002 See REQ-2015-0521R01	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.	Not implemented
ANA-003 See REQ-2015-0521R01	The oneM2M System shall support a standardized format for the rules/policies used to define service logic.	Not implemented

6.4 Security Requirements

Table 9: Security Requirements

Requirement ID	Description	Release
SER-001	The oneM2M System shall incorporate protection against threats to its availability such as Denial of Service attacks.	Partially Implemented in Rel-1
SER-002	The oneM2M System shall be able to ensure the Confidentiality of data.	Implemented in Rel-1
SER-003	The oneM2M System shall be able to ensure the Integrity of data.	Implemented in Rel-1
SER-004	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 and network's security capability e.g. 3GPP GBA for establishing the M2M Services and M2M Applications level security through interfaces to Underlying Network.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
SER-008	The oneM2M System shall support countermeasures against unauthorized access to M2M Services and M2M Application Services.	Implemented in Rel-1
SER-009	The oneM2M System shall be able to support Mutual Authentication for interaction with Underlying Networks, M2M Services and M2M Application Services.	Implemented in Rel-1
SER-010	The oneM2M System shall be able to support mechanisms for protection against misuse, cloning, substitution or theft of security credentials.	Implemented in Rel-1
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.	Implemented in Rel-1
SER-012	The oneM2M System shall be able to support countermeasures against Impersonation attacks and replay attacks.	Partially implemented in Rel-1 (see note 3)
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).	Not implemented
SER-014	The oneM2M System shall be able to provide configuration data to an authenticated and authorized M2M Application in the M2M Gateway/Device.	Implemented in Rel-1
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.	Partially implemented (see note 4)
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.	Implemented in Rel-1
SER-017	The oneM2M System shall be able to mitigate threats identified in oneM2M TR-0008 [i.3].	Implemented in Rel-1
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.	Partially implemented
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.	Implemented in Rel-1
SER-020	The oneM2M System shall enable legitimate M2M Service Providers to provision their own Credentials into the M2M Devices/Gateways.	Implemented in Rel-1 (see note 5)

Requirement ID	Description	Release
SER-021	The oneM2M System shall be able to remotely and securely provision M2M security Credentials in M2M Devices and/or M2M Gateways.	Implemented in Rel-1 (see note 5)
SER-022	The oneM2M System shall enable M2M Application Service Providers to authorize interactions involving their M2M Applications on supporting entities (e.g. Devices/ Gateways/ Service infrastructure).	Implemented in Rel-1
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.	Partially implemented
SER-024	The oneM2M System shall enable M2M Applications to use different and segregated security environments.	Partially implemented
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).	Implemented in Rel-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).	Implemented in Rel-1
SER-027 See REQ-2015-0558R01	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.	Implemented in Rel-2
SER-028 See REQ-2015-0568R04	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.	Implemented in Rel-2
SER-029 See REQ-2015-0568R04	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.	Implemented in Rel-2
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.	Implemented in Rel-2
SER-031 See REQ-2015-0569R03	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.	Implemented in Rel-2
SER-032 See REQ-2015-0569R03	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.	Implemented in Rel-2
SER-033 See REQ-2015-0569R03	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.	Implemented in Rel-2
SER-034 See REQ-2015-0575R01	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.	Partially Implemented
SER-035 See REQ-2015-0575R01	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.	Partially Implemented
SER-036 See REQ-2015-0575R01	The oneM2M System shall enable security protocol end-points to authenticate each other without relying on intermediate service layer entities (whether trusted or untrusted).	Implemented in Rel-2
SER-037 See SEC-2015-0515R02	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).	Partially Implemented
SER-038 See SEC-2015-0515R02	The oneM2M System shall be able to expose an interoperable interface to provide Access Control Policies by means of specified access control policy language.	Not implemented
SER-039 See SEC-2015-0515R02	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.	Implemented in Rel-2

Requirement ID	Description	Release
SER-040 See SEC-2015-0517R05	When the M2M Devices are grouped and the M2M Gateway is authorized as the delegate of the group to access the M2M Server, the M2M Gateway shall be able to, perform Mutual Authentication with the M2M Server, on behalf of the M2M Devices in the group.	Not Implemented
SER-041 See SEC-2015-0517R05	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.	Implemented in Rel-2
SER-042 See SEC-2015-0522R02	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.	Not Implemented
SER-043 See REQ-2015-0590R01	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.	Not Implemented
SER-044 See REQ-2015-0591R04	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.	Not Implemented
SER-045 See REQ-2015-0604R02	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.	Not Implemented
SER-046 See REQ-2015-0605R04	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.	Implemented in Rel-2
SER-047 See REQ-2015-0605R04	The oneM2M System shall enable to protect portions of individual application data at-rest (e.g. hosted data) for confidentiality protection.	Implemented in Rel-2
SER-048 See REQ-2015-0605R04	The oneM2M System shall ensure that the end-to-end data Credentials are protected for Confidentiality, integrity and against tampering.	Implemented in Rel-2
SER-049 See REQ-2015-0605R04	The oneM2M System shall ensure that the end-to-end data Credentials are protected from exposure to intermediate entities.	Implemented in Rel-2
SER-050 See REQ-2015-0620	The oneM2M System shall enable pre-defined conditions to be protected from unauthorized modification.	Implemented in Rel-2
SER-051 See REQ-2015-0620	The oneM2M System shall enable the deletion of M2M data produced/stored by the M2M Devices/Gateways based on request from an authorized entity.	Implemented in Rel-2
SER-052 See REQ-2015-0621R01	The oneM2M System shall store and process privacy preferences in an interoperable manner.	Implemented in Rel-2
SER-053 See REQ-2015-0621R01	The oneM2M System shall support privacy profiles at various levels to care for conditions of legal requirements, manufacturers, and data subjects.	Implemented in Rel-2
SER-054 See REQ-2015-0621R01	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).	Implemented in Rel-2
SER-055 See REQ-2015-0623R01	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.	Not implemented
SER-056 See REQ-2015-0623R01	The oneM2M System shall allow overriding of security settings by a privileged User through standardized API.	Not implemented
SER-057 See REQ-2015-0623R01	The oneM2M System shall support a mechanism enabling addition/deletion of information enabling authentication of oneM2M entities through standardized API.	Not implemented

Requirement ID	Description	Release
SER-058 See REQ-2015-0627R02	The oneM2M System shall enable delegation of security functions (e.g. message authentication/integrity protection) of an entity to a trust-worthy entity.	Implemented in Rel-2
SER-059 See REQ-2015-0628R01	The oneM2M System shall protect the authenticity, Integrity, and Confidentiality of the representation of the delegated access rights.	Implemented in Rel-2
SER-060 See REQ-2015-0628R01	The oneM2M System shall be able to revoke the representation of the delegated access rights.	Implemented in Rel-2
SER-061 See 0585R01-App-ID Requirements	The oneM2M System shall be able to verify the App-ID to support the detection of impersonation or to support revocation.	Not implemented
SER-062 See REQ-2016-0056R01	The oneM2M System shall be able to reuse the privacy policy of the Underlying Network.	Not implemented
SER-063 See REQ-2016-0056R01	The oneM2M System shall be able to share its privacy policy with the Underlying Network.	Not implemented
SER-064 See REQ-2017-0005R03	The M2M Devices shall provide a mechanism to prevent installation or modification of the software/middleware/firmware which run on the M2M Devices, unless it is authorized by an allowed stakeholder.	Implemented in Release 3?
SER-065 See REQ-2017-0005R03	The oneM2M System shall be able to detect installation or modification of the software/middleware/firmware of M2M Devices that has not been authorized by an allowed stakeholder.	Implemented in Release 3?
SER-066 See REQ-2017-0005R03	The oneM2M System shall enable allowed stakeholders to restrict or prevent operation of M2M devices using software/middleware/firmware that the stakeholders did not authorize.	Implemented in Release 3?
SER-067 See REQ-2017-0005R03	The oneM2M System shall be able to prevent malfunction of M2M Devices caused by receiving unsolicited messages or information.	Implemented in Release 3?
SER-068 See REQ-2017-0030R05	The information exchanged within the oneM2M System shall use cryptographic technology to ensure information authentication and information integrity.	Implemented in Rel-2
SER-069 See REQ-2017-0030R05	The oneM2M System shall be able to securely transfer information by using an appropriate method such as digital signature.	Implemented in Rel-2
SER-070 See REQ-2017-0030R05	The oneM2M System shall be able to support security mechanisms to protect cryptographic keys and cryptographic operations by using tamper resistant elements such as TPM (Trusted Platform Module), HSM (Hardware Security Module) and SIM (Subscriber Identity Module).	Partially Implemented Note 7
SER-071 See REQ-2017-0030R05	The oneM2M System shall be able to support processing and granting of requests based on access rights of a resource if the required conditions are met.	Implemented in Rel-1
SER-072 See REQ-2017-0030R05	The oneM2M System shall provide privacy protection mechanisms at the central server.	Implemented in Rel-2
SER-073 See REQ-2017-0031R05	The oneM2M system shall be able to support authentication using device key and the integrity check ofM2M Device(s).	Rel-3?
SER-074 See REQ-2017-0031R05	The oneM2M system shall be able to support anonymization of the t information being provided, when requested by M2M Applications.	Rel-3/future releases?
SER-075 See REQ-2017-0031R05	The oneM2M System shall apply appropriate security levels for Applications that can have safety impacts (e.g. protection from malicious attacks).	Rel-3/future releases?

Requirement ID	Description	Release
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.		
NOTE 6: An M2M device may include e.g. firmware managed by an OEM vendor, middleware managed by a service provider and software managed by an application provider. The entity managing a software piece is designed as “allowed stakeholder” in the requirements above.		
NOTE 7: Support for SIM is supported in Release 1 and Release 2.		

6.5 Charging Requirements

Table 10: Charging Requirements

Requirement ID	Description	Release
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.	Implemented in Rel-1 (see note 4)
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.	Partially implemented (see note 2)
CHG-003	The oneM2M System shall provide means to coordinate charging data records for data usages with differentiated QoS from the Underlying Network.	Not implemented
CHG-004	The oneM2M System shall be able to utilize existing charging mechanisms of Underlying Networks.	Not implemented (see note 3)
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.	Implemented in Rel-1
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).	Not implemented
CHG-007 See REQ-2017-0031R05	The oneM2M System shall support mechanisms to correlate charging information (e.g. data/records) from different M2M Application Service Providers.	Rel-3/future releases?
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 use 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.		

6.6 Operational Requirements

Table 11: Operational Requirements

Requirement ID	Description	Release
OPR-001	The oneM2M System shall provide the capability for monitoring and diagnostics of M2M Applications.	Implemented in Rel-1
OPR-002	The oneM2M System shall provide the capability for software management of M2M Applications.	Implemented in Rel-1
OPR-003	The oneM2M System shall be able to configure the execution state an M2M Application (start, stop, restart).	Implemented in Rel-1
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.	Not implemented
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" (see note).	Implemented in Rel-2
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.	Implemented in Rel-2
OPR-007 See REQ-2015-0550R03	The oneM2M System shall be able to support receipt of the status information of the Underlying Network if supported by the Underlying Network.	Not implemented
OPR-008 See REQ-2015-0550R03	The oneM2M System shall be able to provide the M2M Applications with status information received from the Underlying Network.	Not implemented
OPR-009 See 0585R01-App-ID Requirements	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.	Implemented in Rel-2
OPR-010 See 0585R01-App-ID Requirements	The oneM2M System Registration Authorities shall be able to collect and maintain supporting required information when assigning an App-ID.	Implemented in Rel-2
NOTE: "Time controlled" is equivalent to the MTC Features specified in clause 7.2 of ETSI TS 122 368 [1].		

6.7 Communication Management Requirements

Table 12: Communication Management Requirements

Requirement ID	Description	Release
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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.	Implemented in Rel-1
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).	Partially implemented (see note 1)

Requirement ID	Description	Release
CMR-006 See REQ-2015-0564R02	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.	Implemented in Rel-1
CMR-007 See REQ-2015-0564R02	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, clause 6.6) as well as information received from the Applications (such as the information referred to in OPR-005, clause 6.6, or categorization of communications requested by the applications).	Partially Implemented (see note 2)
CMR-008 See REQ-2015-0564R02	The oneM2M System shall support data aggregation based on communication policies when exchanging data between the M2M Gateway/Device/Infrastructure Domain.	Implemented in Rel-1
CMR-009 See REQ-2015-0564R02	The oneM2M System should support data compression based on communication policies when exchanging data between the M2M Gateway/Device/Infrastructure Domain.	Not Implemented
CMR-010 See REQ-2015-0564R02	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.	Implemented in Rel-2
CMR-011 See REQ-2015-0564R02	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.	Implemented in Rel-2
CMR-012 See REQ-2015-0564R02	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.	Implemented in Rel-2
CMR-013 See REQ-2015-0564R02	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.	Implemented in Rel-2
CMR-014 See REQ-2015-0564R02	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.	Implemented in Rel-1
CMR-015 See REQ-2015-0601R01	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.	Implemented in Rel-2
CMR-0016 See REQ-2017-0001R03	The oneM2M system shall support the data to be transmitted to IoT platform with strict timing and packet loss requirements, determined by the application(s).	Not Implemented
CMR-0017 See REQ-2017-0001R03	The oneM2M system shall support the data to be transmitted from IoT platform to subscribed devices with highest priority, with strict timing and packet loss requirements, determined by the application(s).	Not Implemented
CMR-0018 See REQ-2017-0001R03	The oneM2M System shall be able to detect and report the missing data in time series, for each source of time sensitive data which is sent to the IoT platform.	Implemented in Rel-2
CMR-0019 See REQ-2017-0001R03	The oneM2M System shall be able to detect and report the missing data in time series, for each time sensitive application receiving data.	Implemented in Rel-2
NOTE 1: Long lived security context and registration is covered, M2M Sessions are not covered. NOTE 2: CMDH policies (application side) is implemented, information from the Underlying Network can be utilized but the method for provisioning via Mcn is not covered.		

6.8 LWM2M Interworking Requirements

Table 13: LWM2M Interworking Requirements

Requirement ID	Description	Release
LWM2M-001 See REQ-2015-0517R04	The oneM2M System shall provide the capability to transparently transport LWM2M Objects between LWM2M Clients and M2M Applications.	Implemented in Rel-2
LWM2M-002 See REQ-2015-0517R04	The oneM2M System shall provide the capability to translate LWM2M Objects into a semantic representation of the LWM2M Object as oneM2M resources.	Implemented in Rel-2
LWM2M-003 See REQ-2015-0517R04	The oneM2M System shall provide the capabilities of the LWM2M Server in order to interwork between LWM2M Clients and M2M Applications.	Implemented in Rel-2
LWM2M-004 See REQ-2015-0517R04	The oneM2M System shall provide the capability for M2M Applications to discover LWM2M Clients using the LWM2M Client's Endpoint Name.	Implemented in Rel-2
LWM2M-005 See REQ-2015-0517R04	When transparently transporting LWM2M Objects, the oneM2M System shall provide the capability for M2M Applications to discover the defining of LWM2M Objects transported by the oneM2M System.	Not implemented
LWM2M-006 See REQ-2015-0517R04	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.	Implemented in Rel-2
LWM2M-007 See REQ-2015-0517R04	The oneM2M System shall provide capability to onboard devices that incorporate a LWM2M Client.	Implemented in Rel-2
LWM2M-008 See REQ-2015-0517R04	The oneM2M System shall provide the capability to interoperate the underlying security mechanisms of the LWM2M Client with the security capabilities provided by the oneM2M System.	Implemented in Rel-2

7 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	Release
NFR-001	Continua Health Alliance is incorporating a RESTful approach to its design. To support CHA, oneM2M should consider RESTful styles and approaches while designing the M2M architecture.	Implemented in Rel-1
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.	Implemented in Rel-1

Annex A (informative): Requirements for the next release

The requirements contained in this Annex are gathered and targeted for the next release of oneM2M.

1. Functional Requirements
    - 1.1 Overall System Requirements
    - 1.2 Management Requirements
    - 1.3 Semantics Requirements
        - 1.3.1 Ontology Related Requirements
        - 1.3.2 Semantics Annotation Requirements
        - 1.3.3 Semantics Query Requirements
        - 1.3.4 Semantics Mashup Requirements
        - 1.3.5 Semantics Reasoning Requirements
        - 1.3.6 Data Analytics Requirements
    - 1.4 Security Requirements
    - 1.5 Charging Requirements
    - 1.6 Operational Requirements
    - 1.7 Communication Management Requirements
    - 1.8 LWM2M Interworking Requirements

History

Document history		
V2.7.1	September 2016	Publication
V2.10.2	March 2020	Publication