ONEM2M
TECHNICAL SPECIFICATION

Document Number	oneM2M-TS-0002-V-0.6.0
Document Name:	oneM2M Requirements Technical Specification
Date:	< 2013-10-16>
Abstract:	This present document contains an informative functional role model and normative technical requirements for oneM2M.

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

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

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

Copyright Notification

No part of this document may be reproduced, in an electronic retrieval system or otherwise, except as authorized by written permission.

The copyright and the foregoing restriction extend to reproduction in all media.

© 2013, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC).

All rights reserved.

Notice of Disclaimer & Limitation of Liability

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

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

Contents

Contents 3
1 Scope 4
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and acronyms 6
3.1 Definitions 6
3.2 Acronyms 6
4 Conventions 8
5 Introduction to the M2M ecosystem 9
5.1 Functional roles description 9
6 Functional Requirements 11
6.1 Overall System Requirements 11
6.2 Management Requirements 16
6.3 Abstraction & Semantics Requirements 17
6.3.1 Abstraction Requirements 17
6.3.2 Semantics Requirements 18
6.4 Security Requirements 18
6.5 Charging Requirements 20
6.6 Operational Requirements 21
6.7 Communication Request Processing Requirements 21
7 Non-Functional Requirements (non-normative) 22
History 23

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

6. 1 Scope

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

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

2 References

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

2.1 Normative references

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

[1] oneM2M TR0004, “oneM2M Definitions and Acronyms”

[2] 3GPP TS 22.368, "Service Requirements for Machine-Type Communications (MTC); Stage 1"

[3] oneM2M TS0003, “oneM2M Security Solutions”

2.2 Informative references

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

(http://member.onem2m.org/Static_pages/Others/Rules_Pages/oneM2M-Drafting-Rules-V1_0.doc)

[i.2] ETSI TS102 689 V1.1.1, Machine-to-Machine communications (M2M);M2M service requirements

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

3 Definitions and acronyms

3.1 Definitions

For the purposes of the present document, the terms and definitions given in "oneM2M Definitions and Acronyms" [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in [1].

Dynamic Device/Gateway Context: see definition in [1].

Event: see definition in [1].

Event Categories: see definition in [1].

Infrastructure Domain: see definition in [1].

Information Model: see definition in [1].

M2M Application: see definition in [1].

M2M Application Service: see definition in [1].

M2M Application Service Provider: see definition in [1].

M2M Area Network: see definition in [1].

M2M Common Services: see definition in [1].

M2M Device: see definition in [1].

M2M Service: see definition in [1].

M2M Service Administrative State of a M2M Device: see definition in [1].

M2M Service Operational Status of a M2M Device: see definition in [1].

M2M Service Provider: see definition in [1].

M2M Service Subscription: see definition in [1].

M2M Session: see definition in [1].

M2M System: see definition in [1].

Network Operator: see definition in [1].

Static Device/Gateway Context: see definition in [1].

Underlying Network: see definition in [1].

User: see definition in [1].

3.2 Acronyms

For the purposes of the present document, the following abbreviations apply:

CHA: Continua Health Alliance

GSMA: Global System for Mobile Communications Association

HSM : Hardware Security Module

OMA : Open Mobile Alliance

Qos: Quality of Service

SMS : Short Message Service

USSD : Unstructured Supplementary Service Data

WAN: Wide Area Network

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

4 Conventions

The key words “shall”, “shall not”, “should”, “should not”, “may”, “need not” in this document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

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***

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

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.

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

6 Functional Requirements

6.1 Overall System Requirements

Requirement ID	Description	Release
OSR-001	The M2M System shall be able to allow communication between M2M Applications by using multiple communication means based on IP Access.	
OSR-002	The M2M 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) as well as rich computing (e.g. large CPU, memory) or communication (e.g. 3/4G wireless modem, wireline) capabilities.	
OSR-003	The M2M System shall support the ability to maintain M2M Session in coordination with application session for those M2M Applications that require it.	
OSR-004	M2M System shall support the ability to support session-less application communications for those M2M Applications that require it.	
OSR-005	The M2M 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.	
OSR-006	The M2M 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 Note: The set of features or APIs to be supported depends on the M2M Common Services and access to available APIs.	
OSR-007	The M2M 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.	
OSR-008	The M2M 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 M2M System shall support the ability for single or multiple M2M Applications to interact with a single or multiple M2M Devices/Gateways	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	(application in the device/gateway). Note: The relation M2M Network Application to M2M Device/Gateway may be 1:1, 1:n, n:1 and/or n:m.	
OSR-010	The M2M 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-011	The M2M 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 or request from M2M Applications.	
OSR-012	The M2M System shall support communications between M2M Applications and Devices supporting M2M Services by means of continuous or non-continuous connectivity.	
OSR-013	The M2M 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 M2M System shall be able to communicate with M2M Devices, behind an M2M Gateway that supports heterogeneous M2M Area Networks.	
OSR-015	The M2M System shall support different communication patterns including infrequent communications, small data transfer, large file transfer, streamed communication.	
OSR-016	The M2M 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 M2M 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 M2M System, individually, as a subset or as a complete set of services.	
OSR-018	The M2M 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. Note:No roaming on M2M Service level is assumed by this requirement.	
OSR-019	The M2M 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;	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	• for specified data	
OSR-020	The M2M System shall be able to support policies and their management regarding the aspects of storage and retrieval of data/information.	
OSR-021	The M2M System shall be able to provide mechanisms to enable sharing of data among multiple M2M Applications.	
OSR-022	When some of the components of M2M System are not available (e.g. WAN connection lost), the M2M System shall be able to support the normal operation of components of the M2M System that are available.	
OSR-023	The M2M System shall be able to identify the M2M Services to be used by M2M Service Subscriptions. Note: M2M Service Subscriptions are not Application subscriptions (e.g., Home Energy Management).	
OSR-024	The M2M System shall be able to identify the M2M Devices used by M2M Service Subscriptions.	
OSR-025	The M2M System shall be able to identify the M2M Applications used by M2M Service Subscriptions.	
OSR-026	If provided by the Underlying Network, the M2M 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 M2M 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. Note: Transparent exchange of information implies information that is mainly interpreted by the M2M Application and the Underlying Network Provider.	
OSR-028	The M2M System shall be able to trigger a series of commands to actuators on behalf of M2M Applications.	
OSR-029	The M2M System shall be able to support sending common command(s) to each actuator or sensor via a group.	
OSR-030	The M2M System shall be able to support the management (i.e. addition, removal, retrieval and update) of the membership of a group.	
OSR-031	The M2M System shall be able to support a group as a member of another group.	
OSR-032	The M2M 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. Note: Based on the Event Categories and via interworking with Underlying Networks, the M2M System can support differentiated services (by providing Quality-of-Service) requested by M2M Applications.	
OSR-033	Based on the Dynamic Device/Gateway Context of the M2M Gateway and/or Device and the defined Event Categories, the M2M System shall provide the capability to dynamically adjust the scheduling of reporting and notification of the M2M Device/Gateway.	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	Note: 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.	
OSR-034	The M2M System shall support seamless replacement of M2M Devices as well as M2M Gateways (e.g., redirecting traffic, connection, recovery, etc.).	
OSR-035	The M2M 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 M2M System should provide mechanisms to accept requests from M2M Application Service Providers for compute/analytics services.	
OSR-037	The M2M 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 M2M System shall support the inclusion of M2M Application's QoS preference in service requests to Underlying Networks.	
OSR-039	The M2M 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 M2M System shall be able to leverage multiple communication mechanisms (such as USSD or SMS) when available in the Underlying Networks.	
OSR-041	The M2M System shall provide a mechanism, which supports the addition of new M2M Services without impact to M2M interface interoperability	
OSR-042	The M2M 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 M2M System shall be able to verify that members of a group support a common set of functions.	
OSR-044	The M2M 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-045	The M2M System shall be able to be aware of the reachability status and to utilize reachability schedules generated by either the M2M Device or the Infrastructure Domain.	
OSR-046	The M2M System shall be able to support capability for the M2M Application to select communication protocol acknowledgment mechanisms.	
OSR-047	The M2M System shall be able to support mechanism for the M2M Devices and/or Gateways to report their geographical location information to M2M	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	Applications. Note: Geographical location information can be more than simply longitude and latitude.	
OSR-048	The M2M System shall provide an M2M Service that allows M2M Devices and/or Gateways to share their own or other M2M Devices' geographical location information. Note: Geographical location information can be more than simply longitude and latitude.	
OSR-049	The M2M 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 M2M 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 M2M 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 M2M 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.	
OSR-053	The M2M System shall provide a means that enables the interoperability of interfaces among different releases. Note: "means" above does not imply only technical mechanisms.	
OSR-054	The M2M 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 M2M 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.	
OSR-056	The M2M System shall enable discovery of usable M2M Applications on an M2M Gateway or at an M2M Device .	
OSR-057	The M2M System shall enable discovery of M2M Gateways and M2M Devices available to an M2M Application for data exchange.	
OSR-058	The M2M System shall be able to provide time stamps as needed by common service functions.	
OSR-059	The M2M System shall be able to support Role-based access control based on M2M Service Subscriptions.	
OSR-060	The M2M System should support time synchronization with an external clock source.	
OSR-061	M2M Devices and M2M Gateways may support time synchronization within the M2M System.	

OSR-062	The M2M System shall enable means of testing the connectivity towards a set of M2M Applications.	
OSR-063	The M2M System shall be able to manage the scheduling of M2M Service Layer connectivity and messaging between the Infrastructure Domain and M2M Devices/Gateways.	
OSR-064	The M2M System shall be able to aggregate messages depending on message delay tolerance and/or category.	
OSR-065	The M2M System shall be able to provide mechanisms to accept M2M Applications for distribution, from M2M Application Service Providers.	
OSR-066	The M2M 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 M2M System shall be able to take operational and management action as requested by M2M Applications.	
OSR-068	When available from an Underlying Network, the M2M 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 M2M 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 M2M 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.	
OSR-071	The M2M System shall be able to enable an authorized M2M Application to set the M2M Service Administrative State of a M2M Device.	
OSR-072	The M2M System shall be able to initiate a set of well-defined actions (e.g. trigger upon a threshold, compare a value …) to one or more M2M Application(s) on behalf of another M2M Application.	

Table 1 Overall System Requirements

6.2 Management Requirements

Requirement ID	Description	Release
MGR-001	The M2M System shall be able to support management and configuration of M2M Gateways/ Devices including resource constrained M2M Devices.	
MGR-002	The M2M 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 M2M 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.	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

MGR-004	The M2M System shall support common means to manage devices enabled by different management technologies (e.g. OMA DM, BBF TR069).	
MGR-005	The M2M System shall provide the capability to manage multiple devices in a grouped manner.	
MGR-006	The M2M System shall provide the capability for provisioning and configuration of devices in M2M Area Networks .	
MGR-007	The M2M System shall provide the capability for monitoring and diagnostics of M2M Gateways/Devices in M2M Area Networks .	
MGR-008	The M2M System shall provide the capability for software management of devices in M2M Area Networks.	
MGR-009	The M2M System shall provide the capability for rebooting and/or resetting of M2M Gateways/Devices and other devices in M2M Area Networks.	
MGR-010	The M2M System shall provide the capability for authorizing devices to access M2M Area Networks.	
MGR-011	The M2M System shall provide the capability for modifying the topology of devices in M2M Area Networks,subject to restriction based on management policy of M2M Area Network.	
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	The M2M System shall be able to identify and manage M2M Service status of M2M Devices.	
MGR-014	The M2M System shall be able to retrieve events and information logged by M2M Gateways/ Devices and other devices in M2M Area Networks.	
MGR-015	The M2M 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 M2M 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 M2M System shall support the capability to map M2M service subscription role(s) to roles used within technology specific Device Management protocols.	

Table 2 Management Requirements

6.3 Abstraction & Semantics Requirements

6.3.1 Abstraction Requirements

Requirement ID	Description	Release
ABR-001	The M2M System shall provide a generic structure for data representation.	

ABR-002	The M2M System shall be able to provide translation mechanisms between Information Models used by M2M Applications, M2M Devices/Gateways, and other devices.	
ABR-003	The M2M System shall provide capabilities to represent Virtual Devices and Things, (which are not necessarily physical devices.)	

Table 3 Abstraction Requirements

6.3.2 Semantics Requirements

Requirement ID	Description	Release
SMR-001	The M2M System shall provide capabilities to manage semantic descriptions of resources and M2M Applications, e.g, create, retrieve, update, delete, associate/link.	
SMR-002	The M2M System shall support a common modeling language for semantic descriptions (including relationships between Things) in order to make them available to M2M Applications.	
SMR-003	The M2M System shall be able to provide interworking capabilities between different modeling languages for semantic descriptions.	
SMR-004	The M2M System shall provide capabilities to discover M2M Resources based on semantic descriptions.	
SMR-005	The M2M System shall support the capability to access semantic descriptions which are outside of the M2M System.	
SMR-006	The M2M System shall be able to support capabilities for performing M2M data Analytics based on semantic descriptions from M2M Applications and /or from the M2M System.	
SMR-007	The M2M System shall be able to provide capabilities for performing Semantic Mash-up using M2M data from M2M Applications and/or from the M2M System (e.g. to create Virtual Devices, offer new M2M Services, etc.)	

Table 4 Semantics Requirements

6.4 Security Requirements

Requirement ID	Description	Release
SER-001	The M2M System shall incorporate protection against threats to its availability such as Denial of Service attacks.	
SER-002	The M2M System shall be able to ensure the confidentiality of data.	
SER-003	The M2M System shall be able to ensure the integrity of data.	
SER-004	In case where the M2M Devices support USIM / UICC and the Underlying Networks support network layer security, the M2M System shall be able to leverage device's USIM / UICC credentials and network's security capability	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	e.g. 3GPP GBA for establishing the M2M Services and 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 M2M System is aware of Underlying Network's bootstrapping capability e.g. 3GPP GBA, the M2M System shall be able to expose this capability to M2M Services and Applications through API.	
SER-006	In case where the M2M Devices support USIM / UICC and the Underlying Networks support network layer security, the M2M 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 M2M 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 M2M System shall support countermeasures against unauthorized access to M2M Services and M2M Application Services.	
SER-009	The M2M System shall be able to support mutual authentication for interaction with Underlying Networks, M2M Services and M2M Application Services.	
SER-010	The M2M System shall be able to support mechanisms for protection against misuse, cloning, replacement or theft of security credentials.	
SER-011	The M2M System shall protect the use of the identity of an M2M Stakeholder within the M2M System against discovery and misuse by other stakeholders.	
SER-012	The M2M System shall be able to support countermeasures against Impersonation attacks and Replay attacks.	
SER-013	The M2M 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 M2M System shall be able to provide configuration data to an authenticated and authorized M2M Application in the M2M Gateway/Device.	
SER-015	The M2M System shall be able to support mechanisms to provide Subscriber identity to authorized and authenticated M2M Applications when the M2M System has the Subscriber's consent.	
SER-016	The M2M 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 M2M System shall be able to mitigate threats identified in TS-0003[3].	
SER-018	The M2M 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 M2M System shall be able to use service-level credentials present inside the M2M device for establishing the M2M Services and Applications level security.	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

SER-020	The M2M System shall enable legitimate M2M Service Providers to provision their own credentials into the M2M Devices/Gateways.	
SER-021	The M2M System shall be able to remotely and securely provision M2M security credentials in M2M Devices and/or M2M Gateways.	
SER-022	The M2M System shall enable M2M Application Service Providers to authorize interactions involving their M2M Applications on supporting entities (e.g. Devices/ Gateways/ Service infrastructure).	
SER-023	If a Hardware Security Module (HSM) is supported, the M2M Device shall be able to use the HSM to support security.	
SER-024	The M2M System shall enable M2M Applications to use different and segregated security environments.	
SER-025	The M2M System shall be able to prevent unauthorized M2M Stakeholders from identifying and/or observing the actions of other M2M Stakeholders in the M2M System, e.g. access to resources and services. Note: The above requirement does not cover whatever is outside of the M2M System, e.g. Underlying Networks.	
SER-026	The M2M System shall be able to provide mechanism for the protection of confidentiality of the geographical location information. Note: Geographical location information can be more than simply longitude and latitude.	

Table 5 Security Requirements

6.5 Charging Requirements

Requirement ID	Description	Release
CHG-001	The M2M System shall support collection of charging specific information related to the individual services facilitated by the M2M 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.	
CHG-002	The M2M 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 M2M System shall provide means to coordinate charging data records for data usages with differentiated QoS from the Underlying Network.	
CHG-004	The M2M System shall be able to reuse existing charging mechanisms of Underlying Networks.	
CHG-005	The M2M 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	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	• provider-to-subscriber accounting including additional functions like statistics.	
CHG-006	The M2M 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. Note: 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.	

Table 6 Charging Requirements

6.6 Operational Requirements

Requirement ID	Description	Release
OPR-001	The M2M System shall provide the capability for monitoring and diagnostics of M2M Applications.	
OPR-002	The M2M System shall provide the capability for software management of M2M Applications.	
OPR-003	The M2M 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 M2M System shall have the ability to schedule traffic via the Underlying Network based on instructions received from the Underlying Network.	
OPR-005	The M2M 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 information includes the following features for an M2M Device: • Time controlled for devices to send or receive data only during defined time intervals. Note: “Time controlled” is equivalent to the MTC Features specified in [i.2] (section 7.2 of 3GPP TS 22.368)	
OPR-006	Depending on availability of suitable interfaces provided by the Underlying Network the M2M System shall be able to provide information related to usage and traffic characteristics of M2M Devices or M2M Gateways to the Underlying Network.	

Table 7 Charging Requirements

6.7 Communication Request Processing Requirements

Requirement ID	Description	Release
CRPR-001	The M2M System shall be able to support M2M Gateways and M2M Devices	

	that offer communication services to M2M Application to buffer incoming messages for communicating data to another M2M Gateway/Device/Infrastructure Domain.	
CRPR-002	The M2M System shall be able to support forwarding buffered messages depending on communication policies and based on service preference associated with the buffered messages.	
CRPR-003	The M2M 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	
CRPR-004	The M2M 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.	
CRPR-005	The M2M 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).	

Table 8 Communication Request Processing Requirements

7 Non-Functional Requirements (non-normative)

This section 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 M2M System. But as they cannot necessarily be expressed as requirements per se, they shall be introduced and expressed in this section.

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.	
NFR-002	The M2M System should communicate using protocols that are efficient in terms of amount of exchanged information over amount of exchanged data measured in bytes.	

Table 9 Non-Functional Requirements

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

History

This clause shall be the last one in the document and list the main phases (all additional information will be removed at the publication stage).

Publication history		
V1.1.1	<dd-Mmm-yyyy>	<Milestone>

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

Draft history (to be removed on publication)		
V.0.0.1	11 Mar 2013	Rapporteur Input – Skeleton Draft
V.0.0.2	11 Mar 2013	Implement the agreed contributions until TP#3: oneM2M-REQ-2012-0054R07 oneM2M-REQ-2013-0180R03 oneM2M-REQ-2013-0195R01 oneM2M-REQ-2013-0143R02 oneM2M-REQ-2013-0154R03 oneM2M-REQ-2013-0155R03 oneM2M-REQ-2013-0228R02 oneM2M-REQ-2013-0198R03 oneM2M-REQ-2013-0162R02 oneM2M-REQ-2013-0170R04 oneM2M-REQ-2013-0134R02

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.0.3	24 Apr 2013	Implement the agreed contributions: oneM2M-REQ-2013-0174R05 oneM2M-REQ-2013-0187R07 oneM2M-REQ-2013-0269R02 oneM2M-REQ-2013-0148R04 oneM2M-REQ-2013-0149R03 Note: no changes are required by 149R03. It only states that the current charging requirements covers the overlapped proposals. oneM2M-REQ-2013-0247 Note: Operational Section was added oneM2M-REQ-2013-0252R02 oneM2M-REQ-2013-0268R01 oneM2M-REQ-2013-0285R02 oneM2M-REQ-2013-0310R01 oneM2M-REQ-2013-0271R02 oneM2M-REQ-2013-0291R03 oneM2M-REQ-2013-0280R02
V0.1.0	20 May 2013	Implement the agreed contributions: oneM2M-REQ-2013-0179R08
V0.2.0	03 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0297R04 oneM2M-REQ-2013-0274R01 oneM2M-REQ-2013-0273R02
V0.3.0	17 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0274R02

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.4.0	24 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0157R06 oneM2M-REQ-2013-0368R01 oneM2M-REQ-2013-0267R05 oneM2M-REQ-2013-0275R03 oneM2M-REQ-2013-0320R02 oneM2M-REQ-2013-0287R05 oneM2M-REQ-2013-0329R01 oneM2M-REQ-2013-0189R08 oneM2M-REQ-2013-0311R02 oneM2M-REQ-2013-0331R02 oneM2M-REQ-2013-0341R01 oneM2M-REQ-2013-0343R04 oneM2M-REQ-2013-0344R05 oneM2M-REQ-2013-0363R02 oneM2M-REQ-2013-0372R01 oneM2M-REQ-2013-0376R01 oneM2M-REQ-2013-0173R05 oneM2M-REQ-2013-0313R02 oneM2M-REQ-2013-0375 oneM2M-REQ-2013-0345R01

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.5.0	09 Aug 2013	Implement the agreed contributions: oneM2M-REQ-2013-0357R05 oneM2M-REQ-2013-0358R01 oneM2M-REQ-2013-0359R04 oneM2M-REQ-2013-0335R03 oneM2M-REQ-2013-0366R02 oneM2M-REQ-2013-0371R01 oneM2M-REQ-2013-0138R05 oneM2M-REQ-2013-0316R03 oneM2M-REQ-2013-0333R03 oneM2M-REQ-2013-0337R05 oneM2M-REQ-2013-0338R02 oneM2M-REQ-2013-0349R02 oneM2M-REQ-2013-0350R05 oneM2M-REQ-2013-0373R03 oneM2M-REQ-2013-0374R02 oneM2M-REQ-2013-0378R01 oneM2M-REQ-2013-0381R03 oneM2M-REQ-2013-0392R01 oneM2M-REQ-2013-0394R02 oneM2M-REQ-2013-0397R01 oneM2M-REQ-2013-0384R03 oneM2M-REQ-2013-0360R03 oneM2M-REQ-2013-0403R01 oneM2M-REQ-2013-0404R01
V0.5.1	22 Aug 2013	1. Modify the text of Abstract. 2. Chang “OneM2M” to “oneM2M”.

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.5.2	16 Oct 2013	1. Create new section 6.7 Communication Request Processing Requirements. 2. Move OSR-042, OSR-043, OSR-044 and OSR-045 from section 6.1 to section 6.7. 3. Implement the agreed contributions at TP#7: oneM2M-REQ-2013-0340R04 Definition of Event Categorization oneM2M-REQ-2013-0413R05-Requirements_cleanup oneM2M-REQ-2013-0418R02-CR_on_SER-015 oneM2M-REQ-2013-0419R02 Proposed clean-up of some unclear requirements in TS-0002 oneM2M-REQ-2013-0421R02 Security Requirements Modification
V0.6.0	17 Oct 2013	Do some changes to keep consistent with oneM2M-Template-TS-20130923.

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.