|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | <REQ#44> |
| Source:\* | Saïd Gharout <said.gharout@orange.com>  Francois Ennesser <Francois.Ennesser@gemalto.com>  James HU <QH8316@att.com>  Dale Seed <Seed.Dale@ConvidaWireless.com>  Mjodrag Djurica, TNO, Miodrag.djurica@tno.nl |
| Date:\* | 2017-03-14 |
| Reason for Change/s:\* | REQs according to use case patch the connected home from TR0001 |
| CR against: Release\* | Rel 4 |
| CR against: WI\* | Active <Work Item 01>  MNT maintenance / < Work Item number(optional)>  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements / < Work Item number (optional)>  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS0002 v4.1.0 |
| Clauses \* | 6.1, 6.4 |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Impacted other TS/TR(s) | <TS/TR number>, <Version Number>, and <Description on which aspect should be reflected in this TS/TR> |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO |
| Template Version: January 2017 (Do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

\*\*\*\*\*\*\* Start of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 |
| 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 |
| 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. | Partially implemented  (see note 18) |
| 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 |
| 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 |
| 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 |
| 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 viathe 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 |
| 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  (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. (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) . (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. (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. (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? |
| OSR-134  See REQ-2017-0048R02 | The oneM2M System shall enable provisioning, installation, configuration and registration methods of field devices for different management systems (e.g. allowing different entities to own and manage the device) or application systems  (e.g. allowing different entities to utilise the device data). | future releases? |
| OSR-135  See REQ-2017-0048R02 | The oneM2M System shall enable registrations to include information identifing the peer entites, and related information (e.g. management privilege, subscription etc.), necessary for establishment of the respective peer relationships. | future releases? |
| OSR-136  See REQ-2017-0048R02 | The oneM2M System shall enable registrations using a complete set of information context for the peer entities (termed "full registrations"). | future releases? |
| OSR-137  See REQ-2017-0048R02 | The oneM2M System shall enable registrations using only a subset of information context for the peer entities (termed "lightweight registration"). | future releases? |
| OSR-138  See REQ-2017-0048R02 | The oneM2M System shall enable "lightweight registrations" instances with different entities, which pertain to a common peer entity, to use different sets of information about the common peer entity as needed. | future releases? |
| OSR-139  See REQ-2017-0048R02 | The oneM2M System shall enable correlation of the "full registration" and the "lightweight registration" instances pertaining to a common peer entity. | future releases? |
| OSR-140  See REQ-2017-0048R02 | The oneM2M System shall enable differentiation of the "full registrations" and the "lightweight registrations" instances pertaining to a common peer entity. | future releases? |
| OSR-141  See REQ-2017-0073R02 | The oneM2M system shall be able to maintain information about the correlation status of a data set and update it dynamically based on application request |  |
| OSR-142  See REQ-2018-0021R02 | The M2M System (e.g. through the GW) shall be able to dynamically obtain authenticated metadata (e.g. Firmware version, Manufacturer ID, HW version) from all the IoT/M2M Devices located in the Home (e.g. the LAN). |  |
| 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 requirments is TBD. | | |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Start of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

## 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) |
| 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 |
| 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 thegroup | 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 |
| 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? |
| SER-076  See REQ-2018-0001 | The oneM2M System shall be able to provide a framework for end-to-end authentication of user applications to the M2M vendor’s specific nodes (non oneM2M). |  |
| SER-077  See REQ-2018-0021R02 | The M2M System shall be able to dynamically trigger the secure Firmware/Software update of IoT Devices located in the Home. |  |
| 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.  NOTE6: 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. | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*