oneM2M
Technical Report

Document Number	TR-0001-V5.2.2
Document Name:	Use Cases Collection
Date:	2025-06-06
Abstract:	This oneM2M Technical Report includes a collection of use cases from various M2M industry segments. Use cases focus on the sequence of interactions among actors, and may include potential requirements.
Template Version:	January 2017 (Do not modify)

The present document is provided for future development work within oneM2M only. The Partners accept no liability for any use of this report.

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

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

1 Scope

The present document includes a collection of use cases from a variety of M2M industry segments. Each use case may include a description, source, actors, pre-conditions, triggers, normal and alternative flow of sequence of interactions among actors and system, post-conditions, illustrations and potential requirements. The potential requirements provide an initial view of what oneM2M requirements could arise from the Use Case as seen by the contributor. These are intended to help the reader understand the use case's needs. These potential requirements may have been subsequently submitted by the contributor for consideration as candidate oneM2M requirements, which may or may not have been agreed as a oneM2M requirement (often after much editing). As such, there may not be a direct mapping from the potential requirements to agreed oneM2M requirements [i.15]

2 References

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. 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.

Not applicable.

2.2 Informative references

Clause 2.2 shall only contain informative references which are cited in the document itself.

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 TR 102 935 v2.1.1, Machine to Machine communications (M2M);Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform
- [i.3] ETSI TS 102 689 V1.1.1, Machine-to-Machine communications (M2M); M2M service requirements
- [i.4] ETSI TR 102 732, Machine to Machine Communications (M2M); Use cases of M2M applications for eHealth
- [i.5] ETSI TR 102 897, Machine to Machine Communications (M2M); Use cases of M2M applications for City Automation
- [i.6] HGI-GD017-R3, Use Cases and Architecture for a Home Energy Management Service
- [i.7] ISO/ IEC 15118 Road vehicles, vehicle to grid communication
- [i.8] Mandate 486, MANDATE FOR PROGRAMMING AND STANDARDISATION ADDRESSED TO THE EUROPEAN STANDARDISATION BODIES IN THE FIELD OF URBAN RAIL
- [i.9] DIN specification 70121, ELECTROMOBILITY - DIGITAL COMMUNICATION BETWEEN A D.C. EV CHARGING STATION AND AN ELECTRIC VEHICLE FOR CONTROL OF D.C. CHARGING IN THE COMBINED CHARGING SYSTEM
- [i.10] ETSI TR 102 638, Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Definitions
- [i.11] 3GPP TS 22.368, Service requirements for Machine-Type Communications (MTC); Stage 2
- [i.12] 3GPP TS 23.682, Architecture enhancements to facilitate communications with packet data networks and applications
- [i.13] 3GPP TR 23.887, Architectural Enhancements for Machine Type and other mobile data applications
- [i.14] Communications Guidelines defined in Continua Health Alliance, The Continua Health Alliance, Version 2012 Design Guidelines
- [i.15] oneM2M TS-0002 Requirements Technical Specification
- [i.16] ETSI TS 103.383 Smart Cards; Embedded UICC; Requirements Specification
- [i.17] IEC 61850 Communication networks and systems in substations
- [i.18] oneM2M TR-0013 Home Domain Enablement Technical Report
- [i.19] oneM2M TR-0018 Industrial Domain Enablement Technical Report
- [i.20] oneM2M TR-0016 Authorization Architecture and Access Control Policy
- [i.21] oneM2M TR-0026 Vehicular Domain Enablement Technical Report
- [i.22] ETSI TR 103 546 SmartM2M: Requirement & Feasibility study for Smart Lifts in IoT
- [i.23] ETSI TR 103 714 SmartM2M; Study for oneM2M Discovery and Query use cases and requirements

- [i.24] Lixin Gao. On inferring autonomous system relationships in the internet. IEEE/ACM Trans. Netw. 9(6): 733-745, 2001 https://dl.acm.org/doi/10.1109/90.974527
- [i.25] Luigi Liquori, Rossano Gaeta, and Matteo Sereno. A Network Aware Resource Discovery Service. EPEW 2019
- 16th European Performance Engineering Workshop, Nov 2019, Milano, Italy, Volume 12039 of Lecture Notes in Computer Science, Springer Verlag, pages 84-99, 2019, https://hal.inria.fr/hal-01895452
- [i.26] Raphael Chand and Michel Cosnard and Luigi Liquori. Powerful resource discovery for Arigatoni overlay network. Future Generation Computing System, volume 23, number 1, pages 31-38, 2008, https://hal.inria.fr/hal-00909630
- [i.27] IETF RFC 4271: Border Gateway Protocol 4 (BGP4), 2006, https://tools.ietf.org/html/rfc4271
- [i.28] void
- [i.29] void
- [i.30] void
- [i.31] ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach
- [i.32] AIOTI Report: IoT Relation and Impact on 5G, Release 3.0, https://aioti.eu/wp-content/uploads/2020/05/AIOTI-IoT-relation-and-impact-on-5G-R3-Published.pdf
- [i.33] void
- [i.34] void

3 Definition of Terms and Abbreviations

3.1 Terms

Advanced Semantic Discovery (ASD): an extension of the present oneM2M semantic discovery across a network of CSEs statically connected among them in a *tree-like* topology inside a single or multiple Service Provider (SP), including non oneM2M ones and in a *mesh-like* topology between the root of the different SPs

Advanced Semantic Discovery Query (ASDQ): word in the Advanced Semantic Discovery Query Language (ASDQL) according to the Theory of Formal Languages

Advanced Semantic Discovery Query Language (ASDQL): extension of the actual oneM2M Semantic Discovery Query Language (SDQL), which has to be suitable enough to describe queries that will be resolved in a *cooperative* way by a distributed network of CSEs

> NOTE: Each CSE involved in the resolution participates in resolving subqueries and aggregating results by coordinating and cooperating among each other's.

Semantic Discovery Agreement (SDA): aims at adding a semantic registering information for the cooperation between CSEs

> NOTE 1: With an analogy with the Border Gateway Protocol 4 [i.27], 2 kinds of cooperations are set:
>
> - CSE1 to CSE2 meaning that CSE1 takes advantage of the infrastructure, MN-CSEs, and AEs registered in CSE2, and also shares security policies of CSE2. CSE1 is a_CUSTOMER_ and CSE2 is a_PROVIDER._
>
> - CSE1 to CSE2 means that CSE1 and CSE2 mutually share infrastructure, MN-CSEs, and AEs and common security policies. CSE1 and CSE2 are *PEERS.*
>
> NOTE 2: CUSTOMER and PROVIDER are roles that conform an *asymmetric relationship* , while PEER is a role conforming a *symmetric relationship* . NOTE 3: Inside a single Service Provider, the SDA is not mandatory since it can be considered as PEER.

Semantic Discovery Routing (SDR): CSEs support a distributed Semantic Discovery Routing that listens for Advanced Semantic Discovery Query (ASDQ) and:

- i) reduces the Advanced Semantic Discovery Query (ASDQ) by means of the Semantic Query Resolution (SQR);
- ii) solves and forwards in a distributed way the queries;
- iii) reconstructs the partial results, sending back to the originator of the Advanced Semantic Discovery Query (ASDQ).

> NOTE: Generally, two kinds of routing are discriminated, namely:
>
> 1. “Exhaustive”. As example, in the case that a semantic resource exists somewhere in the CSEs network, then the system will explore the entire distributed network until it will found it.
> 2. “Non-exhaustive”. As example, even in the case a semantic resource that exists somewhere in the CSEs network, the system will explore part of the distributed network until it will be stopped.

Semantic Query Resolution (SQR): each CSE contains a Semantic Query Resolution capability that takes as input an Advanced Semantic Discovery Query (ASDQ) and:

- i) as output, produces a *normalized* Advanced Semantic Discovery Query (ASDQ);
- ii) produces a set of ordinary oneM2M Semantic Discovery Query (SDQ) from the normalized Advanced Semantic Discovery Query (ASDQ) one.

Semantic Recommendation (SR): capability in the CSE that takes routing decisions for forwarding a received Advanced Semantic Discovery Query (ASDQ)

> NOTE: This capability uses the Semantic Routing Tables (SRT) and the Semantics Discovery Agreement (SDA).

Semantic Routing Table (SRT): contained in each CSE provides suitable routes to propagate the discovery queries according to the SDA

3.2 Abbreviations

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

A/C Air Conditioner ACL Access Control List
ADN Application Dedicated Node
AE Application Entity
AHD Application Hosting Device AIOTI Alliance for Internet Of
Things Innovation
AL Authorization Level AMC Agriculture Monitoring administration
Centre
AMI Advanced Metering Infrastructure AMS Asset Management
System AP Applications Provider API Application Programming
Interface ARIB Association of Radio Industries and Business ARPU
Average Revenue per User ASD Advanced Semantic Discovery
ASDQ Advanced Semantic Discovery Query
ASDQL Advanced Semantic Discovery Query Language
ATIS Alliance for Telecommunications Industry Solutions BGP4
Border Gateway Protocol 4 BMS Building Management System
CCSA China Communications Standards Association CIS Customer
Information System CL Criticality Level CMS Cryptographic
Message Syntax CNF Conjunctive Normal Form
CP Care Provider CPU Central Processing Unit CSE Common
Services Entity
DAP Data Aggregation Point
DCS Distributed Control System DER Distributed Energy
Resources DMS Distribution Management System DNF Disjunctive
Normal Form
DNP Distributed Network Protocol DP Device Provider DR
Demand Response DRX Discontinuous reception DSO Distribution
System Operator DAP Data Aggregation Point DB DataBase DTG
Digital TachoGraph DVR Digital Video Recorder EGW Energy
GateWay EHR Electronics Health Record EMS Energy Management
System EP Equipment Provider
EPBA Equipment Provider Back-end Application ESI Energy
Services Interface ETC Electronic Toll Collection ETRI Electronics
and Telecommunications Research Institute ETSI European Telecommunications
Standards Institute ETWS Earthquake and Tsunami Warning System

EU European Union eUICC Embedded Universal Integrated Circuit
Card EV Electric Vehicle EVC Electric Vehicle Charging
EVCE Electric Vehicle Charging Equipment EVC-SP Electric Vehicle
Charging Service Provider FAN Field Area Network FFS For
Further Study FGT Formal Graph Topology
GPS Global Positioning System HAMS Home Automation Management
System HAN Home Area Network HEM Home Energy Management
HEMS Home Energy Management System HLR High-Level Requirement
HMI Human Machine Interface HSM Hardware Security Module HV
High Voltage I/F InterFace
IAC Irrigation Administration Centre
ICCID Integrated Circuit Card Identifier IEC International
Electrotechnical Commission IMSI International Mobile Subscriber
Identity IN-CSE Infrastructure Node - Common Services Entity
IP Internet Protocol ITS Intelligent Transportation System
LAN Local Area Network LATAM Latin American LDR Low Data
Rate LG Lucky Goldstar M2M Machine-to-Machine
M2MSP M2M Service Provider
Mca Reference Point for M2M Communication with AE
Mcc Reference Point for M2M Communication with CSE
MDMS Meter Data Management System MDM Medical Device Manufacturer
MDN Mobile Directory Number MDMMS Medical Device Monitoring &
Management Service MN Middle Node MN-CSE Middle Node - Common
Services Entity
MNO Mobile Network Operator MSCN M2M Service Capabilities
Network MSISDN Mobile Station International Subscriber Directory
Number MSP M2M Service Platform MTC Machine Type Communications
MV Medium Voltage M2M Machine to Machine NW NetWork
PAN Personal Area Network PC Personal Computer PEV Plug-in
Electric Vehicle PHEV Plug-In Hybrid Electric Vehicle PKCS
Public Key Cryptology Standards PLC Power Line Communications
PMU Phase Measurement Unit PPM Privacy Policy Manager
QoS Quality of Service RL Redaction Leve lRTU Remote
Terminal Unit RDF Resource Description Framework
SAREF Smart Applications REFerence ontology
SCADA Supervisory Control And Data Acquisition SDA Semantics
Discovery Agreement
SDQ Advanced Discovery Query
SDQL Semantic Discovery Query Language
SDQM Semantic Discovery resolution Query Mechanism
SDDTE Small Data and Device Triggering Enhancements SDR Semantic
Discovery Routing
SDREQ Semantic Discovery REQuest
SDRM Semantic Discovery Routing Mechanism
SDRP Semantic Discovery Routing Protocol
SGCG Smart Grid Coordination Group SGIP Smart Grid Interoperability

Panel SIM Subscriber Identity Module SLA Service Level Agreement SM Smart Meter SMS Short Message Service SN Sleepy Node SP Service Provider SPARQL Simple Protocol and RDF Query Language

SQR Semantic Query Resolution

SQRS Semantic Query Resolution System

SR Semantic Recommendation

SRQM Semantic Resolution Query Mechanism

SRS Semantic Recommendation System

SRT Semantic Routing Tables

SW SoftWare T&C Terms and Conditions

TSO Transmission System Operator TIA Telecommunications Industry Association TSDSI Telecommunications Standards Development Society, India TTA Telecommunications Technology Association

TTC Telecommunications Technology Committee TV TeleVision

UD User Device UE User Equipment UEPCOP User Equipment Power Consumption OPtimizations UIM User Identity Module USB Universal Serial Bus URI Universal Resource Identifier

WAM Wide Area Measurement WAMS Wide Area Measurement System

WAN Wide Area Network WCDMA Wideband Code Division Multiple Access WG Wireless Gateway WLAN Wireless Local Area Network

3GPP 3rd Generation Partnership Project

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in this document are to be interpreted as described in the oneM2M Drafting Rules [i.1]

5 Energy Use Cases

5.1 Wide area, energy related measurement/control system for advanced transmission and distribution automation

5.1.1 Description

Background:

- Phase Measurement Units (PMUs, aka Synchrophasors) in power electrical systems, is a technology that provides a tool for power system operators and planners to measure the state of the electrical system and manage power quality.
- PMUs are positioned across the high voltage (HV) transmission and Medium voltage (MV) distribution network, operated by transmission and distribution system operators (TSO/DSO) respectively, typically in a

substation where network node connections are made and the distribution of load is of importance.

- PMUs usually generate bulk statistical information transmitted hourly or daily or event based. They are capable of continuously monitoring the wide-area network status online, so continuous information streaming data will be available to control centres from hundreds of PMUs at once which requires a stable communication network with sufficient capacity and quality.
- The communications network that is used to collect, monitor and control electricity power systems (HV transmission and MV Distribution power systems) are usually owned by Electricity TSO/DSO and are very secure and reliable.
- PMUs are sampled from widely dispersed locations in the power system network and synchronized from the common time source of a global positioning system (GPS) radio clock. PMUs measure voltages and currents at diverse locations on a power grid and output accurately time-stamped voltage and current phasors, allowing for synchronized comparison of two quantities in real time. These comparisons can be used to assess system conditions.

Description:

- This use case shows the feasibility of High voltage /MV supervision through the interconnection of PMUs especially via mobile broadband communication networks. Thus not requiring any additional TSO/DSO internal network extensions especially in remote sites.
- Through analysis of PMU power state information collected in operator control centres (TSO/DSO), the TSO/DSO can send control information to PMUs, in the same mobile broadband communication network, to control the power flow in the power system.
- Transmission delay of less than a second for the transmission of PMU measurements in near real time to TSO/DSO in the case of control centres.
- Black-out causes propagates within minutes and sometimes only seconds through entire national and even international transport & distribution networks. So the transmission of control is critical in the range of less than seconds.

5.1.2 Source

oneM2M-REQ-2012-0030R07 Wide area Energy related measurement/control system for Advanced transmission and Distribution Automation

Note: from ETSI TR 102 935 v2.1.1 [i.2]

5.1.3 Actors

- Energy system operators:

  - Transmission System Operator (TSO) is responsible for operation, maintenance and development of the transmission network in its own control area and at interconnections with other control areas, long-term power system ability to meet the demand, and grid connection of the transmission grid users, including the DSOs.
  - Distribution System Operator (DSO) is responsible for operation, maintenance and development of its own distribution grid and where applicable at the connections with other grids, ensuring the long-term ability to meet the distribution demand, regional grid access and grid stability, integration of renewables at the distribution level and regional load balancing (if that is not done by the balance responsible party).
- Communication operator (s) provider of the access network (Telcos)
  - System operators and/or providers of service layer platform(s) which can provide services/common functionalities for applications that are independent of the underlying network(s).

5.1.4 Pre-conditions

Communication/connectivity networks (phase network) to collect the measurements from PMUs to centres.

5.1.5 Triggers

System conditions deducted from the analysis of collected data trigger a counter measure action for example to curtail or reduce power flow in a HV/MV transmission.

5.1.6 Normal Flow

Interactions between actors and system required for successful execution of the use case or scenario.

An example flow for the TSO scenario:

1. WAMS application subscribes to PMU data which is owed by the Transmission System Operator
2. Measurements requested are sent back through (service provider) Telco operator and System Operator to TSO centre for the WAM application
3. Measurements sent to the system operator are collected and can be stored by the operator.
4. Notification message is sent to WAMS application in TSO control centre when the system operator receives the measurement. WAMS application/TSO control centre can pull/push the data measurements
5. Based on measurements collected, WAMS application/ TSO control centre initiates a control command to shut down a transmission line under its controlled area

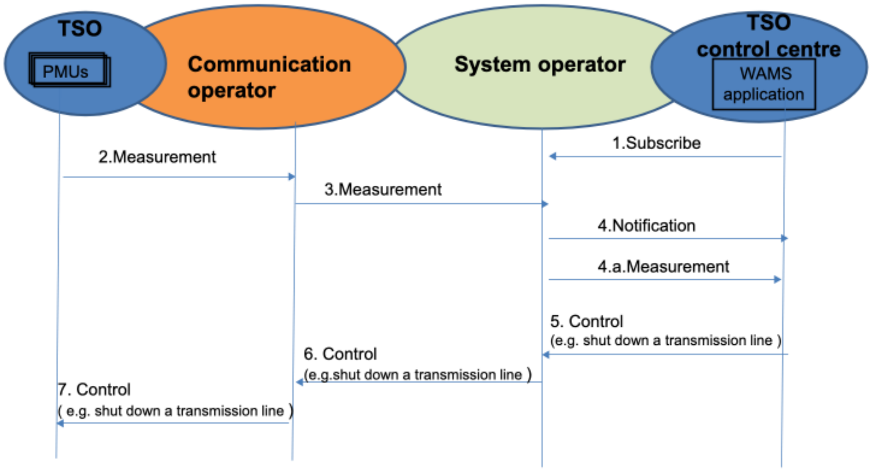


Figure 1: Figure 5.1.6-1 An example flow for the TSO scenario

6. The Control command is sent to system operator where an appropriate communication network is selected to send the control command
7. Then control command is sent by system operator to the PMU under TSO controlled area to initiate the execution of the command e.g. the shutdown of a specific transmission line

An example flow for DSO scenario:

1. WAMS application subscribes to the PMU data
2. Measurements are sent through Telco operator
3. Measurements sent to system operator where they are stored.
4. Notification sent to WAMS application in DSO control centre when the measurements are received by system operator. WAMS application in DSO control centre pulls the measurements
5. Based on measurements collected WAMS application in DSO control centre, initiates a control command to reduce flow in a particular region under its controlled area.
6. Control command sent to system operator where an appropriate communication network is selected to send the control command.
7. Then control command is sent to the PMU under DSO control to initiate the execution of the command e.g. the change of power flow.

5.1.7 Alternative Flow

None

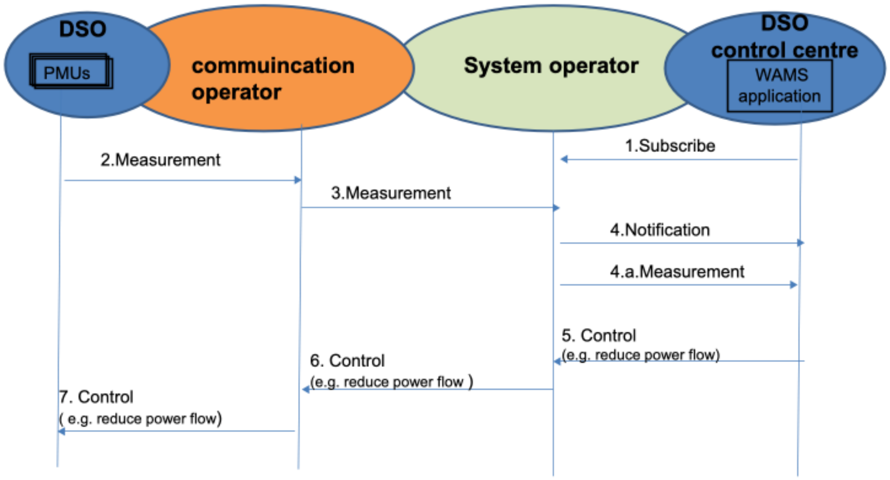


Figure 2: Figure 5.1.6-2 An example flow for DSO scenario

5.1.8 Post-conditions

Corrective or Restricted operation of power electrical network as a result of the preventive action because of the shut-down of (a part) power network.

5.1.9 High Level Illustration

5.1.10 Potential Requirements

Extracted from ETSI service requirements [i.3] (Ref TS102 689 V1.1.1) but suitable for this use case.

1. Data collection and reporting capability/function
   The M2M System (e.g. be owned by System Operator) shall support the reporting from a specific M2M Device (e.g. PMU) or group of M2M Devices or group of M2M collectors in the way requested by the M2M Application (e.g. WAM) as listed below:
   - a. a periodic reporting with the time period being defined by the M2M application;
   - b. an on-demand reporting with two possible modes. One is an instantaneous collecting and reporting of data, the other one is a reporting of the data that were pre-recorded at the indicated specific time period;
   - c. an event-based reporting e.g. transient fault (*Note specific time requirements FFS*)
2. Remote control of M2M Devices
   The M2M System shall support the capability for an Application to re-

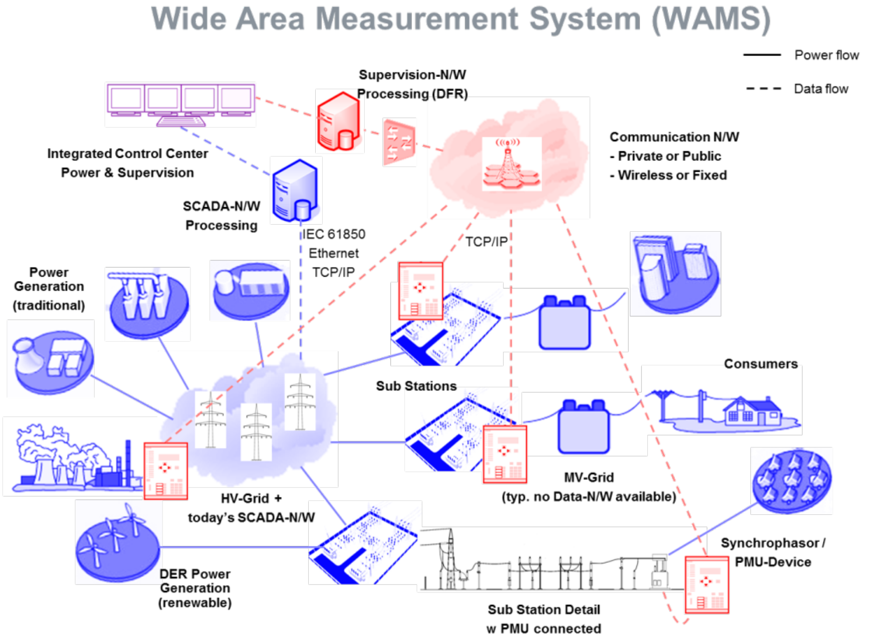


Figure 3: Figure 5.1.9-1 High Level Illustration of Wide Area Measurement System

motely control M2M Devices that support this capability; e.g. control power flow or shut down a regional power network to prevent a black-out event

3. Information collection & delivery to multiple applications
   The M2M System shall support the ability for multiple M2M Applications (in this use case the WAM) to interact with multiple applications on the same M2M Devices (in this case can interact with many PMUs) simultaneously
4. Data store and share
   The M2M System shall be able to store data to support the following requirements:
   - a. Provide functionality to store and retrieve data.
   - b. Establish storage policies for stored data (e.g. define maximum byte size of the stored data).
   - c. Enable data sharing of stored data subjected to access control
5. Security requirements
   - a. Authentication of M2M system with M2M devices/ /collectors
     The M2M system shall support mutual authentication with M2M Device or M2M Gateway/collector. For example mutual authentication may be requested between a service providers/operators and the entity requesting the service. The parties may choose the strength of authentication to ensure appropriate level of security.
   - b. Authentication of applications on M2M devices with M2M applications on the network
     When there is a request for data access or for M2M Device/Gateway access, the M2M Device or M2M Gateway access, the application on M2M Device or M2M Gateway shall be able to mutually authenticate or M2M Applications on the Network from which the access request is received.
   - c. Data integrity
     The M2M System shall be able to support verification of the integrity of the data exchanged.
   - d. Prevention of abuse of network connection
     M2M security solution shall be able to prevent unauthorized use of the M2M Device/Gateway.
6. Privacy
   The M2M System shall be able to protect confidentiality of collected information.
   - a. Security credential and software upgrade at the Application level.
     - i. Where permitted by the security policy, M2M System shall be able to remotely provide the following features, at the Application level:
     - ii. Secure updates of application security software and firmware of the M2M Device/Gateway.
     - iii. Secure updates of application security context (security keys and algorithms) of the M2M Device/Gateway.

- b. This functionality should be provided by a tamper-resistant Secured Environment (which may be an independent Security Element) in M2M Devices/Gateways supporting this functionality.

7. Continuous Connectivity
   The M2M System shall support continuous connectivity, for M2M applications requesting the same M2M service on a regular and continuous basis. This continuous connectivity may be de-activated upon request of the Application or by an internal mechanism in the M2M system.

5.2 Analytics for M2M

5.2.1 Description

The term "analytics" is often used to describe complex algorithms applied to data which provide actionable insights. Simpler algorithms may also provide actionable insights - here we use the term "compute" for them. Both "analytics" and "compute" may be used similarly by an M2M System to provide benefits to M2M applications. This use case uses a simple "compute" example to introduce the topic.

M2M application service providers may wish to use analytics for several purposes. There are many analytics providers who may offer their libraries directly to application service providers. However there are situations where application service providers may wish to apply analytics to their M2M data from devices before it is delivered to the "back-end" of the application "in the cloud".

To satisfy M2M application service provider needs, a oneM2M system may offer compute/analytics capabilities which may be internally or externally developed. Furthermore, these compute/analytics capabilities may be geographically distributed. Benefits to M2M application service providers might include:

- Convenience - due to integration
- Simplicity - due to a cross-vertical standardized analytics interface
- Cost savings - due to resource minimization (of compute, storage, and/or network)
- Improved performance - due to offloading/edge computing

M2M service providers may also benefit by deploying distributed compute/analytics to optimize operations such as regional management e.g. device/gateway software updates.

The use case described below assumes:

- millions of devices continuously report M2M data from devices at geographically diverse locations
- the M2M application is interested in receiving only certain sets of data based upon changes in particular data elements.

Use of oneM2M computation and analytics for anomaly detection and filtering avoids the use of bandwidth needed to transport unnecessary device data to the back-end of the M2M application. To enable the oneM2M system to do this, the M2M application specifies:

1. Which device data (the baseline set) is needed to create a baseline (which is indicative of “normal” operation).
2. The duration of the training period used to set a baseline
3. The method to create/update the baseline
4. Which device data (the trigger set) is to be compared to the baseline
5. The method of comparison between the baseline set and the trigger set.
6. The variation of M2M data in comparison to the baseline used to trigger action
7. Which data (the storage set) is to be stored in addition to the data used in the baseline.
8. Which data (the report set, which may include data from the baseline set, trigger set and the storage set) which is to be reported to the M2M application upon trigger.
9. “Location directives” which expresses where the device data collection point, storage and compute/analytics program and libraries should be located. (Distributed, possibly hierarchical locations may be specified, and may be defined by max response time to devices, geographic location, density of convergent device data flows, available compute/storage capacity, etc.).
10. “Lifecycle management directives” for compute/analytics program and libraries instances e.g. on virtual machines.

The action by the oneM2M system in response to a trigger in this use case is to send the filtered report set to the M2M application; however, other alternative actions are summarized below (which would require different information from the M2M application).

Example of distributed, non-hierarchical location of analytics use case - normal flow

A hierarchical version of this use case would locate different compute/analytics at different levels of a hierarchy.

5.2.2 Source

oneM2M-REQ-2013-0102R03 Analytics for oneM2M

5.2.3 Actors

Devices - aim is to report what they sense
Analytics library provider - aim is to provide analytics libraries to customers
M2M application service provider - aim is to provide an M2M application to users

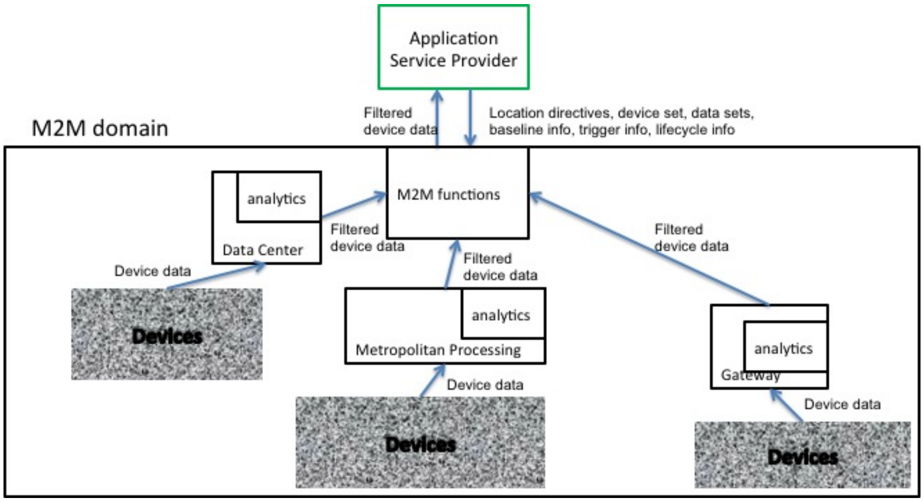


Figure 4: Figure 5.2.1-1 Analytics Use Case for M2M

5.2.4 Pre-conditions

Before an M2M system's compute/analytics may be used, the following steps are to be taken:

1. The M2M application service provider requests compute/analytics services from the oneM2M system. A request may include parameters required by analytics to perform computation and reporting, plus parameters required by the oneM2M system to locate and manage the lifecycle of the analytics computation instance (see 5.2.1).
2. The oneM2M system selects a source Analytics library provider for, and obtains the appropriate analytics library.
3. The oneM2M system provisions the appropriate analytics library at a location that meets the M2M application service provider's location directives.
4. The oneM2M system generates a program based upon the M2M application service provider's request.
5. The oneM2M system provisions the appropriate program based upon the M2M application service provider's request at the location(s) of step 3.
6. The oneM2M system starts collecting M2M data from devices and inputs them into the provisioned compute/analytics program for the duration of the baseline-training period. A baseline is established, which may include bounds for M2M data ranges, bounds for frequency of M2M data received, bounds for relative M2M data values to other M2M data values, etc.

5.2.5 Triggers

Triggering is described within 5.2.7.

5.2.6 Normal Flow

1. The devices provide M2M data to the oneM2M system.
2. The oneM2M system stores a set of M2M data (the storage set) from the devices
3. The oneM2M system uses analytics to compare M2M data (the trigger set) from devices with the baseline.
4. The oneM2M system determines whether the variation between the M2M data set and the baseline exceeds the specified bounds of the trigger condition, if it does then the following action occurs:
5. The oneM2M system sends the requested M2M data (the report set), to the M2M application service provider.

5.2.7 Alternative Flow 1

The action to be taken by the oneM2M system following a trigger may be different than step 11 above.

For example, the action may be to initiate conditional collection where for some duration or until some other trigger occurs.

- A. A current collection scheme of device data is modified e.g. more frequent updates, or
- B. A new collection scheme is initiated

Other alternative actions may include, but are not limited to:

- Initiating device/gateway diagnostics e.g. following a drop in the number of responding devices
- Sending control commands to devices
- Sending alerts to other oneM2M system services e.g. fraud detection
- Sending processed (e.g. cleansed, normalized, augmented) data to the application

5.2.8 Post-conditions

None

5.2.9 High Level Illustration

Concrete Example Oil and Gas

The above description is of the abstracted use case; a more concrete example is as follows:

Oil and gas exploration, development, and production are important potential use cases for M2M. To stay competitive energy companies are continuously increasing the amount of data they collect from their field assets, and the sophistication of the processing they perform on that data. This data can literally originate anywhere on Earth, is transported to decision makers over limited bandwidths,

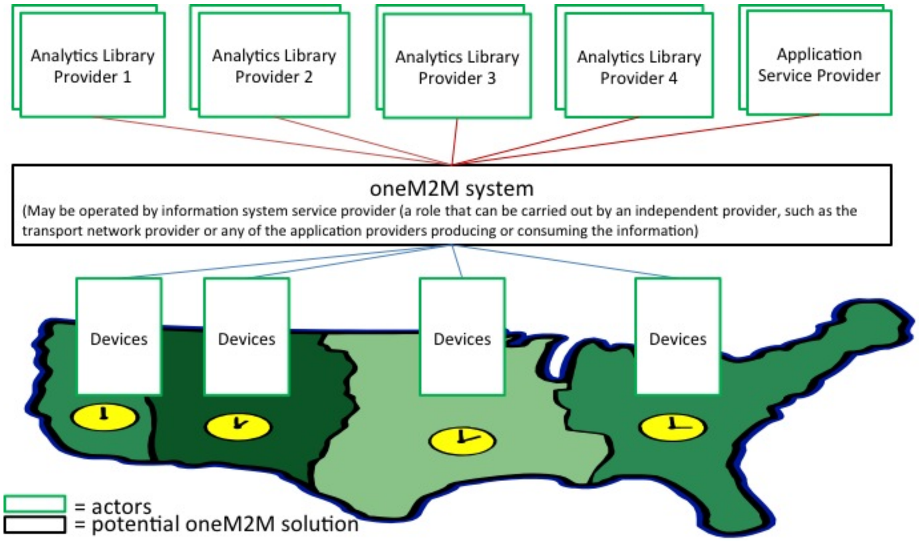

Analytics Library Provider 1
Analytics Library Provider 2
Analytics Library Provider 3
Analytics Library Provider 4
Application Service Provider
oneM2M system
(May be operated by information system service provider (a role that can be carried out by an independent provider, such as the transport network provider or any of the application providers producing or consuming the information)
Devices
Devices
Devices
Devices
= actors
= potential oneM2M solution

Figure 5: Figure 5.2.9-1 High level illustration of Analytics use case

and often must be reacted to on real-time time scales. An M2M system can prove very useful in its ability to perform analytics, data storage, and business intelligence tasks closer to the source of the data.

Oil and Gas companies employ some of the most sophisticated and largest deployments of sensors and actuators networks of any vertical market segment. These networks are highly distributed geographically, often spanning full continents and including thousands of miles of piping and networking links. Many of these deployments (especially during the exploration phases) must reach very remote areas (hundreds of miles away from the nearest high bandwidth Internet connection), yet provide the bandwidth, latency and reliability required by the applications. These networks are typically mission critical, and sometimes life critical, so robustness, security, and reliability are key to their architecture.

Oil and gas deployments involve a complex large-scale system of interacting subsystems. The associated networks are responsible for the monitoring and automatic control of highly critical resources. The economic and environmental consequences of events like well blowouts, pipeline ruptures, and spills into sensitive ecosystems are very severe, and multiple layers of systems continuously monitor the plant to drive their probability of occurrence toward zero. If any anomalies are detected, the system must react instantly to correct the problem, or quickly bring the network into a global safe state. The anomalies could be attributable to many different causes, including equipment failure, overloads, mismanagement, sabotage, etc. When an anomaly is detected, the network must react on very fast timescales, probably requiring semi-autonomous techniques and local computational resources. Local actions like stopping production, closing valves, etc. often ripple quickly through the entire system (the system can't just close a valve without coordinating with upstream and downstream systems to adjust flows and insure all parameters stay within prescribed limits). Sophisticated analytics at multiple levels aids the system in making these quick decisions, taking into account local conditions, the global state of the network, and historical trends mined from archival big data. They may help detect early signs of wear and malfunction before catastrophic events happen.

Security is critical to Oil and Gas networks. This includes data security to insure all data used to control and monitor the network is authentic, private, and reaches its intended destination. Physical security of installations like wells, pump stations, refineries, pipelines, and terminals is also important, as these could be threatened by saboteurs and terrorists.

There are three broad phases to the Oil and Gas use case: Exploration, Drilling and Production. Information is collected in the field by sensors, may be processed locally and used to control actuators, and is eventually transported via the global internet to a headquarters for detailed analysis.

Exploration

During the exploration phase, where new fields are being discovered or surveyed, distributed process techniques are invaluable to manage the vast quantities of data the survey crews generate, often in remote locations not serviced by high bandwidth internet backbones. A single seismic survey dataset can exceed one Petabyte in size. Backhauling this data to headquarters over the limited communications resources available in remote areas is prohibitive (Transporting a petabyte over a 20Mb/s satellite link takes over 12 years), so physical transport of storage media is currently used, adding many days of time lag to the exploration process. Distributed computing can improve this situation. A compute node in the field is connected to the various sensors and other field equipment used by the exploration geologists to collect the data. This node includes local storage arrays, and powerful processor infrastructures to perform data compression, analysis, and analytics on the data set, greatly reducing its size, and highlighting the most promising elements in the set to be backhauled. This reduced data set is then moved to headquarters over limited bandwidth connections.

Drilling

When oil and gas fields are being developed, large quantities of data are generated by the drilling rigs and offshore platforms. Tens of thousands of sensors monitor and record all conditions on the rig, and thousands of additional sensors can be located downhole on the drill string, producing terabyte data sets. Distributed compute nodes can unify all of these sensor systems, perform advanced real-time analytics on the data, and relay the appropriate subset of the data over the field network to headquarters. Reliably collecting, storing and transporting this data is essential, as the future performance of a well can be greatly influenced by the data collected and the decisions made as it is being drilled.

A subset of the data collected (wellhead pressure, for example) is safety critical, and must be continuously analysed for anomalies in real-time to insure the safety of the drilling operations. Because of the critical latency requirements of these operations, they are not practical for the Cloud, and distributed computing techniques are valuable to achieve the necessary performance.

Production

Once wells are producing, careful monitoring and control is essential to maximize the productivity of a field. A field office may control and monitor a number of wells. A computing node at that office receives real-time reports from all the monitoring sensors distributed across the field, and makes real-time decisions on how to best adjust the production of each well. Some fields also include injection wells, and the computing node closes the feedback loop between the injection rates and the recovery rates to optimize production. Some analytics are performed in the local computing node, and all the parameters are stored locally and uplinked to headquarters for more detailed analysis and archiving. Anomalies in sensor readings are instantly detected, and appropriate reactions are quickly computed and relayed to the appropriate actuators.

The Pump Station shown also includes a computing node. It is responsible for monitoring and controlling the pumps / compressors responsible for moving the product from the production field to the refinery or terminal in a safe and efficient manner. Many sensors monitor the conditions of the pipelines, flows, pressures, and security of the installation for anomalous conditions, and these are all processed by the local computing node.

Conclusion

The oneM2M Services Layer could offer “cloud-like” services to M2M Applications of computation/analytics functions commonly used across verticals, where those functions are optimally placed near to the sources of M2M data.

These services could include:

1. Advertisement of services to M2M Applications
2. Acceptance of M2M Applications’ directives over the “North-bound” interface.
3. Selection of where the requested computation/analytics functions are optimally placed
4. Provisioning and maintenance of virtual machine and computation/analytics functions (provided by oneM2M provider or 3rd party)
5. Redirection of M2M traffic to the virtual machine
6. Delivery of virtual machine output to other virtual machines or directly to M2M Applications (e.g. of filtered M2M data)

The M2M Applications and the M2M Service Provide may benefit from these services:

- oneM2M Services Layer use of virtual machines on behalf of M2M Appli-

cations (e.g. to trigger new/modified data collection or device diagnostics or low latency M2M Device control)
- oneM2M Services Layer use of virtual machines on behalf of the oneM2M Service Provider (e.g. optimized device management, fraud detection)

5.2.10 Potential requirements

1. The oneM2M system should be able to accept standardized inputs from M2M application providers which request compute/analytics services. > Note: Many Analytics APIs exist today, the most popular one being Google analytics service
2. The oneM2M system should be able to select analytics libraries from Analytics library providers.
3. The oneM2M system should be able to locate and run instances of compute/analytics programs and libraries at locations requested by M2M applications service providers.
4. The oneM2M system should be able to manage the lifecycle of instances of compute/analytics programs and libraries.
5. The oneM2M system should be able to steer device data to inputs of instances of compute/analytics programs
6. The oneM2M system should be able to take operational and management action as a result of analytics reports received.
7. The oneM2M system should specify supported compute/analytics triggers and actions.

5.3 Smart Meter Reading

5.3.1 Description

This clause provides selected Smart Meter Reading use cases

5.3.2 Source

oneM2M-REQ-2013-0217R02 Smart Meter Reading Use Case

> Note: use case information extracted from SGIP/OpenSG

REQ-2015-0563 pCR on smart meter reading

5.3.3 Actors

- Smart Meters (SM), Data Aggregation Points (DAPs),
- Advanced Metering Infrastructure (AMI) Head-end,
- Meter Data Management System (MDMS),
- Customer Information System (CIS)

5.3.4 Pre-conditions

Availability of meter data.

Smart Meters which are deployed in a block (e.g. same house, building, community, etc.) with the same behavior based on default configuration or charging policy could be assigned as a group.

5.3.5 Triggers

Smart meter on-demand or bulk interval meter read request events

5.3.6 Normal Flow

Smart Grid Interoperability Panel (SGIP) (http://www.sgip.org) and OpenSG users group (http://osgug.ucaiug.org/default.aspx) have been leading this effort in North America. An informative document has been submitted to OneM2M based on the SGIP activity. In general, a number of external organizations such as the SGIP or the SGCG (Smart Grid Coordination Group) in Europe have been working to define use cases for Smart Grid (SG). Portals such as the Smart Grid Information Clearing House (http://www.sgiclearinghouse.org) to assist with distributing information about smart grid initiatives in the US. The use-cases presented are derived in part from the above publicly available information.

Figure 5.3.6-1 shows the conceptual actors/data flow diagram based on a more detailed diagram developed by SG-Net. The more detailed diagram developed by SG-Net can be seen in the associated submission related to SGIP-based Smart Grid Use Cases.

In Figure 5.3.6-2 each element is an "actor" that is communicating with another actor using the shown data flows. As an example, consider "Smart Meter" in the "Customer" quadrant (lower right). Smart Meter (SM) communicates with a number of other actors, such as a Data Aggregation Point (DAP) located in the AMI Network. The DAP can then transmit the aggregated data to the Utility Service Provider using the Wide Area Network. The meter reading information can reach the data centre for the Utility Service Provider via the AMI Headend which can forward the information to the MDMS which can coordinate with the CIS to store/retrieve meter data and to determine customer billing information. In certain variations such as cellular-based smart metering systems, a DAP entity may be bypassed, or merely serve as a pass-through for the information flow between the utility data centre and the smart meter.

Typically, a utility data centre processing application communicates end-to-end via the AMI Headend with a smart meter data application at the edge. Figure 5.3.6-2 shows two possible flows A and B depending on whether there is a DAP entity along the path from the Utility Data Centre / AMI Headend and the Smart Meter.

In flow A, the Utility Data Centre / AMI Headend can make a request to the Smart Meter directly. Typically there may be 3 to 6 such requests per day (typically $<$ 10 times per day). The request could indicate that the current

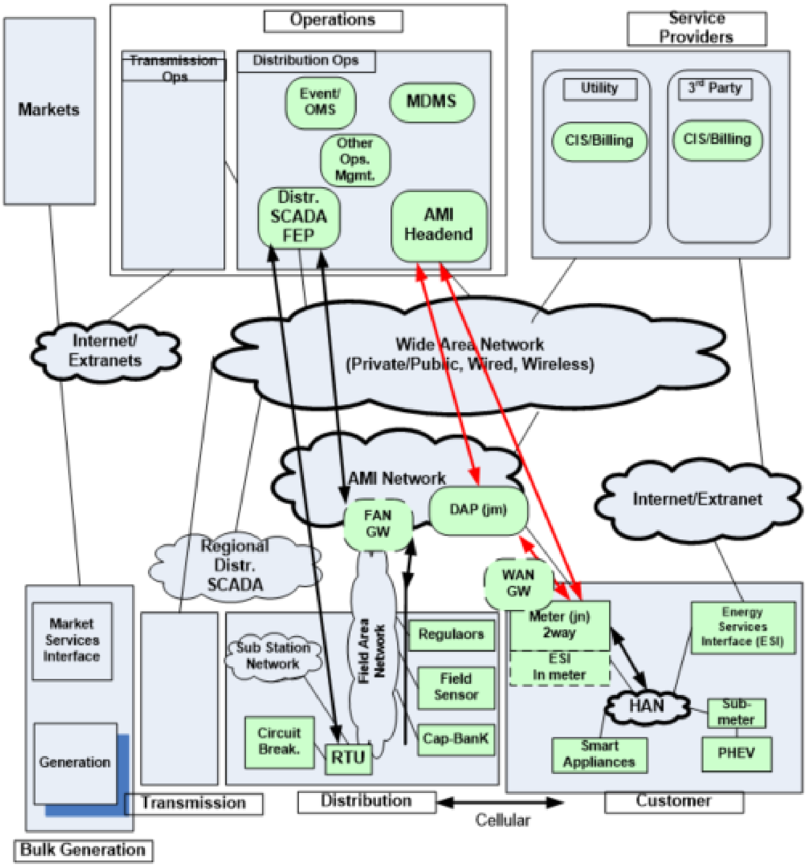


Figure 6: Figure 5.3.6-1 Conceptual Actors/Data Flow Diagram

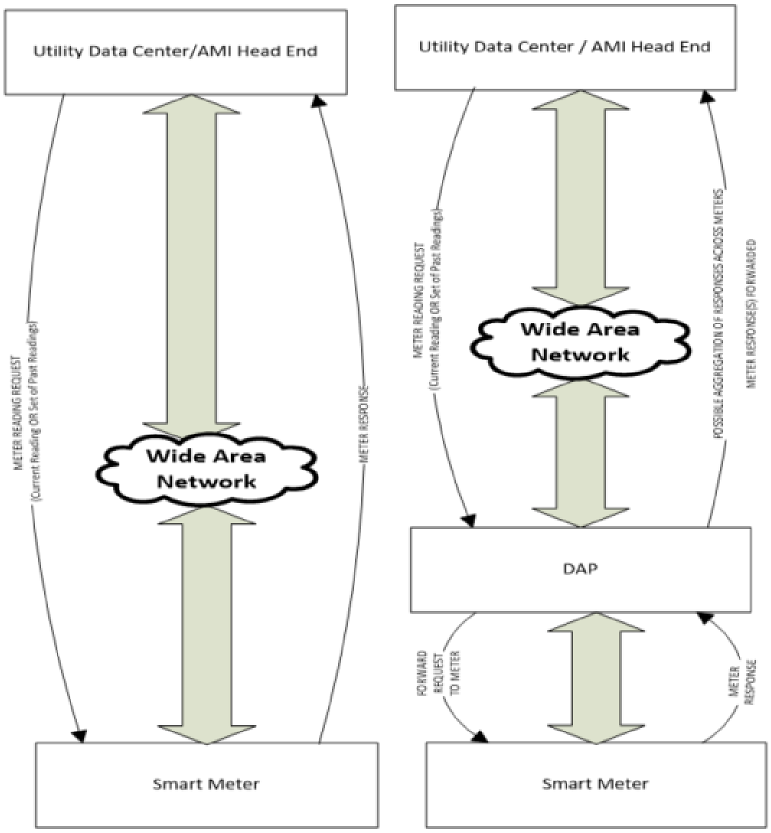

Utility Data Center/AMI Head End
METER READING REQUEST
(Current Reading OR Set of Past Readings)
Wide Area Network
METER RESPONSE
Smart Meter
Utility Data Center / AMI Head End
METER READING REQUEST
(Current Reading OR Set of Past Readings)
Wide Area Network
POSSIBLE AGGREGATION OF RESPONSES ACROSS METERS
METER RESPONSE(S) FORWARDED
DAP
FORWARD REQUEST TO METER
METER RESPONSE
Smart Meter

Figure 7: Figure 5.3.6-2 Typical Smart Meter Reading Flows A (on left) and B (on right)

meter reading is desired. Alternatively, multiple meter readings over a period of time such as for a few hours (e.g. from 2 p.m. to 8 p.m.) for a given day or across days could be requested. The Smart Meter completes the request and communicates it back to the Utility Data Centre / AMI HeadEnd. Typical in such on-demand or bulk-interval read requests, a reasonably immediate response is desired of the order of a few seconds, so that there is not necessarily any significant delay tolerance allowed for the response. However, it is possible that, in current systems or in future systems, such requests could optionally carry a delay tolerance associated with the request depending on the urgency of the request. The size of the meter reading response can be of the order of a few tens to hundreds of bytes, and is also implementation dependent.

In flow B, the Utility Data Centre / AMI Headend can make a request to the Smart Meter that can be received via the DAP. Typically there may be 3 to 6 such requests per day (typically $<$ 10 times per day). The request could indicate that the current meter reading is desired or that multiple meter readings over a period of time are desired. The Smart Meter completes the request and sends its response to the DAP. This response from the Smart Meter to the DAP is typically desired in the order of 15 to 30 seconds, as suggested in the submitted informative document related to SGIP-based Smart Grid Use Cases. However the actual delay in processing can be implementation dependent across smart metering systems across the world. The size of the meter reading response can be of the order of a few tens to hundreds of bytes, and is also implementation dependent.

In case that the Smart Meters belong to a group, there are two ways to distribute the request from the Utility Data Centre / AMI Headend to Smart Meters: the Utility Data Centre / AMI Headend sends a request to DAP then DAP distributes it to all Smart Meters, or the Utility Data Centre / AMI Headend sends same requests to all Smart Meters via DAP which acts as a router. There are several ways to submit the data from Smart Meters to the Utility Data Centre / AMI Headend: The DAP entity can buffer the data for some time, receive data from many meters, and then submit the aggregated data across meters to the Utility Data Centre / AMI Head End. The duration for which the DAP may buffer data can be implementation dependent, and could last for several seconds or minutes. In some variants, the DAP may serve merely as a router, so that it directly forwards the smart meter response to the Utility Data Centre / AMI HeadEnd without performing any aggregation tasks. In further variants, the DAP entity could be merely a virtual processing entity and not a physical one, where such a virtual entity could even potentially reside on the other side (not shown) of the wide area network associated with the Utility Data Centre / AMI Head End. For instance, the Utility Data Centre / AMI Headend could send a request to DAP for distributing it to all Smart Meters in a group, and if the DAP belongs to the third party, the DAP shall serve as a router to directly forward the smart meter response to the Utility Data Centre / AMI HeadEnd without performing any aggregation tasks.

Summary

To summarize, meter reading requests could request a single meter reading or a set of meter readings. Such requests may occur a few times (typically < 10) per day and can be of the order of a few tens of bytes. Meter reading responses can be of the order of a few 10s to 100s of bytes typically. Meter reading responses are typically expected in the order of a few seconds after reception of the request at the meter. Any delay tolerance associated with such requests can be optional or implementation dependent. In some system variants, a DAP entity may not exist at all so that the Utility Data Centre / AMI Head End communicates directly with the smart meter. In other end-to-end system variants, a DAP entity may serve as an intermediate processing or forwarding entity between the Smart Meter and the Utility Data Centre / AMI Head End. In such cases, the DAP entity may be either a physical or virtual processing entity in the end-to-end system and can assist with buffering and aggregating meter reading responses. The duration of buffering or aggregation at the DAP entity can be implementation dependent and could be of the order of a few seconds or minutes typically.

5.3.7 Alternative Flow

None

5.3.8 Post-conditions

None

5.3.9 High Level Illustration

None

5.3.10 Potential Requirements

1. The M2M System shall be able to provide identity verification between the M2M device and the M2M server.
2. The M2M System shall be able to protect confidentiality of data (i.e. Smart Meter Response), even when DAP is deployed by the third party.

5.4 Environmental Monitoring of Remote Locations to Determine Hydropower

5.4.1 Description

Monitoring environmental parameters and effects in remote locations is of increasing interest due to the rapidly changing Global Climate and the world in general. Parameters such as temperate, pressure, water levels, snow levels, seismic activity have significant effects on applications such as green energy (wind and hydro power), agriculture, weather forecasting and tsunami warnings.

The demand for remote monitoring information (real time and historical) has been increasing over the past decade and expected to increase exponentially in the foreseeable future.

Environmental monitoring is a M2M application where satellite is the only communications alternative as no other infrastructure is generally in such remote localities. This case study attached presents one solutions where satellite communication is commonly used for environmental monitoring. This is Hydro power generation through snow/water monitoring.

This attached paper provides an overview of the solution and how satellite is used to support this requirement. The document also outlines why the solution requires M2M remote satellite communications.

5.4.2 Source

oneM2M-REQ-2013-0123R02 Use-case Hydro-Power Monitoring Satellite

5.4.3 Actors

Energy companies

5.4.4 Pre-conditions

Two main requirements exist for remote monitoring in Hydro Power Generation. Firstly, there needs to be monitoring of the flow and supply of water to generate the power itself. Secondly, there needs to be monitoring of the environmental impact the hydro-electricity has on surrounding ecosystems for the storage of water and resulting change in natural flow.

Flow and Supply of Water: Availability and supply of water is fundamental to hydro generated power and is very seasonal and related to the regional climate. In cold climates such as Canada and Norway, water is supplied by snow where reservoirs are located in high locations and catchment areas cover extensive mountain regions. Snow levels, melting periods and supplies are inconsistent throughout the year. Reservoirs and storage facilities are designed to take into account seasonal inconsistencies from mother nature. In more tropical areas such as Brazil, tropical downfalls in the wet seasonal periods are important for flow management and are also seasonal.

Regardless of region, accurate sensors are critical to monitor water flow and supply such as rain fall, snow levels, snow temperature, snow wetness, reservoirs levels and other seasonal parameters. These sensor readings are critical to ensure Hydro companies can accurately predicate and monitor power generation levels. Sensor readings need to be sent back in near real time to Hydro processing plants to maintain operations. The location for the sensors are in mountainous and hard to reach areas that experience harsh environmental factors, partially high water/snow falls. Power or communication infrastructure is generally not available; therefore reliable satellite communication is the only option.

Sensor data is sent back consistently at short interval rates generally every five minutes from a number of multiple sensors in each location. Monthly usages in the region of 5 MB-10MB per month are typical depending on the number of sensor registers to poll and the M2M SCADA (supervisory control and data acquisition) communication protocol used (e.g. Modbus or priority protocol protocols used such as Totalflow).

Environmental impact that hydro-electricity has on surrounding ecosystems: Hydro-Electricity has the potential to affect the local ecosystems upstream and downstream from the generating plants. Government and world regulations are in place to ensure these systems minimize the impact on the local environment. Close monitoring and reporting of the surrounding areas are also part of the monitoring solution. Factors such as soil salinity, water levels, fish stock levels and erosion are some parameters that could be potentially monitored to ensure regulation and adhered to. This type of data is not critical for the power generation, however is required historically for trend analysis. Near real time communications is require for these types of sensors.

Sensor data is sent back long consistently interval rates generally every 30 minutes to 1 hour from a number of multiple sensors in each location. Monthly usages in the region of 1 MB-2 MB per month are typical, depending on the number of sensor registers to poll and the M2M SCADA communication protocol used.

5.4.5 Triggers

Two triggers that initiate information being sent over this architecture.

- Constant polling and
- Conditional polling.

Constant Polling: Sensor polling rates are set by the Hydro operator. This information is used at the host to provide real time data as well as historical for trending analysis. Polling rates depend on the rate of change in environmental changes or how often data is required to make decision on flow rates through the Pembroke. Rates could be every few minutes up to few hours, but rates are constant. This data is very important to determine power requirements for the satellite terminal. The more data the more power that is required.

Conditional Polling: Information can be sent from the RTU based on specified events, sharp rise in water levels, temperate and any specific data. This data must be fed back to the Hydro control (host) in the event critical controls need to be made on the Hydro station.

5.4.6 Normal Flow

Remote Sensor/Satellite Terminal Integration: Remote sensors are normally connected to a Remote Terminal Unit (RTUs) that condition the sensors values into registers that are transmitted (over satellite) to a host. The RTU polls (or changes register value in some circumstances) register values from Programmable

Logic Controllers (PLCs) that are connected to the aforementioned sensors. The RTU will then use a M2M (SCADA) communication protocol to send the register values to the host. SCADA protocol are designed to be very compact, only sending the minimum require data to the host, thus why serial based communication is popular. Modbus, DNP3 (Distributed Network Protocol), IEC 61850 [i.17] (used in electrical substations) or other priority based communication protocols are used and are generally based around serial communication to keep traffic to a minimum. IP is starting to become more popular to support these SCADA protocols.

The host resides in a corporate network of the Hydro provider, which analyses and presents this data into meaning information to make decisions on. The host is normally a hydro-power monitoring application designed specifically by the hydro provider that is integrated with the remote monitoring sites and controls for the Hydro plant. The host normally has a very advanced Human Machine Interface (HMI) to process data to a human operator, and through this, the human operator monitors water flow and controls the amount of water flowing through the penstock to the turbine.

As mentioned, RTUs communicate via either serial (RS-232/485) or IP layer 2 M2M SCADA protocols. Majority of modern based satellite communications systems support IP only layer two protocols and it is very common for RTUs to communicate via serial only. Terminals servers are usually placed in line between RTUs and satellite terminals where serial communication is required.

Satellite Service solution: L Band satellite service are the most popular used by Hydro plants in LATAM and North America. The L band satellite service operates over the L band frequency range (1.5GHz to 1.6GHz). This band is unique as it is not attenuated by weather where other high frequency band solutions operate in. Remote terminals in this application must be able to operate in wet tropical and cold snow ranges.

The terminal normally provides a direct IP network connection to the customer corporate control network (backhaul) via secure IP VPNs or leased line. A backhaul satellite solution is sometimes used for increased reliability. The L band satellite network must offers geographical redundancy for downlink earth station and backhaul infrastructure.

Satellite Terminal Solution: The L band satellite terminal must operate with extremely low power, less than 1W idle and 20W transmit. Majority of power used by remote terminals is used during the idle state. Solar power designs are suitable for the most modern L band satellite terminals terminal to operate in remote locations.

Remote terminal management and control is essential for this remote application. The terminal must continually ensure the terminal is on-net. If the terminal seems to be unable to transmit (or receive), the terminal automatically must reboots and reconnects itself to the network (known as watchdog). This removes the requirement to send someone to reboot the terminal. Remote management is conducted via out of band signalling. Terminal status, manual reboot and remote firmware updates are also essential of the operation of the remote terminal.

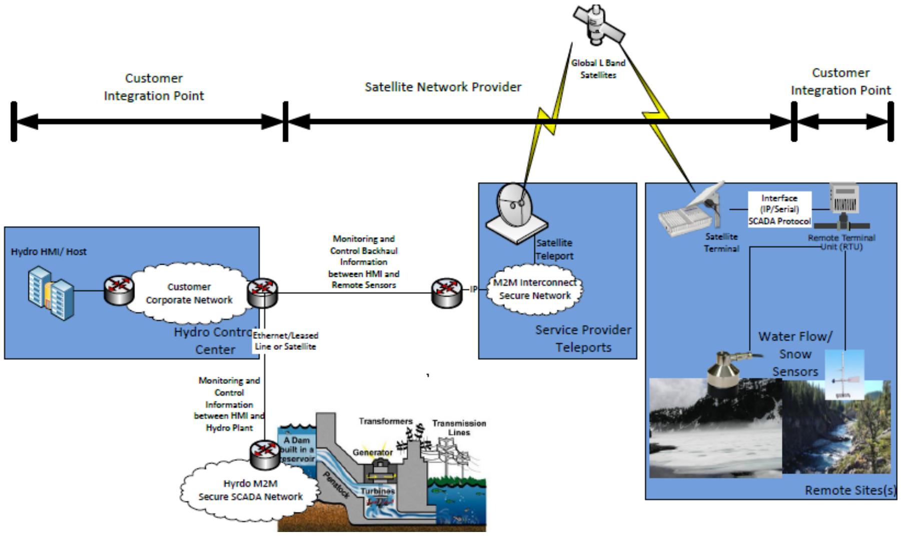
5.4.7 Alternative Flow

None

5.4.8 Post-conditions

None

5.4.9 High Level Illustration



Global L Band Satellites
Customer Integration Point
Satellite Network Provider
Customer Integration Point
Hydro HMI/ Host
Customer Corporate Network
Hydro Control Center
Monitoring and Control Backhaul Information between HMI and Remote Sensors
IP
Ethernet/Leased Line or Satellite
Satellite Teleport
M2M Interconnect Secure Network
Service Provider Teleports
Satellite Terminal
Interface (IP/Serial) SCADA Protocol
Remote Terminal Unit (RTU)
Water Flow/ Snow Sensors
Remote Sites(s)
Monitoring and Control Information between HMI and Hydro Plant
A Dam built in a reservoir
Transformers
Transmission Lines
Generator
Penstock
Turbines
Hyrdo M2M Secure SCADA Network

Figure 8: Figure 5.4.9-1 High Level Illustration of Environmental Monitoring for Hydro-Power Generation using Satellite M2M

5.4.10 Potential Requirements

1. The M2M System shall provide mechanisms for ensuring round trip communications of specified times from sensors to actuators.
2. The M2M System shall support power constrained devices.
3. The M2M System shall support an M2M Application's choice of communications transport characteristics e.g. Reliable or unreliable.
4. The M2M System shall support commonly used communications mechanisms for local area devices, e.g. RS-232/RS422.
5. The M2M System must provide communication availability to exceed 99.5% (1.83 days/year).

5.5 Oil and Gas Pipeline Cellular/Satellite Gateway

5.5.1 Description

This use case addresses a cellular gateway to transport oil and gas pipeline data to a backend server, to remotely monitor, manage and control devices equipped in the pipeline (e.g. meters, valves, etc.).

Oil and gas companies can have meters are remote destinations that makes manual monitoring of the state of these meters as an expensive task to be pursued on a regular basis. Automated monitoring of oil and gas pipeline data can streamline the remote monitoring and management of these remote pipeline meters.

When a fault is monitored on specific link of the pipeline network, it is necessary to open or shut the pipeline valve to block the link or to provide detour route. Also, when there is a necessity to change the quantity of oil and gas in pipeline, the valves should be damped through remote control.

5.5.2 Source

oneM2M-REQ-2013-0294R01 Oil and Gas Pipeline Cellular/Satellite Gateway
oneM2M-REQ-2013-0399 Additional Use Case for Oil and Gas UC

5.5.3 Actors

Oil and gas pipeline meters, valve controllers, cellular networks, backend servers, remote monitoring, management and control software

5.5.4 Pre-conditions

Cellular network connectivity, Satellite connectivity

5.5.5 Triggers

New pipeline sensor data requiring transport to a backend server

Network dynamic access constraint or network utilization constraints or prior network access policy constraints or device energy minimization considerations can cause delay tolerant sensor data to be buffered (and aggregated if needed) at the gateway and transmitted at a later time

Processing of recent measurements can result in remote requests for additional or more frequent measurements

A firmware upgrade becomes available that needs to get pushed to the gateways

5.5.6 Normal Flow

Sensor data related to oil/gas quantity and quality, pressure, load, temperature, and consumption data is forwarded to backend server that is processed by a remote monitoring service associated with the oil and gas pipeline. Pipeline sensors and pipeline cellular gateways can communicate with each other wirelessly (if sensors and gateways are different nodes in the system). Pipeline cellular or satellite gateways can serve as aggregation points. Sensor data may be locally forwarded until it reaches a gateway or directly transmitted to the gateway depending on proximity of the sensor(s) to each gateway on the pipeline.

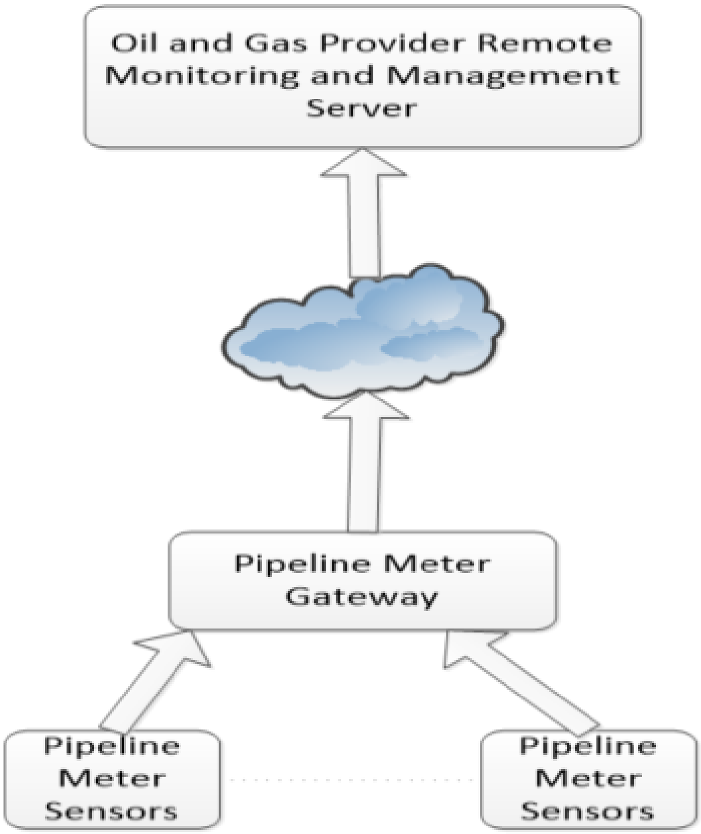


Figure 9: Figure 5.5.6-1 Flow - Oil and Gas Pipeline Gateway

5.5.7 Alternative Flow

Alternative Flow 1

Pipeline meter data can be stored, aggregated, and forwarded at an appropriate time based on network availability constraints or policy constraints or energy minimization constraints for the pipeline meter gateway. Transmission policies can be designed made to minimize network overhead.

Alternative Flow 2

Pipeline meter data can be processed by the remote monitoring and management service. If any anomalies are detected, additional measurements could be triggered, or more frequent measurements could be triggered, or measurements by additional sensors can be triggered by the remote service manager. Firmware upgrades can also be provided by the remote management service. Remote measurement requests are typically triggered or polled only as absolutely needed so as to avoid the overhead of unnecessary polling and network congestion using such schemes with Normal Flow or Alternative Flow 1 preferred for reporting sensor data.

Alternative Flow 3

Valve control data should be delivered in real-time. For this purpose, Pipeline Meter Gateway can be used to transport valve control data as well. The Gateway should be connected to and control the targeted valve controllers.

5.5.8 Post-conditions

Sensor data is stored in a database associated with the backend server. Remote monitoring service verifies the status of the different pipeline meters.

1. Alternative Flow 1
   Data is buffered and transmitted when the network or policy constraints or energy optimization constraints allow transmission of delay-tolerant pipeline sensor data
2. Alternative Flow 2
   More frequent or additional measurement request events can get triggered from the network based on processing of recent measurement data.
3. Alternative Flow 3
   When a valve controller received errored information from the gateway, the valve controller should send a request of retransmission to the gateway.

5.5.9 High Level Illustration

5.5.10 Potential Requirements

Rationale

This use case sets out from the presence of a gateway between one or more oil and gas pipeline sensor(s) and a backend server. One gateway node may serve multiple pipeline sensors and data may be forwarded multi-hop until it reaches a gateway. Data mules can collect data and dump the information at a gateway for transportation. The ability to locally forward data wirelessly between nodes to a local aggregation point serving as a gateway may be desirable depending on

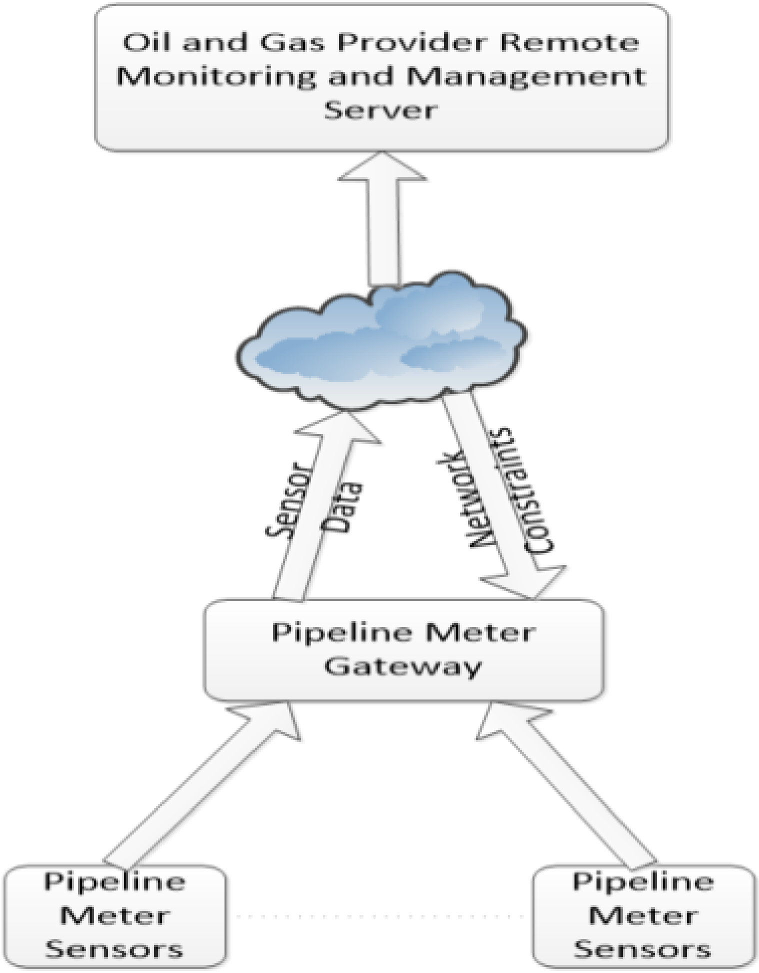


Figure 10: Figure 5.5.7-1 Alternative Flow 1 - Oil and Gas Pipeline Gateway

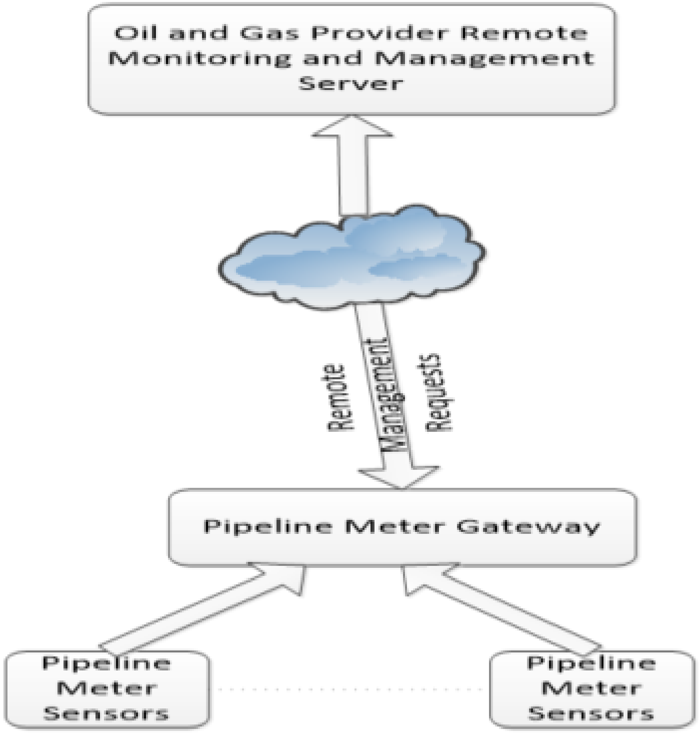

Oil and Gas Provider Remote Monitoring and Management Server
Remote Management Requests
Pipeline Meter Gateway
Pipeline Meter Sensors
Pipeline Meter Sensors

Figure 11: Figure 5.5.7-2 Alternative Flow 2 - Oil and Gas Pipeline Gateway

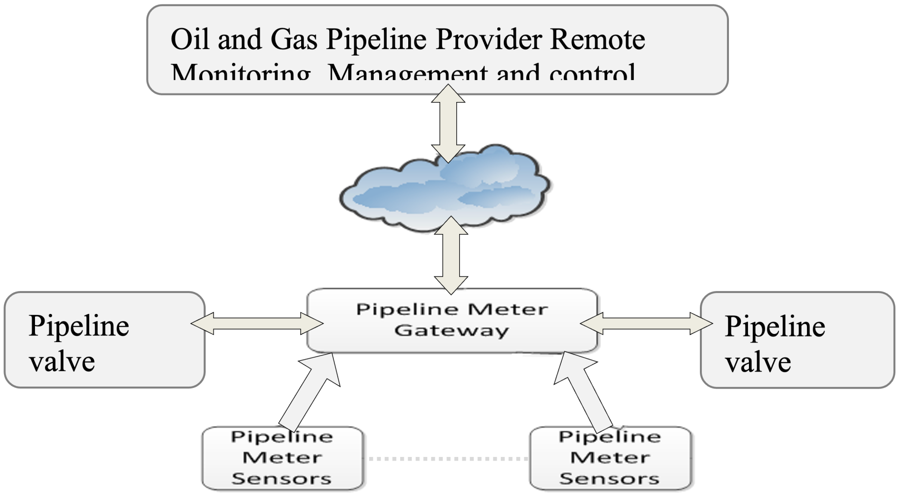


Figure 12: Figure 5.5.7-3 Alternative Flow 3 - Oil and Gas Pipeline Gateway

the location of sensor nodes and gateway nodes. Even though the use case is assuming a cellular/satellite gateway, this restriction is not needed in general.

Resulting requirements:

1. The M2M system shall be capable of supporting gateway nodes that are capable of transporting sensor measurements to back end servers.
2. The M2M system shall be capable of supporting static or mobile peer forwarding nodes that are capable of transporting sensor measurements to a gateway node.

Rationale

Pipeline sensors can measure data at predetermined times. Pipeline sensors can also take measurements at random times or based on a request from a backend server to study the health of the pipeline. Therefore, new measurement data may become available at any time. When measurement data is available, the data can be processed locally to understand the criticality of the information. Based on the criticality/urgency of the information, the data can be transported over the network immediately or in a delay-tolerant manner. If an anomaly is detected with regard to the measured data, more frequent measurements may be taken locally or requested from the backend server, to continually assess the criticality of the situation. In case there is no new or relevant information, the system may choose not to transport unnecessary data to reduce network or reduce device energy usage.

Resulting requirements:

3. Whenever a pipeline sensor has measurement data available, it shall be

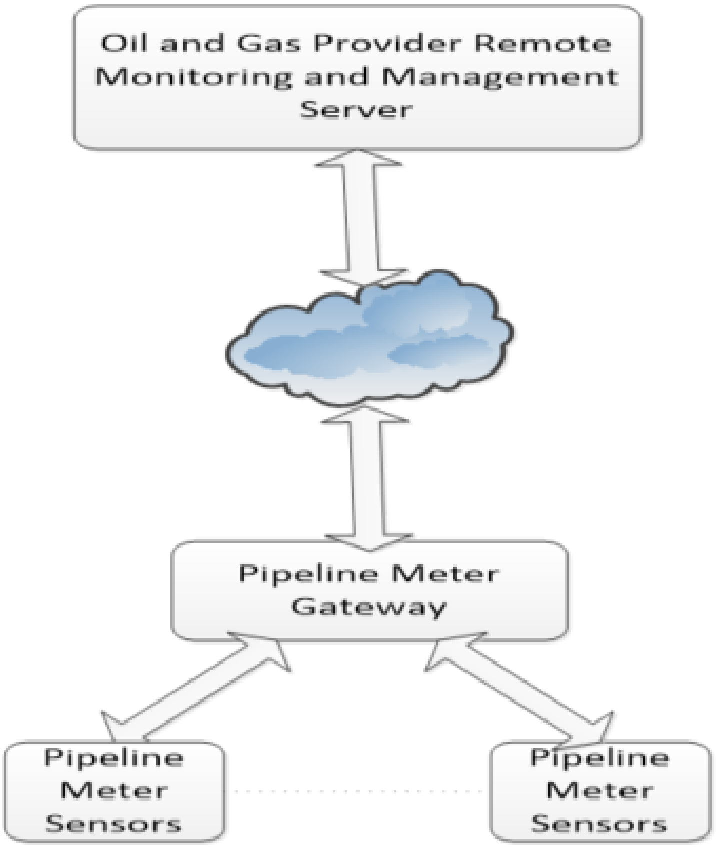


Figure 13: Figure 5.5.9-1 High Level Illustration - Oil and Gas Pipeline Gateway

possible for the sensor to send a request to the local pipeline gateway to transport new measurement data to the backend server.

4. Whenever measurement data is available, it shall be possible for the pipeline sensor or a local processing node/gateway to process the information and assess the urgency or criticality of the information, and tag the data appropriately to be critical/urgent or delay-tolerant.
5. Whenever measurement data is available that is determined to be critical/urgent, it shall be possible for the local gateway to send the information to a backend server as soon as possible (such as within in a few 100s of ms). Delay-tolerant data shall be transported within the delay tolerance specified.
6. Whenever measurement data is available that is determined to be not important, the system may choose to not transport the data to reduce network usage or to reduce device energy usage.
7. More frequent measurements may be taken such as when one or more anomalies are detected in the system, which can result it more data and more frequent urgent transmissions in the system, depending on the criticality of the data.

Rationale

Local analytics service functions can be executed to process sensor information. A service function could consist of evaluation rules based on sensor data, and decisions based on rules associated with the data. An evaluation engine can process the rules to then decide whether/when to transmit data. Analytics processing can also be done in a distributed manner, with additional processing on the backend server, or configurability of the evaluation rules at the local gateway by the backend server.

Resulting requirements:

8. A local analytics service function can be executed on the local processing gateway based on evaluation rules associated with the measurement data, and decisions can be taken based on the processing.
9. A distributed analytics service function can be executed in collaboration with a backend server, where additional processing of data can be performed at the backend server, or where the rules associated with local processing can be configurable by a backend server.

Rationale

Incoming requests from the pipeline sensor to the pipeline gateway may not result in immediate forwarding of the data to the backend server if any of the following is applicable: Dynamically changing cellular network availability (coverage); cellular network utilization constraints (policies); device energy consumption or memory constraints. In one of the flows also the quality of the data to be transported (alert=high priority) was relevant for determining when the connection needs to be triggered. Categorization of traffic such as abnormal/urgent data such as a pipeline failure, versus normal traffic can be done at the gateway. Tagging and processing such traffic differently based on application/network/device constraints can be done at the local processing gateway. The system should allow a provisioning policy for handling categorized traffic at the local processing gateway. In many cases, in oil and gas pipeline systems, it is desirable to avoid unnecessary polling of the sensors and minimized network usage. Therefore it is desirable to enable to the system to determine policies for transmitting data such as a scheduled transmission versus an aggressive polling request based on the urgency of information, or aggregating information based on delay tolerance, to best utilize network resources.

Resulting requirements:

10. The local pipeline gateway needs to be capable to buffer incoming requests from the pipeline sensor for transporting data to the backend server and support forwarding them at a later time - which could potentially be a very long time in the order of hours, days or even more - depending on cellular network availability, cellular network utilization policies, device constraints
11. The local pipeline gateway needs to be capable to accept parameters with incoming requests from the pipeline sensor which define a delay tolerance for initiating the delivery of the sensor measurements or parameters for categorizing sensor measurements into different levels of priority/QoS.
12. The local pipeline gateway needs to be cable of receiving policies which express cellular network utilization constraints and which shall govern the decision making in the gateway when initiating connectivity over cellular networks.
13. The local pipeline gateway needs to be capable to trigger connections to the cellular network in line with the parameters given by the request to transport data and in line with configured policies regarding utilization of the cellular network.
14. The local pipeline gateway shall have the ability to categorize the data based on the abnormality/urgency or delay tolerance of the data.
15. The local pipeline gateway can be provisioned with policies to handle categorized traffic.

Rationale

The use case also describes a flow in which the backend server could initiate an action on the local pipeline gateway. The action could include a request for a measurement, or a firmware upgrade push to the gateway, or a change in the policies associated with data transportation. In particular, the ability to provide remote firmware upgrades or remote provisioning of policies is particularly desirable for these pipeline gateways at remote locations.

Resulting requirements:

16. The M2M system shall support transport of data from the backend server to the local pipeline gateway.

17. The M2M system shall support of triggering a cellular connection to the local pipeline gateway in case the gateway supports such functionality

6 Enterprise Use Cases

6.1 Smart Building

6.1.1 Description

Smart building is a M2M service that utilizes a collection of sensors, controllers, allerter, gateways deployed at the correct places in the building combined with applications and server resides on the Internet to enable the automatic management of the building with just limited human labour. Smart building system can greatly reduce the cost involved in managing the building like energy consumption, labour cost. With the smart building system, services like video monitor, light control, air-condition control and power supply can all be managed at the control centre. Some services can be triggered automatically to save the precious time in case of fire, intruder, gas leak etc.

6.1.2 Source

oneM2M-REQ-2013-0122R04 Use Case Smart Building

6.1.3 Actors

M2M Service Provider : A company that provides M2M service including entities like gateway, platform and enables the communication between them. The M2M Service Provider also exposes APIs for the development of all kinds of applications. The gateway provided by the Service Provider can be used to connect to different devices such as sensors, controllers.

Control Centre : The manage centre of the building, all data collected by the sensor is reported to the Control Centre and all commands are sent from the Control Centre. The Control Centre is in charge of the controlling of the equipment deployed around the building.

Smart Building Service Provider : A company that provides smart building services. A Smart Building Service Provider is a professional in the area. It is in charge of install the device all around the building, set up the Control Centre and provide the application that is used to manage the Control Centre and necessary training to workers in the Control Centre on how to manage the system. The Smart Building Service Provider has a business contract with the M2M Service Provider in utilizing the communication, gateway, M2M platform and APIs provided by the M2M Service Provider.

61.4 Pre-conditions

The Smart Building Service Provider establishes a business relationship with the M2M Service Provider in using the gateway, M2M platform and APIs.

The Smart Building Service Provider installs all the sensors, controllers, allerter in and around the building and sets up the Control Centre in the building with the application to run the system.

The Control Centre belongs to an estate management company and takes charge of several buildings all over the city. The building in the use case is one of them.

6.1.5 Triggers

None

6.1.6 Normal Flow

The light control of the building

The Control Centre needs to control the light in the building by different areas and different floors. The Control Centre also needs to switch on and off all the light in the building. For the management of the lights, the Smart Building Service Provider deployed one gateway in each floor to get connection with the lights in the same floor. Each floor of the building has at least 100 lights and the building has 50 floors above the ground and 5 floors under the ground and each light can be switched separately. The lights in every floor is connected with the gateway using local WIFI network, the gateway is connected with the M2M platform using paid 3GPP network, the Control Centre is connect with the M2M platform using fixed network. A patrolling worker with a mobile device can access to the gateway's local network to switch the lights. The illustration can be seen in figure 6.1.9-1 .

In order to switch the light from the whole floor, instead of sending request from the Control Centre 100 times, the Control Centre creates a group on the gateway of each floor to include all the light on that floor. As a result, the Control Centre could switch the light of a whole floor just by sending one request to the group created on the gateway, the gateway fans out the request to each light to switch them off.

In order to switch the light of the building, instead of sending request from the Control Centre 5500 times, the Control Centre could create a group on the M2M platform to include all the groups created on each gateway on each floor. In this way, the Control Centre simply send one request to the group on the M2M platform, the group fans out the request to the group on every gateway, the group on the gateway fans out the request to each lights to switch it.

The maintenance of the member of the group is the duty of a worker with a mobile device. Whenever a new light is installed, the worker adds the light to the group of the corresponding floor. Whenever a broken light is removed, the worker with the mobile device first searches the light from the group and removes the light from the group.

The Control Centre creates the group in the purpose of controlling the lights, so the group is configured to accept lights only in case the group may cause unexpected result on other devices introduced to the group by mistake. For example, if the type of the group is configured as “light”, then “wash machine” cannot be a member of the group. Because the commands to wash machine is much more complicated. If a wash machine is added to the group of lights by mistake, it may cause unexpected behavior to the wash machine.

The add and remove of the members of the group of each floor is not necessary to be known to the Control Centre, but the Control Centre do know how to switch off the lights from the whole floor. In this way the Control Centre is exempt from the trivial task of maintaining each single light. However in the meantime, the administrator of the Control Centre can always make a list of all the lights and view their status from the Control Centre by retrieving from the group.

Intruder

With the deployment of smart building system, the number of patrollers is greatly reduced. For the security reason, a number of motion detector and cameras are installed all over the building.

The motion detector and the cameras are configured to work together. During the period when certain floor of the building is in safe mode, whenever the motion detector detects a moving object, the camera captures a picture of the moving object immediately. The picture is sent to the Control Centre for the inspector to verify if it is an intruder or an automated image recognition system. As a result of fast reaction, the motion detector must trigger the photo shot as soon as possible.

If the inspector sitting in the Control Centre finds that the object captured in the photo is a dog or a cat, he could just ignore the picture. If the figure caught in the picture is a stranger with some professional tools to break into a room. The inspector could send out a security team as soon as possible to the location based on the location reported from the motion detector.

Fire alarm

In case of an emergency, the residents of the building need to be evacuated immediately. All the devices related to a fire alarm need to be triggered almost at the same time. Whenever the fire sensor detects a fire in the building, a chain group of devices associated with the fire detection shall be turned on simultaneously such as the siren, the evacuation guide light, start the water pouring system, stop the elevator, cut off the electricity at certain areas, send message to the hospital, call the fireman, in a way not interrupting each other. Due to the possible latency and unavailability on the network to the Control Centre, the trigger of the devices on one floor is configured in the gateway.

If only one fire sensor in one room of the building detects a fire with a range less than one square meter, siren and water pouring system in the room would be switched on to alarm the resident to put out the fire. If lots of fire sensors all detect fire together with smoke sensors, temperature sensors reporting unusual situations, the whole fire alarm system will be triggered and all the residents in the building will be evacuated. If in the meantime of a fire alarm, the sensors detect that the temperature is below the threshold which means the fire is under control, the alarm can be cancelled automatically to all sirens and actuators to avoid the panic.

With the configuration on the gateway, the trigger of the devices can be very fast so that the damage caused by the fire can be limited to its minimum

6.1.7 Alternative Flow

None

6.1.8 Post-conditions

None

6.1.9 High Level Illustration

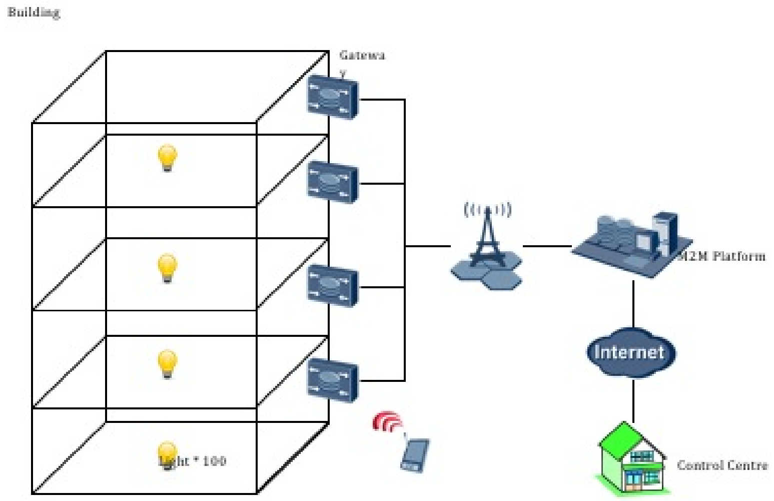


Figure 14: Figure 6.1.9-1 Smart Building Scenario

6.1.10 Potential Requirements

1. The M2M system shall support the action chain harmonize a series of actions among a group of between devices, in a way not interrupting each other.
2. The M2M system shall harmonize a series of actions based on certain conditions that support the action chain between devices shall subject to certain conditions.
3. The M2M system shall support the devices to report their locations.
4. The M2M system shall support a mechanism to group a collection of devices together.
5. The M2M system shall support that same operations can be dispatched to each device via group.
6. The M2M system shall support the members' management in a group i.e. add, remove, retrieve and update.
7. The M2M system shall support that the group can check if its member devices are of one type.
8. The M2M system shall support the group to include another group as a member.

6.2 Machine socialization

6.2.1 Description

A robot is designed to clean rooms in hotel. The task of the robot is to keep all rooms clean. If the hotel has only one robot, it has to clean rooms one by one. If the hotel has two robots, they will complete the task more efficiently if they cooperate with each other. If robot A has cleaned a room, it may inform the other robot that this room has been cleaned, so robot B can move to another room for clean job. This implies that if multiple robots share a same task, cooperation will improve the efficiency. As in the hotel scenario, the robots owner may not tell the robots explicitly that there exists another robot with the same task. So, firstly, the robot must have the capability to discover other robots and find out if they share the same task as itself. Secondly, a robot must realize what kind information will affect other robots behaviour, and it must transmit messages in order to share these information to other co-operators. For example, after a machine scan a room, it will find out the clean status of that room (clean or dirty), when a robot is cleaning a room or after it is cleaned, it will change the status of that room, the information will affect other robots' behaviour, because for any other robots it is unnecessary to go to a room that is being cleaned or has been cleaned by another robot. Thirdly, a robot must have the knowledge about the message interface of other robots. Only with this knowledge, it can send inform or command to another robots.

A cloud robot service platform may play an important role in this hotel scenario. Because the platform may help robots to discover each other, and the platform may initialize a powerful commander to optimize the job with multiple robots.

6.2.2 Source

REQ-2015-0658R01

6.2.3 Actors

- The clean robot is designed to keep all rooms clean. They may cooperate with each other directly or with the help of cloud robot service platform.
- Cloud robot service platform can discover the underline cooperation between machines.

6.2.4 Pre-conditions

- Multi-robots share the same tasks or correlated tasks.

6.2.5 Triggers

1. A robot discover another robot with the same or correlated tasks.

6.2.6 Normal Flow

- A robot A is deployed in a hotel.
- Another robot B is deployed in a hotel.
- Robot A&B discover each other (the discovery is performed by themselves or aided by the cloud robot service platform)
- Robot A share information to robot B and Robot B share information to Robot A.
- The cloud robot service platform help to optimize the task process and help the robots to cooperate with each other.

6.2.7 Alternative Flow

None

6.2.8 Post-conditions

Mone

6.2.9 High Level Illustration

6.2.10 Potential Requirements

1. A M2M infrastructure shall be able to support the machine socialization functionalities, such as existence discovery, correlated task discovery, message interface discovery and process optimization for multiple machines with same tasks.

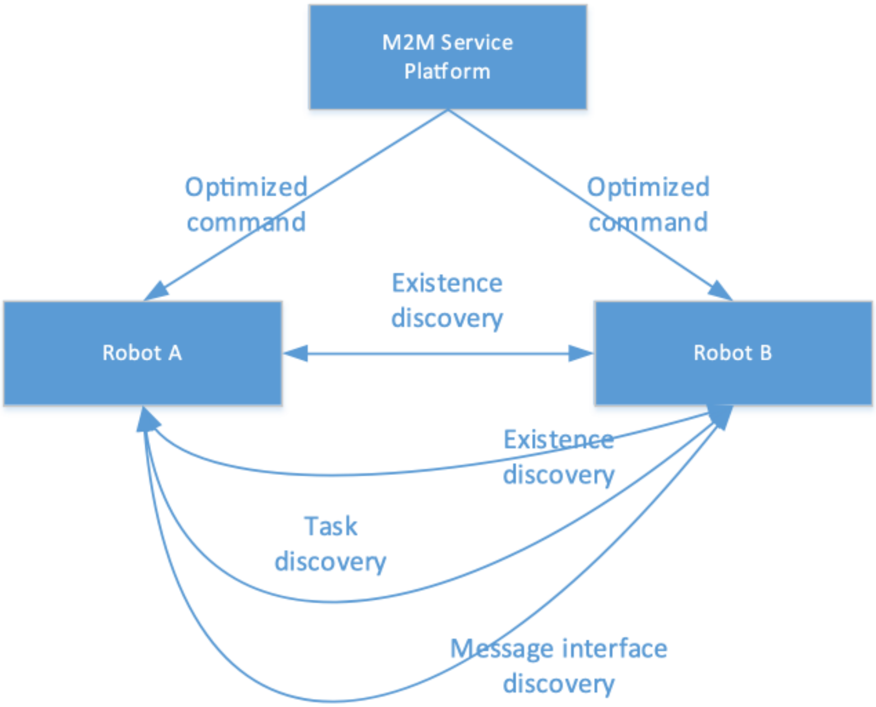


Figure 15: Figure 6.2.9-1 Machine Socialization

6.3 IoT device replacement

6.3.1 Description

In the IoT world, there is a particular IoT device that is composed of various parts. Also, many IoT devices have a life cycle such as start, operate, break, fix, re-operate, replace and terminate. Once such components or devices reach their limit, they need to be removed or replaced.

For example, a vehicle contains a large number of components as follows:

- Battery, 6 - 7 years
- Wiper blade, 1 year
- Oxygen sensor, every 80,000 km
- Tyre position, 5 years
- Timing belt, 80,000 km
- Brake pad, 40,000 km
- Various fuse, whenever there is a failure.

In the case of an electric car, batteries typically have an automotive life of 7-10 years. At the end of that time, their capacity is degraded to 70-80% of their original capacity, and they are less fit for mobility applications. Then such batteris should be replaced with a new battery.

It is very important to know how many replacements happens to such components and devices. Also, when a replacement occurs, the exact time is needed to be recorded. So that the owner of an IoT device or service provider use such information for business purposes.

For example, if many fuse parts have been intensively replaced over a certain period of time, it is suspected that the car is flooded. Also, the car owner can be informed by an IoT service provider about a time to replace a particular component.

There is also a case that the serial number of a device is used as a security key for authentication. In this case, when a device is replaced, new registration or an update of the registration key has to be triggered.

This use case introduces new set of information for the IoT service platform to manage a case where a device is replaced as follows:

- Number of replacements. This information shows how many replacements happens.

- Limited number of replacements. This information shows the maximum amount of replacements that a device can have.
- Replaced time. This information shows when a replacement happened.
- List of IoT applications interested in device replacement. This information contains a list of IoT applications that want to receive a notification about device replacement.

- Conditions for replacement. This information describes where and when a device replacement happens. Various information can be used to describe conditions such as location, time, distance, etc.

6.3.2 Source

RDM-2020-0100R01-Use_case_on_device_replacement

6.3.3 Actors

M2M Service Platform (MSP): A company that provides M2M service including entities like gateway, platform and enables the communication between them. The M2M Service Provider also manages information about device replacement. These information can be exposed to IoT applications.

Car Center: The center for selling and managing vehicles. The center provides advanced services to its premium customers. For example, the center informs their premium customer when to replace a particular component of their customers' car to have a safe driving.

Vehicle: M2M/IoT enabled Smart Vehicle that can send various measured data to MSP and inform the owner of the vehicle about diagnostic information.

6.3.4 Pre-conditions

The Car Center establishes a business relationship with M2M Service Provider in using the gateway, M2M platform and APIs.

The Car Center deploys M2M/IoT sensors and actuators to their vehicles and registers them to M2M Service Provider.

The Car Center runs premium vehicle management service that inform their premium users about various diagnostic information of their car, for example, the lifecycle of each component, when to replace a particular component, how long each component can be used.

6.3.5 Triggers

None

6.3.6 Normal Flow

1. A Car Center sells a smart vehicle to User A.
2. The vehicle is registered to the IoT platform with various components and information.

3. The Car Center uses a premium service managing diagnostic information from the IoT service provider.
4. User A subscribes a replacement service provided by the Car Center.

5. As time passes, a battery of the vehicle reaches its max lifetime, and the capacity is downgraded to 50% of its original capacity.

6. The IoT platform detects this situation using stored replacement related information such as its max lifetime and a condition for the replacement (i.e., battery capacity is lower than 50%).
7. The IoT platform informs a warning to the car centre that indicates a replacement is needed.
8. The Car IoT application indicates and initiates the replacement procedure with the IoT platform. This request includes which component is needed to be replaced.

9. The IoT platform allows the Car application to replace the given component.
10. The Car IoT application sends information to replace the target component.
11. The IoT platform replace the target component with the new information from the Car IoT application.
12. The IoT platform informs the successful operation of the requested replacement.

6.3.7 Alternative Flow

None

6.3.8 Post-conditions

None

6.3.9 High Level Illustration

6.3.10 Potential Requirements

Note: This use case scenario can be partially fulfilled by the existing requirement as below.

Table 2: Table 6.3.10-1 Related exiting requirements

Requirement ID	Description	Release
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

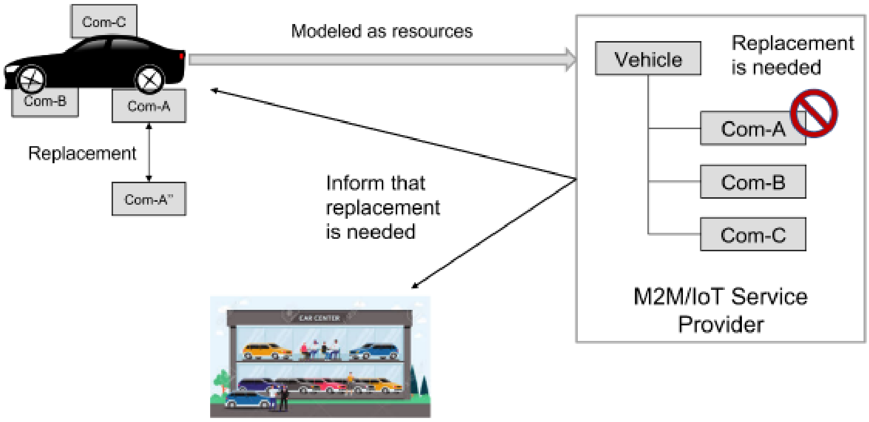


Figure 16: Figure 6.3.9-1 High level illustration of device replacement scenario

Additionally a new requirement is needed.

Table 3: Table 6.3.10-2 New potential requirement

Requirement ID	Description	Release
OSR-xxx	The oneM2M System shall support mechanisms to enable M2M device replacement procedures (e.g., triggering by events, meta data updating)	Not implemented

6.4 Use case for IoT device calibration

6.4.1 Description

IoT sensors measure physical value and convert the measurement to a digital value. For example, a temperature sensor measures the temperature of a place where it locates. Ideally, the same type of sensors manufactured by the same manufacturer should measure the same value if deployed at the same place. However, depending on the characteristics of the sensor device, the measured value may be different. Also, there is a case that a sensor does not have a proper zero reference value, which generates a wrong measurement value.

The sensor's range may shift due to the same conditions just noted, or perhaps the operating range of the process has changed. For example, a process may currently operate in the range of 0 to 200 Celsus, but changes in operation will require it to run in the range of 0 to 500 Celsus.

In the case of CO2 sensors, it is essential to know in which domain the sensors measure the percentage of carbon dioxide. Based on such information, the range, accuracy, or precision can be decided to recommend the proper carbon dioxide. For example, indoor and outdoor air has between 400ppm and 2,000ppm CO2 by volume. This means that for measuring a smart home's indoor air quality, a CO2 sensor requires different calibration equations to apply.

Therefore, each sensor needs to be calibrated before deployment or adjustments for the measured value should be applied.

In order to support calibration, the sensors typically have a separate circuit and memory space internally. For example, the sensors should support a logic to perform calibration and space to store equations for calibration. These resources increase the price of sensors and make it challenging to build a small and cheap sensor.

The basic concept of this use case is to allow IoT platforms to support the calibration of their managing sensors. Typically, when a sensor is deployed for the first time, it needs calibration with a local test machine, and the machine generates results for calibration. The generated calibration value is stored in the cloud IoT platform, where the sensor will be registered and managed. In this case, the sensor does not need to provide any computing power or memory for calibration. When a sensor registers to the IoT platform, the platform checks a corresponding calibration value for the sensor and store such value as an additional parameter to the resource for the sensor. When the sensor generates a measurement, the platform checks the calibration value, and if there exist, the measurement will be adjusted based on the calibration value.

6.4.2 Source

RDM-2022-0005-Use_case_on_IoT_device_calibration

6.4.3 Actors

- Calibration application: a testing device to calibrate IoT devices.
- IoT platform: An IoT platform stores data for device calibration and performs calibration when there is a new measurement.

6.4.4 Pre-conditions

- The sensor device does not have enough computing power and memory to store and perform calibration.

- The IoT platform holds a set of information to support device calibration.

6.4.5 Triggers

- If the IoT platform is configured to support IoT device calibration, a new measurement from an IoT sensor that needs calibration triggers the process for IoT device calibration.

6.4.6 Normal Flow

Figure 6.4.6-1 illustrates the high-level flows of the IoT sensor calibration use case, which consists of the following steps:

- Step 1: The calibration application retrieve calibration parameters for the type of Sensor-1 from the IoT platform.
- Step 2: The calibration application calibrates Sensor-1 using the retrieved parameters and generates calibration results.
- Step 3: The calibration application stores the generated calibration results for Sensor-1.
- Step 4: Sensor-1 registers itself to the IoT platform.
- Step 5: The IoT platform checks the calibration data for Sensor-1 and stores it as parts of associated parameters.
- Step 6: Sensor-1 sends a request to store its new measurement to the IoT platform.
- Step 7: The IoT platform adjusts the measurement based on the calibration results and stores adjusted value.

6.4.7 Alternative Flow

None

6.4.8 Post-conditions

The IoT platform stores the correct measurement after adjusting calibration value.

6.4.9 High Level Illustration

6.4.10 Potential Requirements

1. The oneM2M System shall be able to store calibration parameters for an IoT device and calibrates new measurement.

6.5 Use case for Vanishing IoT Devices

6.5.1 Description

There are sensors that do their job and disappear, similar to a disposable sensor. Such a sensor can be called a “Vanishing sensor”. For example, suppose a system measures the temperature of a jet engine’s exhaust gas to determine the engine’s efficiency. In this case, a vanishing sensor can be installed in the exhaust path

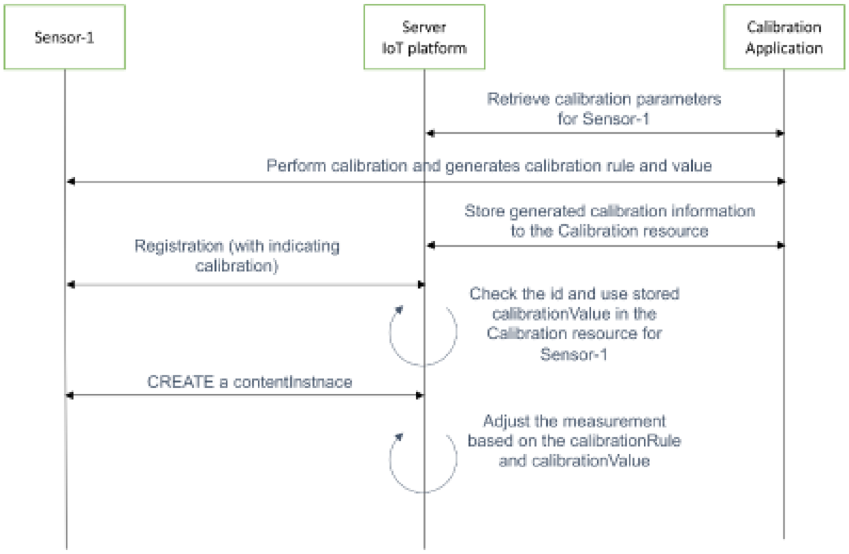

Sensor-1
Server
IoT platform
Calibration
Application
Retrieve calibration parameters
for Sensor-1
Perform calibration and generates calibration rule and value
Store generated calibration information
to the Calibration resource
Registration (with indicating
calibration)
Check the id and use stored
calibrationValue in the
Calibration resource for
Sensor-1
CREATE a contentInstnace
Adjust the measurement
based on the calibrationRule
and calibrationValue

Figure 17: Figure 6.4.6-1 A flow for calibrating IoT devices in the server IoT platform

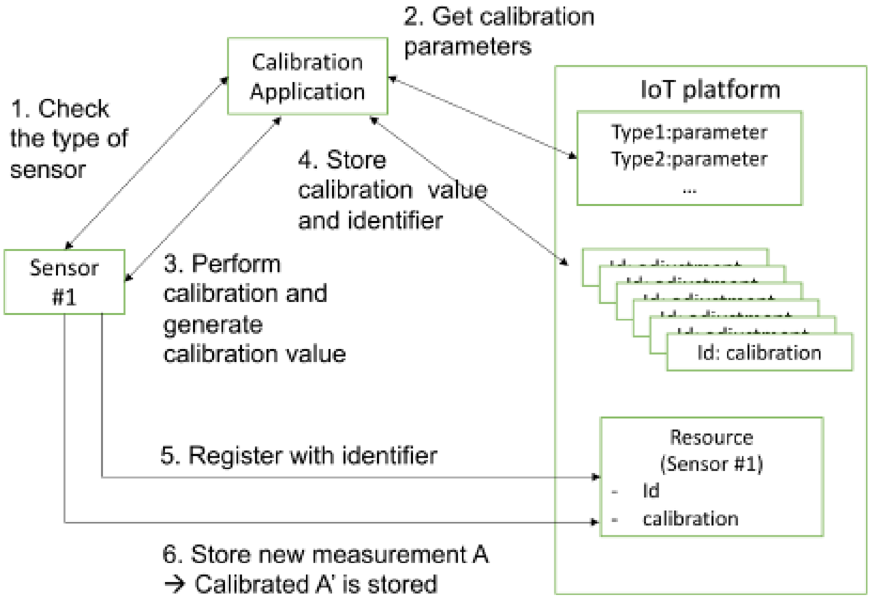


Figure 18: Figure 6.4.9-1 Conceptual diagram of IoT device calibration

where the highest heat of the jet engine is discharged. When the jet engine turns on, the vanishing sensor measures temperature as long as possible before it burns out after a few minutes. However, the temperature in the exhaust path of the jet engine is still essential for the safe operation of the machine.

In order to keep measuring the temperature in the exhaust path, typically, other temperature sensors in a safe location around the engine are used. The last measurement recorded just before the vanishing sensor burned out due to high heat can be used as a reference value for the adjacent sensors measuring in a safe location. The high heat inside the engine can be measured by using the mathematical correlation between the last measured value of the vanishing sensor and the values measured at a safe location. This can virtually recreate the sensor in the exhaust path.

Vanishing sensor has the following three different statuses:

- measuring its value (physically located in a place)
- measuring its value using reference sensors (physically vanished but still working)
- vanishing permanently

In order to manage vanishing sensors throughout their lifecycle, the IoT platform behaves differently. For example, When a sensor physically exists, all the measurements from the sensor are appropriately stored based on the actual measurement value. When the sensor vanishes, the value from adjacent sensors can be used to derive the actual value at the place where the sensor was installed. IoT platform uses a pre-defined mathematical equation to derive such value.

6.5.2 Source

RDM-2022-0009_Use_case_on_vanishing_IoT_sensor

6.5.3 Actors

- Vanishing temperature sensor: Sensors deployed in a place where extreme environment, e.g., high temperature or pressure, so disappears after operating for a certain amount of time.
- Normal sensor referencing a vanishing sensor: Sensors deployed adjacent to a vanishing sensor provide reference measurement.

- IoT platform: An IoT platform that manages data from vanishing and adjacent referencing sensors.

6.5.4 Pre-conditions

- The cloud IoT platform is aware of the relationship between vanishing sensors and their adjacent referencing sensors.
- The cloud IoT platform can generate measurement value from a vanishing sensor even it vanishes through a pre-defined mathematical equation.

6.5.5 Triggers

- Some sensors do their measurement and disappear because of the extreme operating environment, e.g., high temperature and pressure. However, the measurement of where such sensors were deployed may be essential. In this case, the IoT platform generates a measurement of such a place even after these sensors disappear through adjacent sensors that provide reference values.

6.5.6 Normal Flow

Figure 6.5.6-1 illustrates the high-level flows of the managing sensors vanishing after operating for a certain amount of time but still need to generate its measurement.

0. Step 001: IoT sensors (i.e., Sensor-A for vanishing type and Sensor-B for normal type) in a jet engine are installed and measuring temperatures. IoT sensors send measured values to the IoT platform.
1. Step 002: Sensor-A vanishes because of the jet engine's extremely high temperature.
2. Step 003: When Sensor-B generates a new measurement, the IoT Platform stores the new measurement from the reference sensor. Then IoT platform checks the status of the vanishing sensor.
    - If the sensor does not vanish and has generated its new measurement, the IoT platform does nothing.
    - If the sensor vanishes, then the IoT platform applies a pre-defined equation to the measurement of the reference sensor (i.e., Sensor-B). For example, if the measurement of Sensor-B is "100" and the pre-defined equation is "multiply 2", then the generated value for Sensor-A becomes 200.

   Finally, the IoT platform generates a temperature value for Sensor-A and stores the value to the corresponding resource for Sensor-A.

6.5.7 Alternative Flow

None

6.5.8 Post-conditions

None

6.5.9 High Level Illustration

6.5.10 Potential Requirements

The oneM2M System shall be able to generate measured data from sensors that vanish after operating for a certain period because of the extreme environment (e.g., high temperature or pressure) using measurements from adjacent sensors.

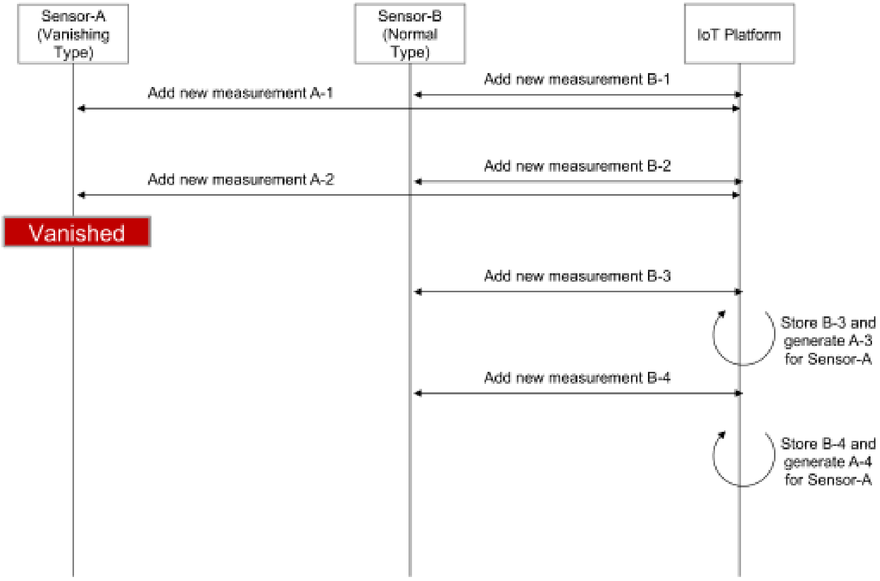


Figure 19: Figure 6.5.6-1 A normal flow for managing sennsors vanishing in extreme environment

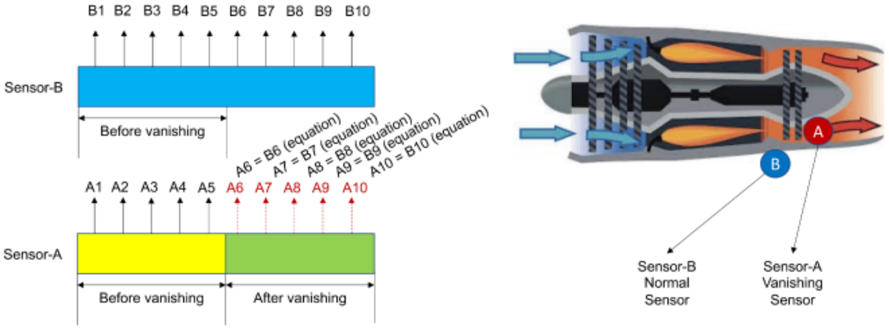


Figure 20: Figure 6.5.9-1 The relationship between values from a normal sensor and vanishing sensor

7 Healthcare Use Cases

7.1 M2M Healthcare Gateway

7.1.1 Description

This use case addresses a healthcare gateway to transport healthcare sensor data from a patient to a backend server and to also support bidirectional communications between a backend server via a gateway. The use case results in a set of potential requirements out of which some are specific to the fact that cellular connectivity is assumed between gateway and backend. Other than that, this use case is not restricted to cellular connectivity.

This use case also addresses the situations where some of M2M System components are not available due to, for example, disaster

7.1.2 Source

oneM2M-REQ-2012-0057R02 Use Case M2M Cellular Healthcare Gateway
oneM2M-REQ-2012-0208R01 Correction to M2M Healthcare Gateway Use Case
oneM2M-REQ-2013-0283R01 Addendum to M2M Healthcare Gateway Use Case
oneM2M-REQ-2013-0185R03 Use case of peer communication
oneM2M-REQ-2013-0356R01 Correction to M2M Healthcare Gateway Use Case,

> Note: Several scenarios also supported by guidelines [i.14]defined in Continua Health Alliance should be covered by this use case.

7.1.3 Actors

- Patients using healthcare sensors
- Health-care gateways (also known as AHDs (Application Hosting Devices) in Continua Health Alliance terminology). Examples of healthcare gateways can include wall plugged devices with wired or wireless connectivity, or mobile devices such as smartphones.
- Operating healthcare service enterprise backend servers (equivalent to a WAN Device (Wide Area Network Device) in Continua Health Alliance terminology)
- Health care providers, operating healthcare enterprise backend servers
- Care givers and authorized users that could eventually access health sensor data
- Wide Area Network operator

7.1.4 Pre-conditions

- Operational healthcare sensor(s) that requires occasionally or periodically transport of sensor data to a backend server.
- A local healthcare gateway is available that can be used to transport data from the healthcare sensor to a backend server. It is open as regards

who owns and/or operates this local gateway. Different scenarios shall be possible supported (patient, healthcare provider, care-giver, M2M service provider, wide area network operator).
- Network connectivity is available for transporting healthcare sensor data from the local gateway to the backend server.
- A backend server that is hosting applications to collect measurement data and makes it available to care-givers, healthcare-providers or the patient.

7.1.5 Triggers

The following triggers could initiate exchange of information according to the flows described further-below:

- Patient-initiated measurement request (Trigger A). In this case, the patient decides to take a measurement and triggers the processing in the system.
- Static configured policy at a healthcare gateway that requests patient to initiate measurement (Trigger B). This can be an explicit message from the gateway device to a patient device, or it could just an indicator on the gateway itself such as a pop-up message or an indicator light requesting measurement.
- Static configured policy at a healthcare gateway that directly requests sensor data without patient intervention (Trigger C). This can be used in conjunction or in lieu of Triggers A or B. Some sensor data may be measurable or accessible without patient intervention so that the gateway merely needs to communicate with one or more sensors to obtain the data.
- Patient monitoring app on healthcare service backend server that triggers generation of sensor data (Trigger D).
- Dynamic patient monitoring request from the healthcare service provider (Trigger E).
- Availability of new patient healthcare data at a healthcare gateway that requires transport to a backend server.
- Availability of new patient healthcare data at a backend server that requires sharing with authenticated users such as a nurse/doctor (healthcare provider) and a patient's relative (such as a child care-giver).
- Health care service provider needing to contact patient to take measurements.
- Analysis of healthcare patient sensor info or trends that triggers the need to take action on behalf of patient (for example determination of a deteriorating health condition).
- QoS-aware data buffering policy on the healthcare gateway.
- Network-aware and/or device-aware delay-tolerant data management policy on the healthcare gateway. Network dynamic access constraints or network utilization constraints or prior network access policy constraints or device energy minimization considerations can cause delay tolerant sensor data to be buffered (and aggregated if needed) at the gateway and transmitted at a later time.

- Failure in the components of the M2M System for the healthcare service. (e.g. functional failure in Wide Area Network, functional failure in Healthcare Service Backend Server).

The following clauses describe different flows that are possible in the m2m healthcare gateway system. For each flow, the events corresponding to the flow are high-lighted in the corresponding figure. Other events may be shown in a figure that are preserved to reflect the different types of processing that can occur in the system, with new events added in each subsequent figure to increase the complexity of the system. The high-level illustration provides a comprehensive summary description of the overall system.

7.1.6 Normal Flow

A measurement of the healthcare sensor is initiated as shown in 7-1. Patient can initiate the generation of sensor data such as taking a glucose meter measurement (Trigger A). The measurement may also be initiated based on some pre-defined schedule.

1. At the healthcare gateway (Trigger B or C).
2. The healthcare sensor data is forwarded to a backend server by a healthcare-gateway. If the data has a QoS indicator such as dynamic latency/bandwidth and/or delay tolerance, the gateway can determine whether to send the data immediately, or whether to buffer and send the data at a later time. Buffered data can be aggregated with past data or future data for a future aggregated transmission over the network. In wireless/cellular networks, aggregated transmissions can reduce the utilization of the network by requesting access to the network less frequently.
3. Measured data (or processed/interpreted versions of the data) that arrives at the healthcare service enterprise backend server may need to be forwarded to authorized subscribers - such as family care-giver or a nurse/doctor - via notifications. Subscriptions can be set up in advance, and configured at the backend server, so that when the data arrives, the subscribers can be notified. Filters can be associated with the subscriptions, so that only selective data or alert information can be sent to subscribers.

7.1.7 Alternative Flow

Alternative Flow 1 - Network/Device-aware transmissions

The flow in figure 7.1.7-1 depicts network/device-aware constraint processing in the system. This flow is the same as the regular flow with the following exceptions: The healthcare sensor data may need be stored on the gateway and forwarded at a future time based on one or more of the following factors:

- delay tolerances associated with the data.

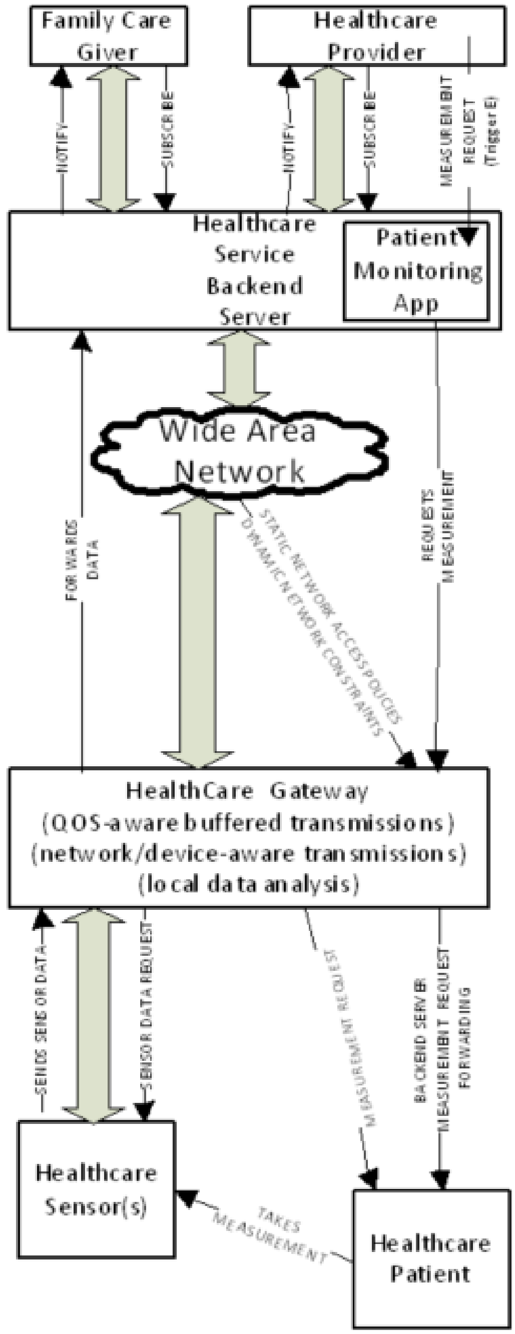


Figure 21: Figure 7.1.6-1 Healthcare Measurement Data Processing Flow

- network policy constraints (efficiency, avoidance of peak loads, protection of spectrum).
- device constraints (energy consumption, data tariff).
- temporary lack of coverage of network connectivity.

Multiple measurements can be aggregated and transmitted together at a future time.

Measurements can be taken with or without patient intervention and sent to the healthcare gateway. As measured data arrives at the healthcare gateway, its QoS indicators such as dynamic latency/bandwidth and delay tolerance can be processed. Delay tolerant data can be buffered and aggregated with past and future delay-tolerant data, with network/device-aware constraints can applied to determine an appropriate time to transmit the data.

Alternative Flow 2 Remote Monitoring

Figure 7.1.7-2 depicts the event flow for remote monitoring from the healthcare service enterprise backend server. The backend server may expect the patient to submit sensor data periodically or with a pre-defined schedule. In the absence of a typically expected sensor data event, the backend server can trigger an event to request the patient to take a measurement.

In this case, the trigger (Trigger D) arrives over a wide-area-network from the patient monitoring app on the healthcare service backend server delivered to the healthcare gateway. The patient monitoring app could generate this request based on a statically configured policy to request measurements or due to some dynamic needs based on processing of previous patient data.

Optionally, the healthcare service provider may generate a measurement request (Trigger E) that can be received by the patient monitoring app on the backend server, which can subsequently submit a request over the wide area network for the patient monitoring request to the healthcare gateway.

The healthcare gateway forwards the received request to the patient. In many cases, it is possible that a device associated with the patient, such as the healthcare cellular gateway, or a smartphone connected to the gateway, does not always have an active network connection, and that such a device may be asleep. In such a case, the measurement request can arrive with a wakeup trigger (such as using an SMS) (also called “shoulder tap” in Continua Health Alliance terminology) to the healthcare gateway, which can then establish connectivity with the backend server to determine the purpose for the trigger, and then subsequently process the patient measurement request.

The patient subsequently takes the sensor measurement upon receiving the request. Alternatively, some sensor measurements could be taken without patient intervention. Measured sensor data is then received at the healthcare gateway, and subsequently transmitted based on processing the QoS/Network/Device-aware constraints for transmission.

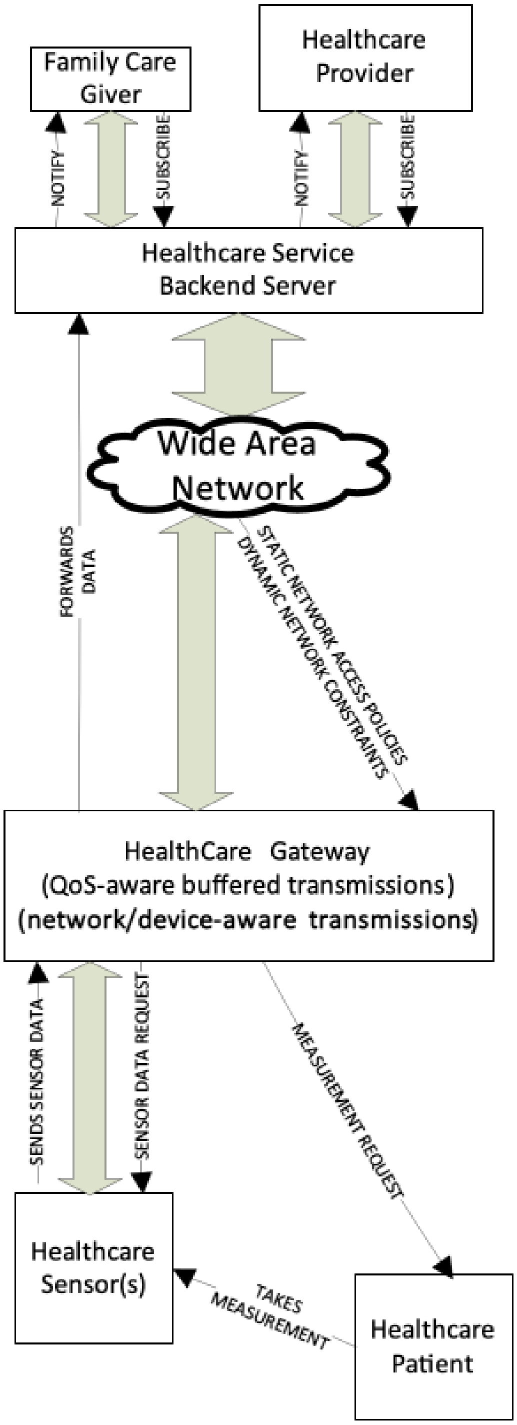


Figure 22: Figure 7.1.7-1 Network/Device-aware Flow

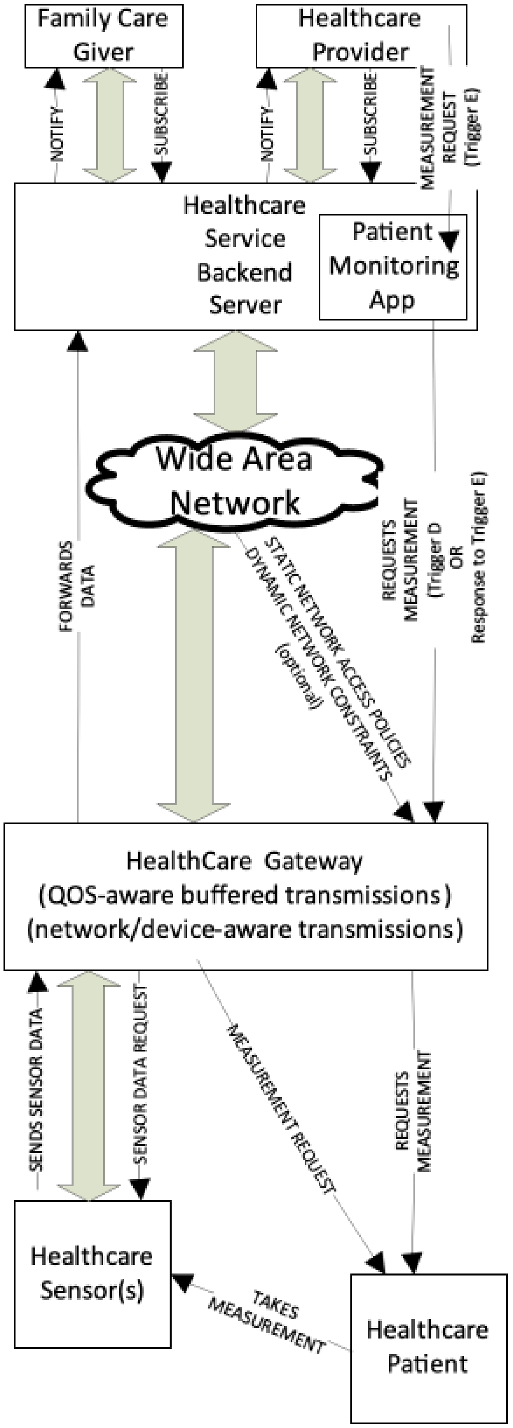


Figure 23: Figure 7.1.7-2 Remote Monitoring Flow

Alternative Flow 3 Local Gateway Data Analysis

Figure 7.1.7-3 illustrates a Local Gateway Data Analysis flow of events. The local gateway node can continuously process the data that it forwards. It can have smart algorithms to detect health anomalies associated with the patient. In case no anomalies are detected, the health sensor data may only be forwarded occasionally (see also alternative flow 1). In case an anomaly is detected, the local gateway needs to send an alert to the health care provider or the care-giver or to the patient if desired.

Alternative Flow 4 - Partial Failure Case

Figure 7.1.7-4 illustrates a partial system failure, i.e. the failure of Healthcare Service Backend Server and/or the failure of the connection between Healthcare Gateway and Wide Area Network. In this situation, nevertheless, components of the healthcare system that are not in failure should continue their normal operations. Examples of the 'normal operation' are as follows:

1. Reports from Healthcare sensor are received by and stored in Healthcare Gateway
2. Notification from Healthcare Gateway (e.g. Measurement triggers) is forwarded to Patient
3. If the messages transmitted between Healthcare Sensors and Healthcare Gateway were encrypted before the failure for the privacy of patients, that encryption should be maintained after the failure. (c.f. For maintaining the security mechanism in an isolated domain, a locally operable key management mechanism can be introduced.)

7.1.8 Post-conditions

1. **Normal flow**
   Sensor data is stored in a database associated with the backend server. Healthcare provider and care-giver observe data to ascertain status of patient's health.
2. **Alternative Flow 1**
   Data is buffered and transmitted when the network constraints or policy constraints or device energy minimization constraints allow the transmission of delay-tolerant data.
3. **Alternative Flow 2**
   Patient takes measurement and sends data to backend server.
4. **Alternative Flow 3**
   Local data analysis with indication of abnormal condition results in an alert message sent to the health care provider and optionally to the patient.
5. **Alternative Flow 4**
   Components of the healthcare system that are not in failure continue their normal operations.

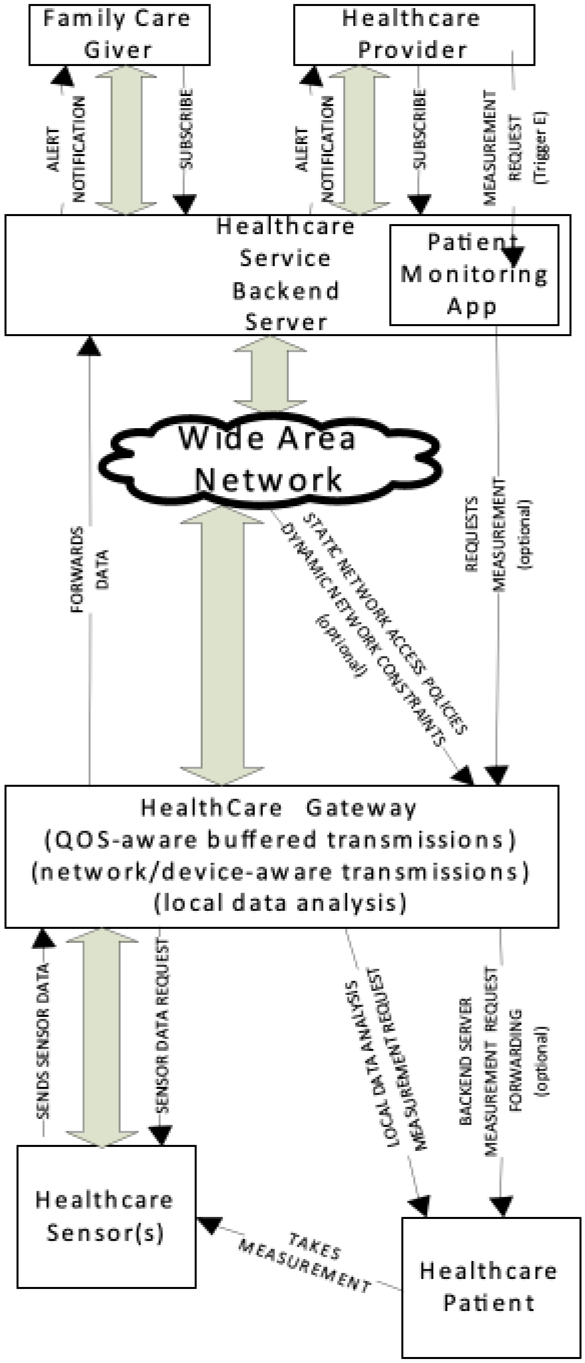

Family Care Giver
Healthcare Provider
ALERT NOTIFICATION
SUBSCRIBE
ALERT NOTIFICATION
SUBSCRIBE
MEASUREMENT REQUEST (Trigger E)
Healthcare Service Backend Server
Patient Monitoring App
Wide Area Network
FORWARDS DATA
STATIC NETWORK ACCESS POLICIES
DYNAMIC NETWORK CONSTRAINTS (optional)
REQUESTS MEASUREMENT (optional)
HealthCare Gateway
(QOS-aware buffered transmissions)
(network/device-aware transmissions)
(local data analysis)
SENDS SENSOR DATA
SENSOR DATA REQUEST
LOCAL DATA ANALYSIS MEASUREMENT REQUEST
BACKEND SERVER MEASUREMENT REQUEST FORWARDING (optional)
Healthcare Sensor(s)
TAKES MEASUREMENT
Healthcare Patient

Figure 24: Figure 7.1.7-3 Local Gateway Data Analysis Flow

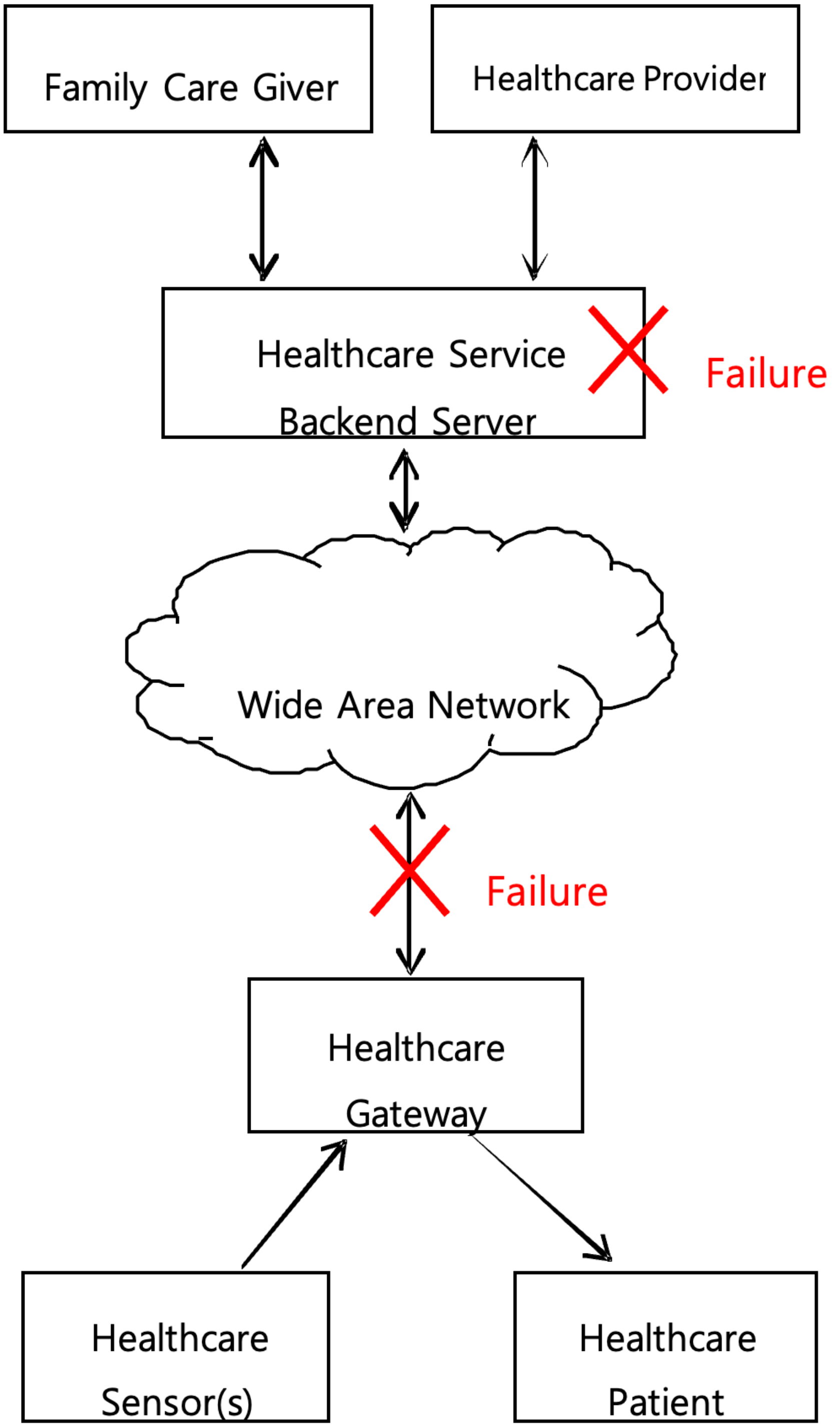


Figure 25: Figure 7.1.7-4 Example of failures in components of the M2M System for healthcare service

7.1.9 High Level Illustration

Figure 7.1.9-1 summarizes the overall description of this use-case. All the flows and connectivity should be self-explanatory based on the discussions in the previous clauses.

7.1.10 Potential Requirements

Rationale

This use case sets out from the presence of a gateway between one or more healthcare sensor(s) and a backend server. Even though the use case is assuming a cellular gateway, this restriction is not needed in general.

Resulting requirement:

1. The M2M system shall be capable of supporting gateway nodes that are capable of transporting sensor measurements to back end servers.

Rationale

Sensors can measure patient data with or without patient initiation. Therefore, new measurement data may become available at any time.

Resulting requirement:

2. Whenever a healthcare sensor has measurement data available, it shall be possible for the sensor to send a request to the local healthcare gateway to transport new measurement data to the backend server.

Rationale

Incoming requests from the healthcare sensor to the healthcare gateway may not result in immediate forwarding of the data to the backend server if any of the following is applicable: Dynamically changing cellular network availability (coverage); cellular network utilization constraints (policies); device energy consumption or memory constraints or mobility, and data delay tolerance/QoS information. In some cases, the delay tolerance may be very low (implying requiring immediate transport) whereas in other cases, the delay tolerance can be significant. In some other variants where real-time delivery or near-real-time delivery is of interest, then real-time latency and bandwidth QoS requirements become significant. More than one healthcare sensor may provide data at the same time, so that the healthcare gateway will need to process one or more concurrent data streams. Event categories associated with the data to be transported (such as alert=high priority) can also be relevant for determining when the connection needs to be triggered.

Resulting requirements:

3. The local healthcare gateway needs to be capable to buffer incoming requests from the healthcare sensor for transporting data to the backend server and support forwarding them at a later time - which could potentially

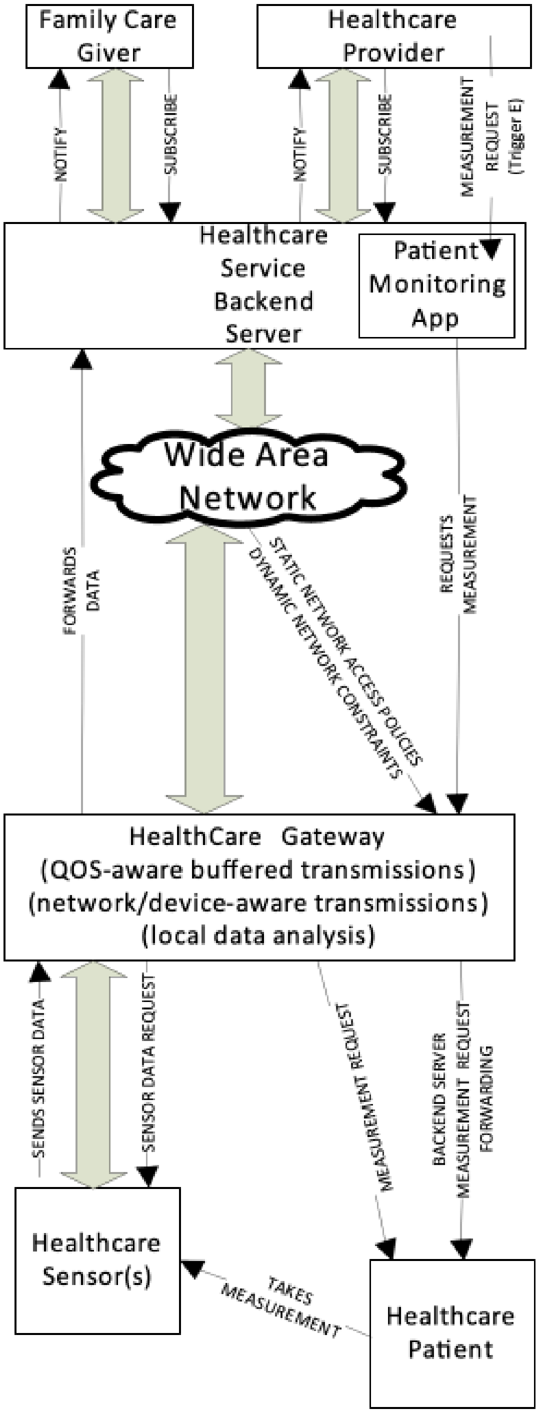


Figure 26: Figure 7.1.9-1 Healthcare Gateway High Level Illustration

be a very long time in the order of hours, days or even more - depending on cellular network availability, cellular network utilization policies, device constraints

4. The local healthcare gateway needs to be capable of accepting parameters with incoming requests from the healthcare sensor source which define a QoS policy for initiating the delivery of the sensor measurements or parameters for categorizing sensor measurements into different levels of priority/QoS.
5. The local healthcare gateway needs to be able to concurrently process multiple streams of data from different sources with awareness for the stream processing requirements for each of the streams. The local healthcare gateway needs to address the QoS policy of one or more concurrent streams while taking into account network constraints such as available link performance and network cost. The local healthcare gateway needs to adapt to dynamic variations in the available link performance or network communication cost or network availability to deliver one or more data streams concurrently
6. The local healthcare gateway needs to be capable of receiving policies which express cellular network utilization constraints and which shall govern the decision making in the gateway when initiating connectivity over cellular networks.
7. The local healthcare gateway needs to be capable to trigger connections to the cellular network in line with the parameters given by the request to transport data and in line with configured policies regarding utilization of the cellular network

Rationale

A subscription and notification mechanism was described in this use case. Only authenticated and authorized users (e.g. care-giver, relatives, and doctors) shall be able to subscribe to healthcare sensor measurement data and get notifications and access to the measured data. These authenticated and authorized stakeholders are typically using applications that use the M2M system to access the measured data.

Resulting requirement:

8. The M2M system shall be capable of supporting a mechanism to allow applications (residing on the local gateway, on the backend server or on the sensor itself) to subscribe to data of interest and get notifications on changes or availability of that data.
9. The M2M system needs to be able to allow access to data that is being transported or buffered only to authenticated and authorized applications

Rationale

The use case also describes a flow in which the backend server could initiate an action on the local healthcare gateway.

Resulting requirements:

10. The M2M system shall support transport of data from the backend server to the cellular healthcare gateway.
11. The M2M system shall support of triggering a cellular connection to the local healthcare gateway in case the gateway supports such functionality.

Rationale

Different subscribers may be interested in different information so that each subscriber may want to get notified only for events of interest to that subscriber:

Resulting requirements:

12. Subscriber-specific filters can be set up at the healthcare service enterprise backend server so that each subscriber can be notified only when information/events relevant to the subscriber are available/occur.

Rationale

The M2M healthcare gateway device can be without an active network connection because it is in a sleep mode of operation to save energy and/or because it is trying to save radio/network resources. A patient monitoring app may be desirous of communicating with the gateway device when the gateway device is in this sleep mode of operation.

Resulting requirements:

13. The M2M system shall be able to support a wakeup trigger (aka "shoulder-tap") mechanism (such as using SMS or alternate mechanisms) to wake up the gateway. The gateway can subsequently establish a network connection and query the enterprise backend server for additional information, and the enterprise backend server may then respond with adequate information to enable further processing of its request.
14. 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.
15. 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 confidentiality and the integrity of data between authorized components of the M2M System that are available.

7.2 Wellness Services

7.2.1 Description

This use case introduces several services based on wellness data collected by wellness sensor devices via mobile device such as smartphones and tablets which is regarded as M2M gateway.

Some wellness sensor devices are equipped with M2M area network module and measure individual wellness data. The mobile device connects to the wellness sensor devices by using the M2M area network technology, collecting and sending the wellness data to application server.

It is important to consider that mobile device as M2M gateway has mobility. For instance, there are possibilities for a mobile device to simultaneously connect to many wearable wellness sensor devices, and to connect newly to wellness sensor devices which have never connected previously at the location of outside.

This use case illustrates potential requirements from the use case of wellness services utilizing mobile device.

7.2.2 Source

oneM2M-REQ-2013-0167R03 Use Case on Wellness Services

7.2.3 Actors

- M2M Device: wellness sensor device is blood pressure sensor, heart rate sensor and weight scale, for example. It can measure wellness data of users, may be multi-vendor, and equipped with several kind of communication protocol.
- M2M Area Network: network which connects between M2M device and M2M gateway.
- M2M Gateway: mobile device (e.g. a smart phone) which can receive wellness data from wellness sensor devices and communicate with application servers.
- Mobile Network: network which has functions to communicate wellness data and control message between M2M gateway and M2M service platform.
- M2M Service Platform: platform where management server is located and which is used by the Application Server to communicate with the M2M Gateway.
- Management Server: server which manages the gateway such as mobile device, and controls its configuration such as installing/uninstalling applications.
- Application Server: server which serves the wellness services such as indicating the graph of wellness data trend.

  Note: Definition of some words is in discussion. Therefore, the description of these actors may change.

7.2.4 Pre-conditions

- Wellness sensor devices are able to establish a connection to the mobile device in order to send wellness data to M2M Service Platform or Application Server.

- It is first time to associate the mobile device with the wellness sensor devices.

7.2.5 Triggers

New wellness sensor devices such as weight scale are detected by mobile device. User tries to associate the detected devices. Examples are below:

- User buys several kind of wearable wellness sensor devices such as blood pressure sensor, heart rate sensor. In order to start monitoring vital data using these sensors, User tries setting of these devices simultaneously. Note that please refer to [i.4] ETSI TR 102 732 “Use cases of M2M applications for eHealth”. (Normal Flow)
- User buys wellness sensor devices such as weight scale, and newly deploys them at User’s house to check the wellness status daily. (Normal Flow)
- User goes to a fitness centre to do exercise and checks the effect by utilizing equipment which is owned by fitness centre and has never connected to User’s mobile device. (Alternative Flow 1)

7.2.6 Normal Flow

Usually wellness sensor devices are bought by Users. These devices are deployed in User’s house, or are worn with User.

- The mobile device detects new wellness sensor devices and tries to connect to it under User’s permission to connect (pairing between sensor device and mobile device).
- The mobile device has established a connection to the wellness sensor device, and then the mobile device receives additional information of the wellness sensor device (e.g. type of device, service certificates of the device, required application software . . .).
- The mobile device is provided with the appropriate application software from the Management Server and is appropriately configured by the Management Server.
- When the User measures the data by using wellness sensor device, the mobile device collects the data and sends it to the Application Server.

7.2.7 Alternative Flow

Alternative Flow 1

1. As indicated in the Normal Flow, usually the wellness service collects the data from wellness sensor devices which the User owns.
2. When the mobile device is brought outside, there is an opportunity to connect new wellness sensor devices (e.g. blood pressure which is set in fitness centre).
3. The mobile device detects new wellness sensor devices and tries to connect to them under User’s permission to connect.

4. The mobile device has established a connection to the wellness sensor device and then the mobile device receives additional information of the wellness sensor device (e.g. type of device, service certificates of the device, required application software . . .).
5. The mobile device is provided with the appropriate application software and is appropriately configured by the Management Server.
6. When the User measures the data by using wellness sensor device, the mobile device collects the data and sends it to the Application Server.

Alternative Flow 2

1. The wellness service may be an optional subscriber service to be charged. The User subscribes it and creates an account on the Application Server.
2. When the User utilizes the wellness service, at first the User needs to activate the service on the Application Server.
3. When the mobile device detects wellness sensor devices, it requests the Management Server to provide appropriate application software with configuration to the mobile device.
4. The Management Server checks with the Application Server if the User has subscribed to the service and activated it or not.
5. And then, if the User is not subscribed to the service or has not activated it, the Management Server does not provide any application software.

Alternative Flow 3

After the User has collected the data, the User is able to disconnect the mobile device from the wellness sensor device and to de-activate the service.

1. If the User brings the mobile device out of the range of M2M Area Network, the mobile device disconnects the wellness sensor device automatically.
2. The User is also able to disconnect these devices by operating settings of the mobile device or by waiting for a while until the wellness sensor device disconnect by itself.
3. The User is also able to cancel the optional service. The User applies the cancellation to the Application Server. After the Application Server accepts the cancellation, the Management Server checks with the Application Server. The Management Server confirms the cancellation, it makes application software de-activate and/or remove from the mobile device.

7.2.8 Post-conditions

- Measured wellness data are stored in the M2M Service Platform or the Application Server.
- User is able to access to the Application Server and explore the graph of the wellness data trend.

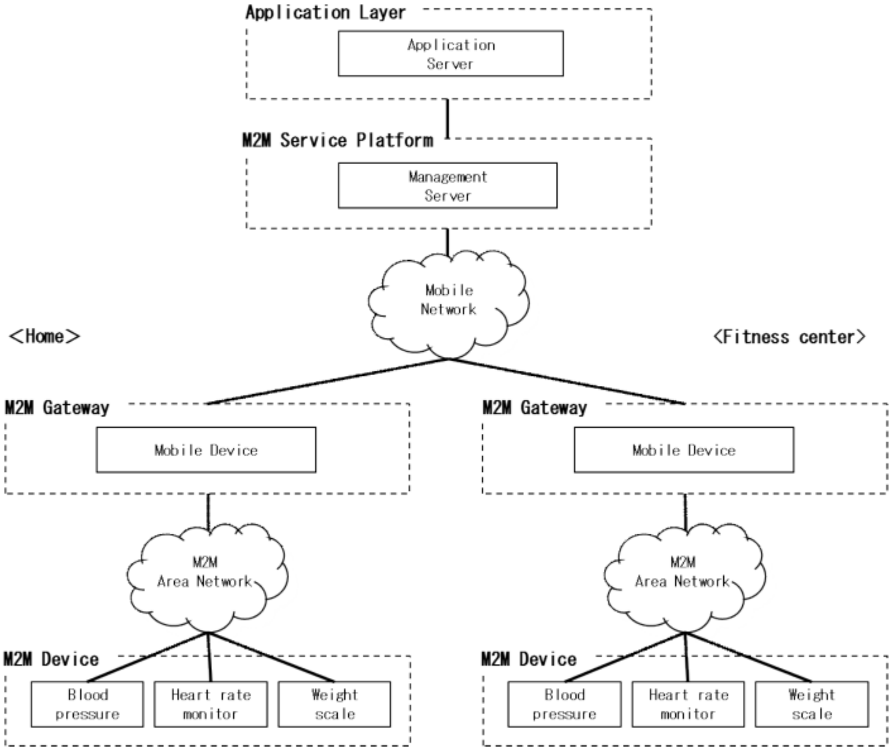


Figure 27: Figure 7.2.9-1 Wellness Service High Level Illustration

7.2.9 High Level Illustration

7.2.10 Potential Requirements

1. M2M Gateway SHALL be able to detect device that can be newly installed (paired with the M2M Gateway).
2. Upon detection of a new device the M2M Gateway SHALL be able to be provisioned by the M2M Service Platform with an appropriate configuration which is required to handle the detected device.
3. The M2M Service Platform SHALL be able to provide an authenticated and authorized application in the M2M Gateway with appropriate configuration data.

7.3 Secure remote patient care and monitoring

7.3.1 Description

E-health applications, that provide the capability for remote monitoring and care, eliminate the need for frequent office or home visits by care givers, provide great cost-saving and convenience as well as improvements. “Chronic disease management” and “aging independently” are among the most prominent use cases of remote patient monitoring applications. More details of the actors and their relationships for these use cases are mentioned in details in an ETSI document [i.4] and are not covered here. Instead this contribution provides an analysis of specific security issues pertaining to handling of electronic health records (EHR) to provide a set of requirements in the context of oneM2M requirement definition work.

Remote patient monitoring applications allow measurements from various medical and non-medical devices in the patient’s environment to be read and analysed remotely. Alarming results can automatically trigger notifications for emergency responders, when life-threatening conditions arise. On the other hand, trigger notifications can be created for care givers or family members when less severe anomalies are detected. Dosage changes can also be administered based on remote commands, when needed.

In many cases, the know-how about the details of the underlying communications network and data management may be outsourced by the medical community to e-health application/ solution provider. The e-health solution provider may in turn refer to M2M service providers to provide services such as connectivity, device management. The M2M service provider may intend to deploy a service platform that serves a variety of M2M applications (other than e-health solution provider). To that end, the M2M service provider may seek to deploy optimizations on network utilization, device battery or user convenience features such as ability of using web services to reach application data from a generic web browser. The M2M service provider may try to provide uniform application programming interfaces (APIs) for all those solution providers to reach its service platform in a common way. From the standpoint of the M2M application, the application data layer rides on top a service layer provided by this service platform. By providing the service platform and its APIs, the M2M SP facilitates development and integration of applications with the data management and communication facilities that are common for all applications.

As part of providing connectivity services, the M2M service provider may also provide secure sessions for transfer of data for the solution providers that it serves. In many jurisdictions around the world, privacy of patient healthcare data is tightly regulated and breaches are penalized with hefty fines. This means the e-health application provider may not be able to directly rely on the security provided by the M2M service provider links/sessions and instead implement end to end security at application layer. This puts additional challenges on the M2M service platform, since it needs to provide its optimizations on encrypted data.

One particular issue with e-health is that not only the data is encrypted, but it may also contain data at different sensitivity levels, not all of which appropriate to each user. For instance in the US the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of protected health information. Different actors within a healthcare scenario may have different levels of authorizations for accessing the data within the health records, so the information system must take care to present the health data to each user according to the level of authorization for that user. A process, common to address this issue is redaction. This means that one starts with a document that originally includes data of all sensitivity levels and then removes any piece of information that has a higher sensitivity level than the pre-determined redaction level (RL). The end result is a redacted version of the initial document that can be presented to a person/entity that has the matching authorization level (AL). Persons with lower AL are not authorized to view this particular version of document. The redaction engine can produce multiple versions of the initial records, where each version corresponds to one redaction level (RL) including material at specific sensitivity level (and lower).

Care must be taken to ensure that only authorized users have access to data. Therefore, the system must match the redaction level (RL) of data with the authorization level (AL) and present the proper version of the record for each actor.

The redaction engine may reside at a policy control server or at the application server operated by the M2M application service provider. The policy server may also hold policies on which users get which authorization level (AL), while an authorization server may be in charge of authenticating each user and assigning her the proper AL.

In a system relying on notifications based on prior subscriptions, data must be examined first to determine which subscribers should receive notifications and then only those subscribers should be capable to retrieve the data about which the notification is sent.

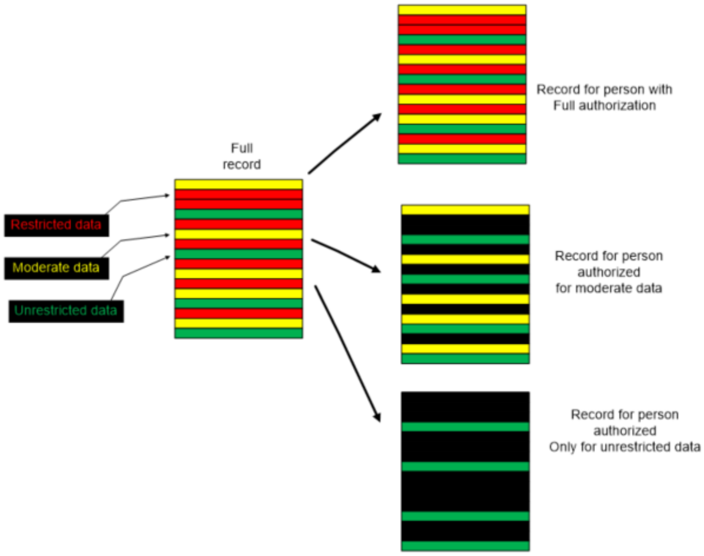


Figure 28: Figure 7.3.1-1 An illustration of a process with 2 levels of redaction. Black colour indicates a data field that is masked from an unauthorized user

7.3.2 Source

oneM2M-REQ-2013-0227R02 e-Health application security use case

7.3.3 Actors

- Patients using sensor (medical status measurement) devices
- E-Health application service providers, providing sensor devices and operating remote patient monitoring, care and notification services
- Care givers (e.g. nurses, doctors, homecare assistants, emergency responders) and other administrative users with authorization to access healthcare data (e.g. insurance providers, billing personnel). We also refer to these entities as “participants in the healthcare episode” in some occasions.
- M2M service providers, network operators, providing connectivity services for the patients, e-health application providers and care givers.

7.3.4 Pre-conditions

- A categorization rule set, that is able to categorize various entries within a medical record according to the sensitivity levels and label them accordingly, must exist.
- A redaction engine that is able to examine the raw medical record and produce different versions of the record at different redaction levels (RL) with only data that is at or below a sensitivity level.

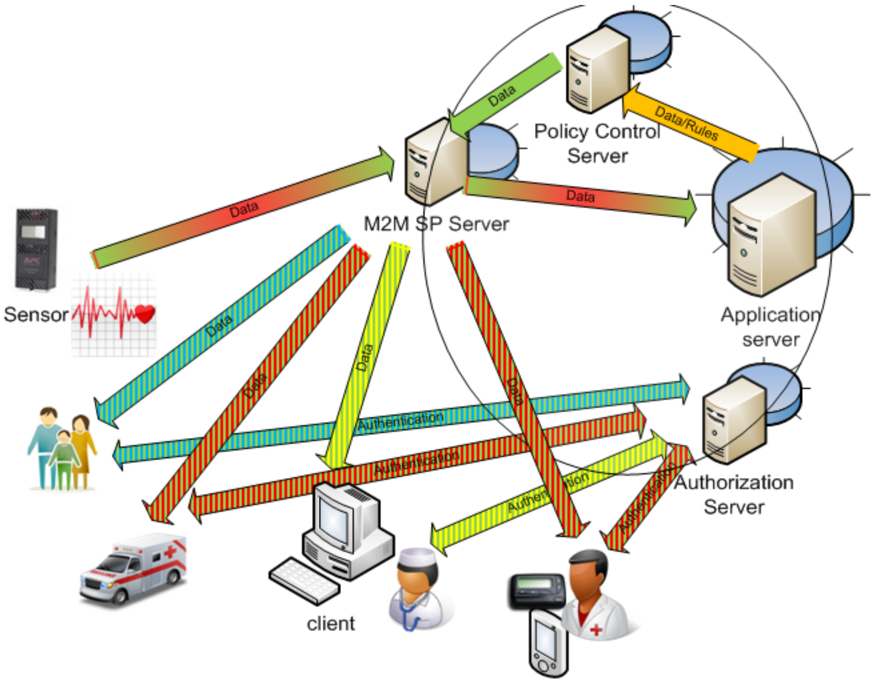


Figure 29: Figure 7.3.1-2 An e-Health application service capable of monitoring remote sensor devices and producing notifications and data to health care personnel based on their authorization level

- A policy engine that is able to examine medical records and determine level of criticality (applicable to one of the flows described).
- A set of authorization policies that describe what authorization level (AL) is required to be able to access data at each redaction level (RL).
- An authorization engine/server that interacts with each user of the e-health application to verify their claimed AL, for example the server may perform an authentication function with the user.
- The e-health application server that is capable of interacting with the authorization server to check the AL of each user to determine the user's RL before serving data at the requested (or appropriate) RL to that user.

7.3.5 Triggers

- Creation of new measurement data by a remote medical device.
- Analysis of received measurement data at application servers, and determination of need for redaction, or creation of alarms and notifications, etc.
- Requests from participants in a health care episode (caregivers) for sensitive medical records.
- Arrival of new participants (new doctors, etc.) in the health care episode

7.3.6 Normal Flow

In the main flow a remote medical device performs a measurement and sends it to an e-health application provider's (AP) application server, which in turn processes the data and notifies the appropriate actors regarding the condition of the patient.

The AP provides an application client to be installed on the device, and the application servers that interact with all the application clients. Both the application client and application server use the data management and communication facilities within the service layer exposed through the service layer APIs.

This flow could be as follows:

- The sensor on the medical device performs a measurement and reports it to the application client on the device.
- The application client (e.g. an e-health application) uses the service layer API to reach the service layer (provided by M2M service provider) within the device to transfer data to the application server. When application level data privacy is required, the application client on the device must encrypt the sensor data before passing the data to the service layer. Since the data must be kept private from service layer function, the encryption keys and engine used by the application client must be kept within a secure environment that is out of reach of the M2M service provider. This may require a set of secure APIs to reach the application's secure environment. It may however be more convenient that these APIs are bundled with the

secure APIs used to reach keys/ environment that secures the service layer, so that each application only deals with one set of APIs.

- The service layer (provided by M2M service provider) passes the data from the device to the M2M service provider servers.
- The M2M service layer at the server side passes the data to the e-health application server.
- At this point, the application needs to prepare to notify any interested parties (caregivers) that have subscribed to receive notifications regarding the status or data received about a patient. However, when application data is encrypted and redaction is to applied, more intelligence must be applied regarding who is authorized to receive a notification regarding status update. This may be done as follows:
- After the e-health application server receives the data from M2M SP server, it decrypts the data, analyses and performs redactions based on application policies (possibly with help of policy servers). This produces multiple versions of the initial data (one at each redaction level). The application server then re-encrypts each redacted version. Each encrypted version needs to be tagged based on the redaction level (RL) it contains and possibly the authorization level (AL) it requires for viewing.
- The application server passes the tagged data (multiple files) to the M2M service provider server (the service layer server)
- The M2M SP server will then sends a notification to each of the subscribers as long as their AL is at or above the level required to view any of the data just received. This means a separate authorization server may have initially performed an authorization of each user that requests to subscribe to data regarding each patient. The authorization would need to assess the identity of the user, her role and the claimed AL before registering the user for notifications. It is possible that the authorization server upon assertion of AL for each user provide the necessary decryption keys for receiving encrypted redacted data to the user's device. In that case, the device that the user is using needs to be authenticated based on a verifiable identity (an identity that is bound to a tamper-proof identity within the secured environment). Alternatively, the decryption keys may be present within the user devices (e.g. specific USB stick!) through other means. In either case a mechanism must exist to release decryption keys stored with an authenticated device's secure storage based on the user authorization and thus a binding of user and device authentications may be important.

7.3.7 Alternative Flow

Alternative Flow No 1

One alternative flow is when a user requests information regarding a patient without having previously subscribed for any notifications. The M2M SP server must first refer the user to the authorization server to assert the user's authorization level (AL) before serving the user with a response.

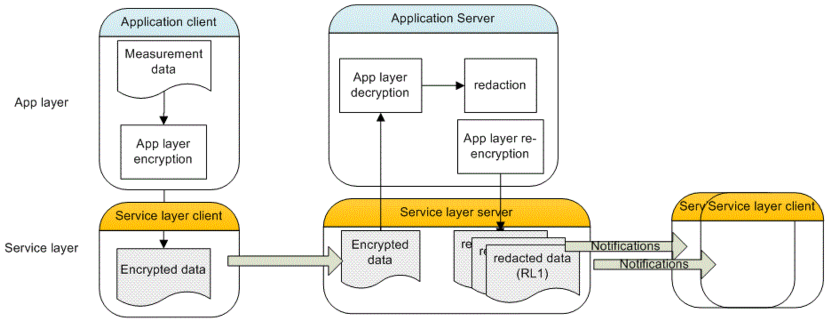


Figure 30: Figure 7.3.6-1 Dealing with Redaction in an M2M system separating Application layer and Service layer. The Service layer functions are provided by M2M service provider, while application layer functions are provided by application provider

Alternative Flow No 2

One alternative flow is when a user requests to provide instruction commands regarding a patient to a remote device. The service must make sure that the user has the proper AL to issue the command.

Alternative Flow No 3

One alternative flow is when users are categorized not based on authorization levels but based on the level of their responsiveness. For instance, a life-critical event must cause the emergency responders to receive notifications and act very quickly, while a less critical event may only lead to a family member to be alerted. The subscription/ notification system should provide this level of granularity, i.e. information can be tagged based on criticality level. There must also be a policy engine that categorize the data based on its criticality level (CL).

7.3.8 Post-conditions

Normal flow

Multiple versions of patient record exist for multiple redaction levels at the M2M service provider servers. Each user can pull the version corresponding to her AL after she has been notified about presence of new data. The server can serve the data based on its RL tagging or AL tagging.

Alternative Flow No 3

Data is tagged with criticality level and served to each user according to their level of responsiveness.

7.3.9 High Level Illustration

Not provided

7.3.10 Potential requirements

1. The M2M system shall support M2M applications with establishing a security context for protecting the privacy of application data from the underlying M2M service.
   This means support of synchronous exchanges required by identification/ authentication/ or other security algorithms for establishment of security associations (keys, parameters, algorithms) for end-to-end encryption and integrity protection of data. Furthermore, any exchanges for establishing the M2M application security context can use the security context at underlying layers (e.g. M2M service layer) to protect the exchanges (as another layer of security), but the M2M application security context, once established, would be invisible to the M2M system.
2. The M2M system must support mechanisms for binding identities used at service layer and/or application layer to the tamper proof identities that are available within the device secured Environment.
   Anchoring higher layer identities to a low level identity (e.g. identities that are protected at the hardware or firmware level) is needed to be able to securely verify claimed identities during device authentication processes at various levels. Also APIs providing lower layer identities to application layer for the purpose of binding application layer identities and lower layer identities.
3. M2M devices and M2M system shall support provisioning of application specific parameters and credentials prior and/or after field deployment, while preserving the privacy of provisioned material from M2M system if needed.
   This means the M2M devices must support identities and credentials that are independent of the M2M system provider credentials and could be used for delivery of application specific parameters/credentials.
4. When M2M application data security is independent of M2M system, the Secured Environment within devices or infrastructure entities shall provide separation between the secured environments for each application and the secured environment for M2M service layer.
5. The secure environment described in requirement above shall provide both secure storage (for keys, sensitive material) and secure execution engine (for algorithms and protocols) for security functions for each application or service layer.
6. The security functions provided by the Secured Environment should be exposed to both M2M service layer and M2M applications through a set of common APIs that allow use of Secured Environment of each of M2M service layer and M2M applications in a uniform fashion.
7. The M2M service layer must be able to perform authorization before

serving users with sensitive data.

8. The authorization process should support more than two authorization levels and the service layer must be able to accommodate response/ notifications to the users based on their level of authorization.
9. The M2M service layer must accommodate tagging of opaque application data for various purposes, such as urgency levels, authorization/redaction levels, etc.
10. There must be a mechanism to allow the M2M application or service layer to bind user credentials/ authorizations to device credentials, such that credentials within the device can be used for security purposes during or after a user is authenticated/ authorized.
11. The M2M service layer must be able to accommodate delay requirements for the application based on the tagging applied to the application data. For instance, data that is marked critical must create notifications for first-level responders.
12. Any software client, especially those performing security functions (e.g. authentication clients) must be integrity protected (signed) and verified after device power up/reset or before launch. Widely deployed standards such PKCS#7 or CMS should be used for code signing.

7..4 Use case for information correlation

7.4.1 Description

Different devices have different functions, but these functions may produce related information. For example, a smart watch can be used to monitor heart rate, number of steps etc.; meanwhile, a treadmill/bicycle can be used to monitor speed, distance, and calories burned. When these devices refer to the same person, the data produced by these devices are highly related, since the data is all about the health of the person.

At the same time, the relationship of different devices is dynamic. For example, when doing home exercise, the smart watch and treadmill are related. Similarly, when doing outside exercise, the smart watch and bicycle are related.

7.4.2 Source

REQ-2017-0073R02 Use case for information correlation

7.4.3 Actors

- Smart Watch Device: has function to monitor the heart rate, number of steps of the End Users.
- Treadmill Device: has function to monitor the speed, distance, calories burned of the End Users.
- Bicycle Device: has function to monitor the speed, distance, calories burned of the End Users.

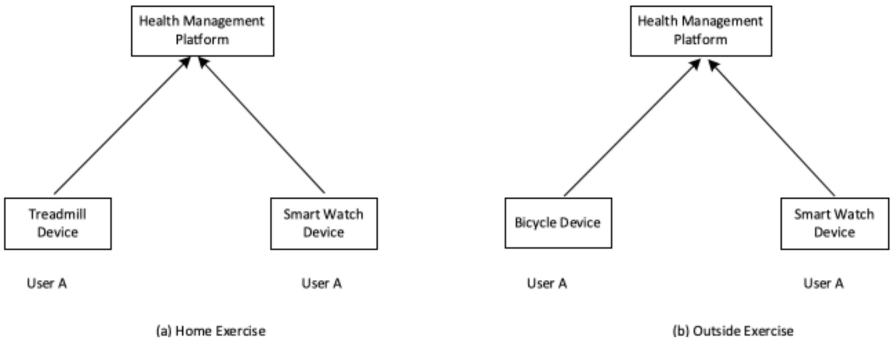


Figure 31: Figure 7.4.1-1 (a) Home exercise and (b) outside exercise use cases for information correlation

- Healthcare Management Platform: manages the healthcare related devices and stores the healthcare related information.
- End User: the user of the healthcare related devices.

7.4.4 Pre-conditions

Smart Watch Device has the capability to discovery the Treadmill Device and Bicycle device, for example, using the NFC technology to discover the Treadmill device and Bicycle device.

7.4.5 Triggers

None

7.4.6 Normal Flow

1. Smart Watch Device, Treadmill Device, Bicycle Device register to Healthcare Management Platform;
2. During home exercise time, User A uses the Smart Watch Device to find the Treadmill Device;
3. Smart Watch Device initiates an information correlation request to the Healthcare Management platform;
4. Healthcare Management platform correlates the information of the Smart Watch Device and Treadmill Device;
5. User A leaves the treadmill device and can't find the treadmill device;
6. The Smart Watch Device initiates an information de-correlation request to the Healthcare Management platform;
7. Healthcare Management platform de-correlated the information of the Smart Watch Device and Treadmill Device.
8. During outside exercise time, User A uses the Smart Watch Device to find the Bicycle Device;

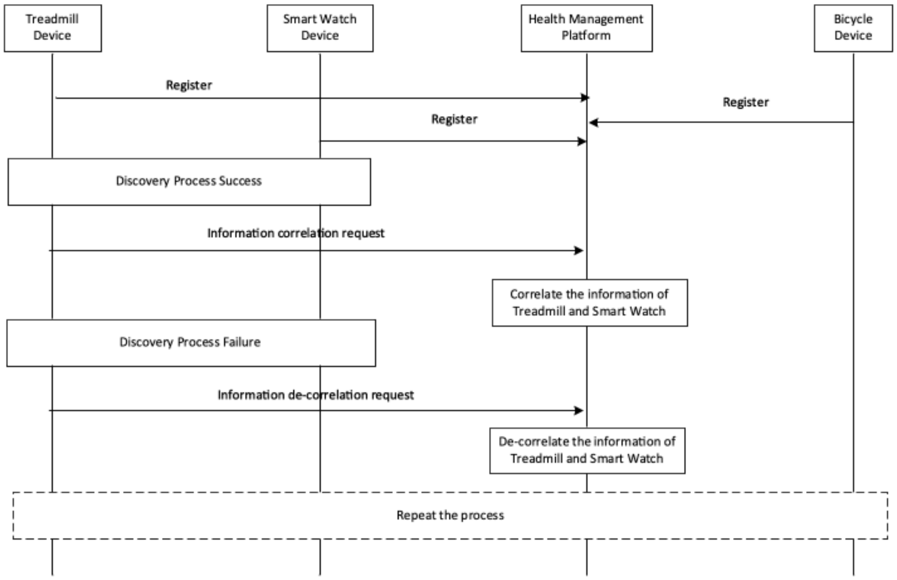

Treadmill Device
Smart Watch Device
Health Management Platform
Bicycle Device
Register
Register
Register
Discovery Process Success
Information correlation request
Correlate the information of Treadmill and Smart Watch
Discovery Process Failure
Information de-correlation request
De-correlate the information of Treadmill and Smart Watch
Repeat the process

Figure 32: Figure 7.4.6-1 Information correlation normal flow

9. Smart Watch Device initiates an information correlation request to the Healthcare Management platform;
10. Healthcare Management platform correlates the information of the Smart Watch Device and Bicycle;
11. User A leaves the bicycle device and can't find the bicycle device;
12. The Smart Watch initiates an information de-correlation request to the Healthcare Management platform;
13. Healthcare Management platform de-correlated the information of the Smart Watch Device and Bicycle Device.

7.4.7 Alternative flow

None

7.4.8 Post-conditions

None

7.4.9 High Level Illustration

None

7.4.10 Potential requirements

1. The oneM2M system shall support the correlation of information from different entities.
2. The oneM2M system shall support de-correlation of information from different entities.

8 Public Services Use Cases

8.1 Street Light Automation

8.1.1 Description

Street Light Automation can be considered as part of the City Automation (ETSI classifier) vertical industry segment - and related to others e.g. Energy, Intelligent Transportation Systems, etc.

Industry segment organisations: none known
Industry segment standards: none known
Deployed: with varying functionality, in multiple countries

Street Light Automation Goals

- Improve public safety
- Reduced energy consumption / CO2 emissions
- Reduce maintenance activity

Methods

- Sensing and control
- Communications
- Analytics

A street light automation service provider, provides services to control the luminosity of each street light dependent upon (resulting in 10 sub-use cases):

Local (street level)

1. Light sensors
2. Power quality sensors
3. Proximity sensors (civilian or emergency vehicles, pedestrians)

Street light automation service provider operation centre

4. Policies (regulatory & contractual)
5. Ambient light analytics (sunrise/sunset, weather, moonlight, etc.)
6. Predictive analytics (lights parts of streets predicted to be used, etc.)

Communications received from other service providers

7. Traffic light service (emergency vehicle priority)
8. Emergency services (vehicle routing, police action, etc.)

9. Road maintenance service (closures and/or diversions)
10. Electricity service (power overload)

8.1.2 Source

oneM2M-REQ-2012-0036R07 Proposed Use Case Street Light Automation

> Note: From public document research: "Street Light Control" use case identified in [i.5] ETSI TR 102 897

8.1.3 Actors

- Street light automation application service provider, has the aim is to adjust street light luminosity.
- Street light devices have the aim is to sense, report, execute local and remote policies, illuminate street.
- Traffic light application service provider, has the aim is to enhance their emergency vehicle service using street lighting.
- Emergency services application services provider, have the aim is to brightly illuminate police action areas and brightly illuminate planned path of emergency vehicles.
- Road maintenance application service provider, has the aim is to obtain extra street light signalling near closed roads.
- Electricity application service provider, has the aim is to have electricity consumers reduce their load when an overload is declared.

8.1.4 Pre-conditions

See sub-case flows.

8.1.5 Triggers

See sub-case flows.

8.1.6 Normal Flow

1. **Sub use case 1 -** Local: Light sensors **Summary** : (no atomic action steps) **Trigger** : Detected light level moves below/above threshold **Action** : Increase/decrease luminosity in a set of street lights **Detailed flow** (no confirmation, etc. - actors in "quotes", system under study in italics)

    a. "Street lights" message the Street light system that street light sensors have detected light level movement below/above threshold.
    b. Street light system informs the "street light operation centre" with the street light sensor information.
    c. "Street light operation centre" messages the Street light system with a street light control message to increase/decrease luminosity according to "street light operation centre" policy.

d. Street light system messages the “street lights” with a street light control message to increase/decrease luminosity according to “street light operation centre” policy.
e. Optionally (normal case), if “street lights” receive a control command from the Street light system within some time, then, “street lights” increase/decrease luminosity in a set of street lights according to “street light operation centre” policy.
f. Optionally (alternative case), if “street lights” do not receive a control command from the Street light system within some time, then, “street lights” increase/decrease luminosity in a set of street lights, according to local policy.

Note that the terminology “policy” refers to a set of rules which may be dependent upon variables output from analytics algorithms.

2. **Sub use case 2 -** Local: Light sensors **Local** : Power quality sensors **Summary** : (no atomic action steps) **Trigger** : Detected input voltage level moves above/below threshold **Action 1** : Send alert message to electricity service provider Action 2: Decrease/increase energy applied to a set of street lights Detailed flow (no confirmation, etc. - actors in “quotes”, system under study in italics)

   a. “Street lights” message the Street light system that street light power sensors have detected input voltage level movement above/below threshold
   b. Street light system informs the “street light operation centre” with the street light sensor information
   c. “Street light operation centre” messages the Street light system with an alert message to “electricity service provider” according to “street light operation centre” policy.
   d. Street light system informs “electricity service provider” of alert message.
   e. “Street light operation centre” messages the Street light system with a street light control message to increase/decrease luminosity according to “street light operation centre” policy.
   f. Optionally (normal case), if “street lights” receive a control command from the Street light system within some time, then, “street lights” increase/decrease luminosity in a set of street lights according to “street light operation centre” policy.
   g. Optionally (alternative case), if “street lights” do not receive a control command from the Street light system within some time, then, “street lights” increase/decrease luminosity in a set of street lights, according to local policy

3. **Sub use case 3 -** Local: proximity sensors (civilian or emergency vehicles, pedestrians) **Summary** : (no atomic action steps) **Trigger** : Civilian or emergency vehicle or pedestrian detected entering/leaving street section **Action** : Increase/decrease luminosity in a set of street lights **Detailed**

flow (no confirmation, etc. - actors in “quotes”, system under study in italics)

  a. “Street lights” message the Street light system that street light power sensors have detected civilian or emergency vehicle or pedestrian detected entering/leaving street section.
  b. Street light system informs the “street light operation centre” with the street light sensor information.
  c. “Street light operation centre” messages the Street light system with a control message to increase/decrease luminosity according to “street light operation centre” policy.
  d. Street light system messages the “street lights” with a street light control message to increase/decrease luminosity according to “street light operation centre” policy.
  e. Optionally (normal case), if “street lights” receive a control command from the Street light system within some time, then “street lights” increase/decrease luminosity in a set of street lights according to “street light operation centre” policy.
  f. Optionally (alternative case), if “street lights” do not receive a control command from the Street light system within some time, then, “street lights” increase/decrease luminosity in a set of street lights, according to local policy.

4. **Sub use case 4 -** Operation Centre: Policies (regulatory & contractual) **Summary** : (no atomic action steps) **Trigger** : SLA non-conformity for low intensity imminent **Action** : Increase luminosity in a set of street lights to keep within SLA **Detailed flow** (no confirmation, etc. - actors in “quotes”, system under study in italics)

   a. The “street light operation centre” detects through analytics that an SLA regarding minimum street light intensity is in danger of not being met.
   b. “Street light operation centre” messages the Street light system with a control message to increase luminosity according to “street light operation centre” policy.
   c. Street light system messages the “street lights” with a street light control message to increase luminosity according to “street light operation centre” policy.

5. **Sub use case 5 -** Operation centre: Ambient light analytics (sunrise/sunset, weather, moonlight) **Summary** : (no atomic action steps) **Trigger 5a** : A band of rain moves across an area of street lights **Action 5a** : Increase/decrease luminosity in a rolling set of street lights **Trigger 5b** : Sunrise/sunset is predicted to occur area in 30 minutes **Action 5b** : Decrease/increase luminosity in a rolling set of street lights **Detailed flow** (no confirmation, etc. - actors in “quotes”, system under study in italics)

   a. The “street light operation centre” detects through analytics that

(5a) a band of rain is moving across an area of street lights, or (5b) Sunrise/sunset is predicted to occur area in 30 minutes.

   b. "Street light operation centre" messages the Street light system with a street light control message to increase/decrease luminosity according to "street light operation centre" policy.
   c. The Street light system messages the "street lights" to increase/decrease luminosity in a set of street lights according to "street light operation centre" policy.

6. **Sub use case 6** - Operation centre: Predictive analytics (lights parts of streets predicted to be used) **Summary** : (no atomic action steps) **Precondition** : Vehicle paths are tracked via proximity sensors and a route model is generated **Trigger** : A vehicle enters a street section which has 85% probability of taking the next left turn **Action** : Increase luminosity on current street section ahead and also on street on next left **Detailed flow** (no confirmation, etc. - actors in "quotes", system under study in italics)

   a. "Street lights" message the Street light system that street light power sensors have detected civilian or emergency vehicle entering street section
   b. Street light system informs the "street light operation centre" with the street light sensor information
   c. "Street light operation centre" messages the Street light system with a control message to increase/decrease luminosity according to "street light operation centre" policy.
   d. Street light system messages the "street lights" with a street light control message to increase/decrease luminosity according to "street light operation centre" policy.

7. **Sub use case 7 -** From other service providers: Traffic light service input (emergency vehicle priority) **Summary** : (no atomic action steps) **Trigger** : An emergency vehicle is approaching a junction **Action** : Increase luminosity in street lights along streets leading away from junction **Detailed flow** (no confirmation, etc. - actors in "quotes", system under study in italics)

   a. "Traffic light service provider" messages the Street light system that emergency vehicle approaching street junction from certain direction.
   b. Street light system informs the "street light operation centre" with the street junction information.
   c. "Street light operation centre" messages the Street light system with a control message to increase luminosity according to "street light operation centre" policy.
   d. Street light system messages the "street lights" with a street light control message to increase luminosity according to "street light operation centre" policy.

8. **Sub use case 8 -** From other service providers: Emergency services input (vehicle routing, police action) **Summary** : (no atomic action steps) **Trigger 8a** : An emergency vehicle route becomes active **Action 8a** : Increase luminosity in street lights along vehicle route **Trigger 8b** : An area is declared as having an active police action **Action 8b** : Increase luminosity in street lights within police action area **Detailed flow** (no confirmation, etc. - actors in “quotes”, system under study in italics)

   a. “Emergency services provider” messages the Street light system that (8a) emergency vehicle street route is active, or (8b) an area is declared as having an active police action
   b. Street light system informs the “street light operation centre” with the street junction information
   c. “Street light operation centre” messages the Street light system with a control message to increase luminosity according to “street light operation centre” policy.
   d. Street light system messages the “street lights” with a street light control message to increase luminosity according to “street light operation centre” policy.

9. **Sub use case 9 -** From other service providers: Road maintenance service input (closures and/or diversions) **Summary** : (no atomic action steps) **Trigger 9a** : A road is closed **Action 9a** : Program a changing luminosity pattern in street lights near to closed road **Trigger 9b** : A route diversion is activated **Action 9b** : Program a changing luminosity pattern in street lights along the streets of the diversion **Detailed flow** (no confirmation, etc. - actors in “quotes”, system under study in italics)

   a. “Road Maintenance service provider” messages the Street light system that (9a) a road is closed, or (9b) a route diversion is activated
   b. Street light system informs the “street light operation centre” with the road maintenance information
   c. “Street light operation centre” messages the Street light system with a control message to set lights to changing luminosity pattern according to “street light operation centre” policy.
   d. Street light system messages the “street lights” with a street light control message to set lights to changing luminosity pattern according to “street light operation centre” policy.

10. **Sub use case 10 -** From other service providers: Electricity service input (power overload) **Summary** : (no atomic action steps) **Trigger** : A power overload situation is declared **Action** : Decrease luminosity in a set of street lights **Detailed flow** (no confirmation, etc. - actors in “quotes”, system under study in italics)

    a. “Electricity service provider” messages the Street light system that (9a) that an overload condition exists across some area.
    b. Street light system informs the “street light operation centre” with

the overload condition information

c. “Street light operation centre” messages the Street light system with a control message to decrease luminosity according to “street light operation centre” policy.

d. Street light system messages the “street lights” with a street light control message to decrease luminosity according to “street light operation centre” policy.

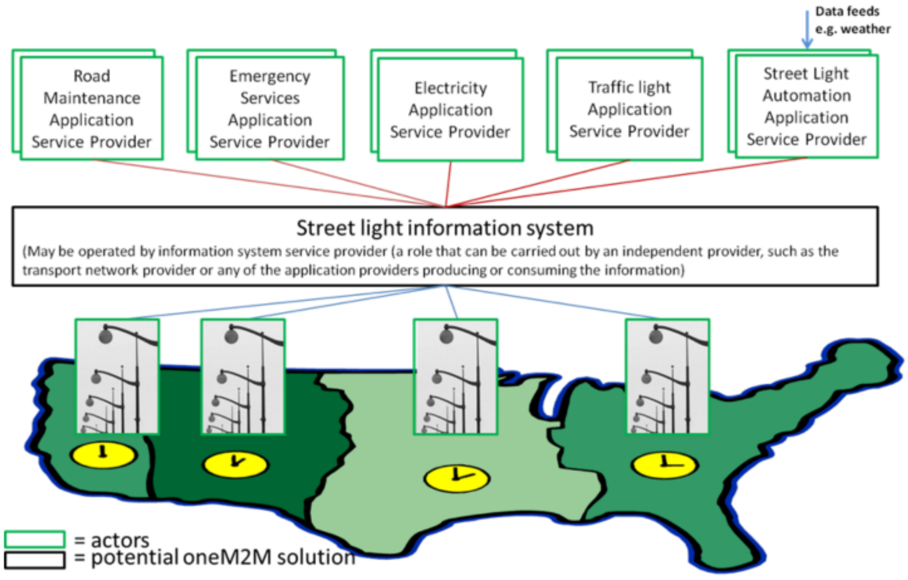
8.1.7 Alternative Flow

In the case of loss of communications, street lights have local policies which they obey.

8.1.8 Post-conditions

Street light luminosity or luminosity pattern is adjusted as needed.

8.1.9 High Level Illustration



Data feeds
e.g. weather
Road Maintenance Application Service Provider
Emergency Services Application Service Provider
Electricity Application Service Provider
Traffic light Application Service Provider
Street Light Automation Application Service Provider
Street light information system
(May be operated by information system service provider (a role that can be carried out by an independent provider, such as the transport network provider or any of the application providers producing or consuming the information)
= actors
= potential oneM2M solution

Figure 33: Figure 8.1.9-1 Street Light Automation High Level Illustration

8.1.10 Potential Requirements

Generic (needed by two or more verticals or applications)

1. The M2M solution shall support the ability to collect information from M2M devices.

2. The M2M solution shall support the ability to deliver collected information from M2M devices to M2M applications.
3. The M2M solution shall support control commands (for devices) from M2M applications.
4. The M2M solution shall support control commands for groups of M2M devices.
5. The M2M solution shall support the ability to receive device application software from M2M applications.
6. The M2M solution shall support the ability to deliver device application software to M2M devices.
7. The M2M solution shall provide mechanisms for information sharing, i.e. receiving information from M2M applications (information providing) to be consumed by other M2M applications (information consuming).
8. The M2M solution shall provide charging mechanisms for information sharing among M2M applications.
9. The M2M solution shall support the ability to provide an estimate of the time period from when a device sent a message to the M2M solution until when it responded with a message to the device.
10. The M2M solution shall provide security context (authentication, encryption, integrity protection) for secure connection between entities. The security context shall include mechanisms and techniques on how to setup a security connection , and where the security connection information is stored and how to establish the secure connection
11. The M2M service layer shall provide security mechanisms to facilitate the end to end security of M2M applications.
12. The M2M service layer shall provide security mechanisms to avoid compromising the end to end security of M2M applications.

Specific (to this vertical/use case)
None

Note that the terminology:

- “Device application software” refers to application software that runs on a device including programs, patches, program data, configuration, etc.
- “M2M application” is any application that makes use of the M2M service layer - some form of prior agreement may be needed.

Security Considerations

- Attack vectors and example impacts:
  - By sending false reports of sensors to applications
  - Energy provider overdriving voltage
- By sending false control commands to devices
  - Blackout to obscure crime
- By blocking valid messages
  - Energy wastage

8.2 Devices, Virtual Devices and Things

8.2.1 Description

The municipality of a Smart City operates an Application Service that monitors traffic flow and switches traffic lights depending on traffic. This “traffic application” controls the traffic lights and a couple of surveillance cameras to observe traffic flow.

The traffic application makes several of the surveillance cameras discoverable in the M2M System and potentially allows access to the data (the video streams) of these cameras. The surveillance cameras can be searched and discovered in the M2M System based on search criteria such as type (e.g. video camera for traffic) and other meta-data (e.g. location or activation state).

In addition to (physical) devices the traffic application publishes “virtual devices” that act similar to sensors and provide derived data such as: number of vehicles that passed during the last minute/hour, average speed of vehicles . . .

Also these “virtual devices” can be searched and discovered in the M2M System based on type and other meta-data.

However, in contrast to the previous case (real devices) virtual devices only implemented as software and do not require a Connectivity Layer. They are data structures published by the traffic application.

The traffic application charges other applications to receive data from these virtual devices.

Finally, the traffic application also publishes “things” in the M2M System like roads and intersections. Other “things” the traffic application might publish are phased traffic lights (green wave).

“Things” are similar to “virtual devices” but have relations to other “things” (e.g. a section of a road lies between two intersections).

A “street”, published by the traffic application, provides information on the average speed of traffic, congestion level, etc. A “series of phased traffic lights” provides information about which traffic lights are in phase, the current minimal/maximal/optimal speed, etc.

The “traffic application” of the Smart City charges other applications to access data from its published “things”.

A second Application Service, a “logistics application” is operated by a company that manages a fleet of trucks to deliver goods all over the country. This “logistics application” provides an optimal route for each truck at any time.

One of the trucks is currently driving in the Smart City. The logistics application has a service level agreement with the traffic application of the Smart City.

The logistics application discovers all things (streets, intersections. . .) that are relevant to calculate an optimal route for the truck, based on type and location. It uses the published data and is charged for the access to these data.

8.2.2 Source

oneM2M-REQ-2012-0073 Use Case on Devices - Virtual devices - Things

8.2.3 Actors

- The municipality of a Smart City (Application Service Provider)
- The fleet management company (Application Service Provider)
- The M2M Service provider (M2M Service provider)

8.2.4 Pre-conditions

- The municipality of a Smart City operates a “traffic application” that monitors traffic flow and switches traffic lights.
- The fleet management company operates a “logistics application” that manages a fleet of trucks.
- Both Applications are using the same M2M Service Capabilities Network (MSCN) operated by the M2M Service provider.
- The traffic application allows the logistics application to access some of its Devices, Virtual devices and Things.

8.2.5 Triggers

None

8.2.6 Normal Flow

- The traffic application creates Virtual devices (e.g. traffic sensors) and Things (e.g. streets, series of phased traffic lights…) for use by other M2M applications in the MSCN of the M2M Service operator.
- The traffic application publishes the semantic description (types, relations, and meta-data) of its Devices (e.g. cameras), Virtual devices and Things in the MSCN of the M2M Service operator. The traffic application restricts discoverability of its Virtual devices and Things to applications provided by business partners of the municipality of a Smart City.
- The traffic application enables access to the data of some of its traffic cameras to all M2M applications, but access to the data of virtual devices and things is restricted to applications of business partners (e.g. the logistics application).
- The logistics application searches the MSCN of the M2M Service operator for things and virtual devices in the vicinity of the truck. Based on the semantic search criteria (described by reference to a taxonomy or ontology) only the things and virtual devices that are useful for calculating the route of the truck are discovered.

- The logistics application reads the data from relevant things and virtual devices and calculates the optimal route for the truck.
- The logistics application is charged by the MSCN of the M2M Service operator for reading the data from things and virtual devices of the traffic application.
- The traffic application is reimbursed for usage of its things and virtual devices.

8.2.7 Alternative Flow

None

8.2.8 Post-conditions

None

8.2.9 High Level Illustration

None

8.2.10 Potential Requirements

1. The M2M System shall provide a capability to an Application shall be able to create Virtual Devices and Things in the M2M Service Capability Network.
2. The M2M System shall provide a capability to an Application shall be able to publish semantic descriptions and meta-data (e.g. location) of its Devices, Virtual Devices and Things in the M2M Service Capability Network.
3. The M2M System shall provide a capability to an Application to search for and discover Devices, Virtual Devices and Things in the M2M Service Capability Network based on their semantic descriptions and meta-data. The supported formats of semantic descriptions shall be described in the oneM2M standard.
4. The M2M System shall provide a capability to an Application shall be able to control, via the M2M Service Capability Network, access to semantic descriptions and meta-data of its Devices, Virtual Devices and Things.
5. The M2M System shall provide a capability to an Application shall be able to allow, via the M2M Service Capability Network, access to its Devices, Virtual Devices and Things to individual other applications.

8.3 Car/Bicycle Sharing Services

None

Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2012-0132R01 Use Case: Car/Bicycle Sharing Services

8.4 Smart Parking

None

> Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2013-0169R03 Use Case Smart Parking

8.5 Information Delivery service in the devastated area

8.5.1 Description

Background

- When a disaster occurs in the metro area, many victims require various kinds of information such as traffic, safety and evacuation area. However, it may be difficult to collect such information immediately and properly.

Description

- This is the use case of a M2M Service that transmits required information to the User Devices (UDs) of disaster victims immediately and automatically. Some of the information shall be maintained before a disaster happens.
- UD connects to the Wireless Gateways (WGs). The WGs properly provide the UDs with the information stored on its local DB to avoid the network congestion.
- When Disaster Sensor detect a serious disaster, the Service Provider multicasts the latest information which the victims need such as traffic congestion, locations of closest hospitals and evacuation area. The UDs receive and update the information automatically.
- After the disaster happens, the Service Provider continues to update the information according to the situation of traffic, safety and evacuation area as well as the data from Disaster Sensors and Equipment for public information.

8.5.2 Source

oneM2M-REQ-2012-0074R09 Use Case: Information Delivery service in the devastated area

8.5.3 Actors

- Service Provider has the aim to assist disaster victims by providing information to victims who have User Devices (UDs).
- Disaster Sensor shall detect a disaster and send the disaster detection to the Service Provider.
- Equipment shall send information to the Service Provider.
- The UDs shall receive the information from the Service Provider to support the disaster victim in emergency.

- Wireless Gateway (WG) can send the information from the Service Provider to the UDs by wireless connection (e.g. Wi-Fi, 3GPP) in an emergency.

8.5.4 Pre-conditions

- In times when disasters are not present (peace time), the Equipment collects information to be used for disaster situations (emergencies). The information is maintained in the DBs on the Service Provider's Disaster Information Network.
- The Service Provider shall have reliable, secure communication with the Disaster Sensor by checking the certificate issued by the Disaster Sensor.
- When receiving information regarding a disaster from the Service Provider, the WGs shall have the method to check if the information is reliable prior to distributing the information to UDs.
- UDs shall be able to receive the message from the Disaster Sensor by the other communication paths.
- The WG may be used for the other services for specific UDs in peace time. In case of emergency, every subscribed UDs should be able to receive the message from the Service Provider through the WG.
- Communication connections among UDs, WGs and Service Provider are established.
- When the network connectivity is available, the information on DB in the Service Provider-Disaster Information Network and local DBs in the WGs should be capable of being regularly synchronized and updated.

8.5.5 Triggers

The detection of a disaster (emergency) by the disaster sensor

8.5.6 Normal Flow

Normal flow for collecting information during a disaster

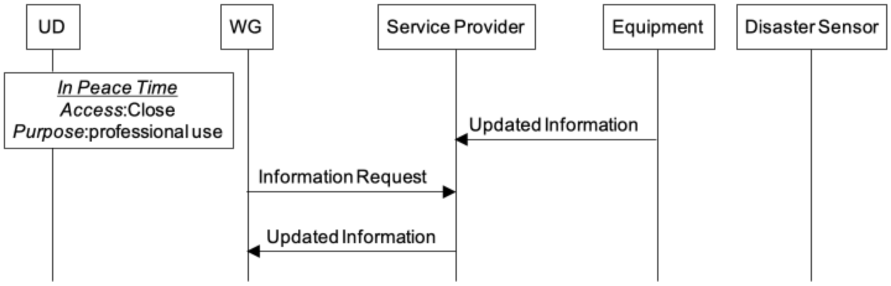


Figure 34: Figure 8.5.6-1 In Peace Time

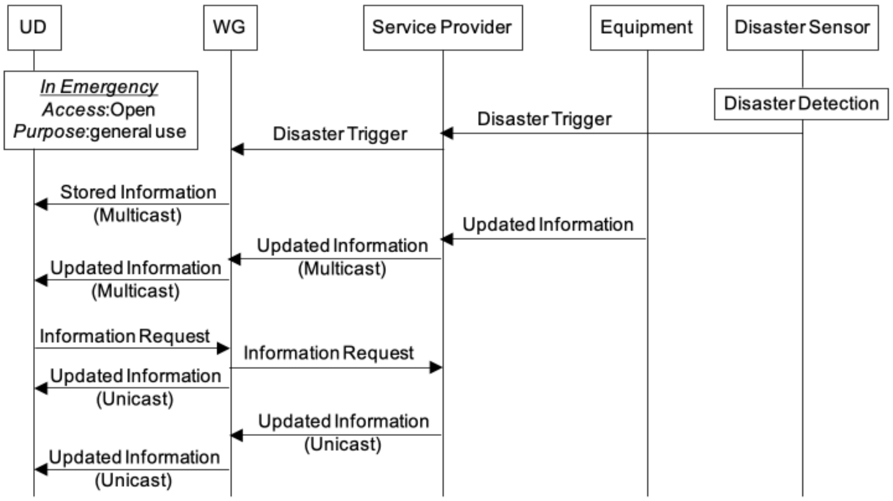


Figure 35: Figure 8.5.6-2 In emergency

13. WGs request the updated information from the Service Provider in peace time repeatedly and stores the information in their local DBs.
14. Disaster Sensors send messages to start the processing flow of the information delivery service to the Service Provider if they detect the disaster trigger.
15. The Service Provider should be able to allow every UD to access to the Databases in the WGs and Service Provider's Disaster Information Network.
16. The Service Provider sends the latest information to UDs automatically. WGs can send the stored information on the local DB to the UDs in order to suppress the network congestion.

8.5.7 Alternative Flow

UDs can request their dedicated information from WGs. When the network connectivity between the WG and Service Provider is established, WGs can request from the Service Provider the dedicated information for the UDs (e.g. family safety and their refuge area, personal medical information).

8.5.8 Post-conditions

None

8.5.9 High Level Illustration

P8.5.10 otential Requirements

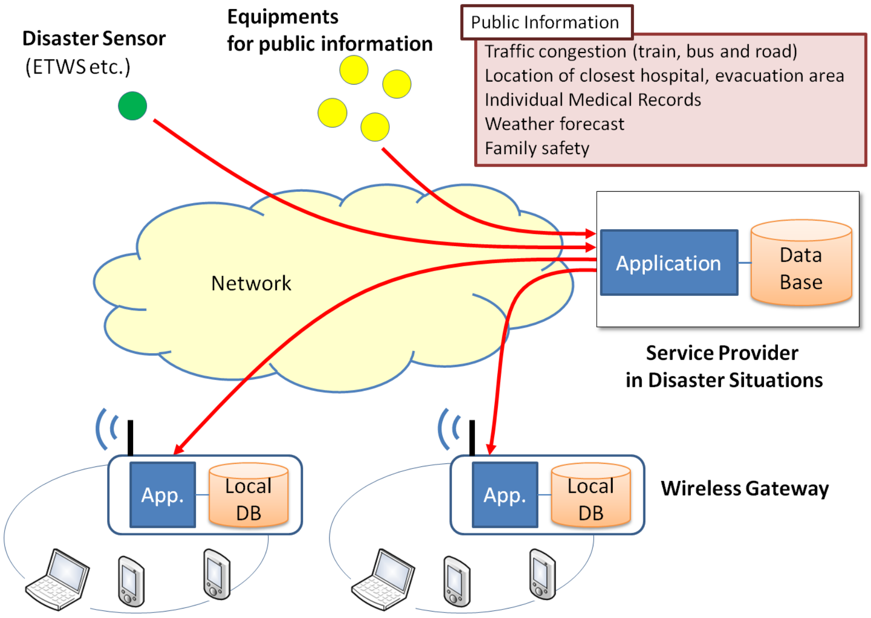


Figure 36: Figure 8.5.9-1 High Level System View

Table 4: Table 8-1 Potential Requirements

Requirement ID	Classification	Requirement Text
HLR-088-a	Data reporting	The M2M System shall provide capabilities to Applications to update/synchronize Application specific databases between the Network Application and Gateway Application. Fulfilled by HLR-041.

Requirement ID	Classification	Requirement Text
HLR-087	Data reporting	The M2M System shall support transmission of Application specific data (e.g. tsunami and earthquake detection sensor data) from Devices and oneM2M external sources (e.g. ETWS data) to Applications in the Network. Fulfilled by HLR-046.
HLR-088-b	Data storage	A (wireless) Gateway shall be able to autonomously provide Devices that are attached via the LAN of the Gateway with trusted data that is locally stored in the Gateway. Trusted data and retrieval fulfilled by HLR-041 ACLs.
HLR-088-c	Data reporting	When the WAN connection between the Gateway and Service provider is not possible, the Gateway shall continue to provide data that is locally stored on the Gateway to authorized Devices.

Requirement ID	Classification	Requirement Text
HLR-089	Data reporting	A (wireless) Gateway shall be able to transmit data (e.g. disaster warnings) to M2M Devices that are connected to the Gateway and are authorized to receive the data. Fulfilled by HLR-010.
HLR-092-a	Security	A M2M Device that receives broadcast data from a (wireless) Gateway shall be able to verify that the (wireless) Gateway is authorized to broadcast the data (e.g. disaster warnings) and that the data is authentic. Fulfilled by HLR-185 and HLR-213.
HLR-092-b	Security	The M2M System shall provide capabilities to the Service Provider to enable/disable open access of M2M Devices to the Gateway. If access of M2M Devices to the Gateway is open any M2M Device shall be allowed to receive data from the Gateway. If access of M2M Devices to the Gateway is not open only authorized M2M Devices shall be allowed to receive data from the Gateway. Fulfilled by HLR-180, HLR-201

8.6 Holistic Service Provider

8.6.1 Description

In this use case a “Holistic Service Provider” provides M2M Application services for a large building, an industry facility, a sports complex, a public infrastructure, etc. In contrast to ‘normal’ M2M Application service providers a Holistic Service Provider mainly aggregates and combines data from other M2M Application service providers of the facility, e.g. to provide analytics ore forecast services.

In this use case a Holistic Service Provider for a football stadium provides the optimal fill status of the water reservoir of the stadium, taking into account:

- Event calendar and occupancy patterns for the planned events
- Current weather conditions and forecast,
- Ticket sales,
- lawn irrigation with the target to enable a high level of rain water

The requirement for such a scenario is that M2M Application service providers can provide limited access to a subset of their M2M data to the Holistic Service Provider. In addition this needs to be done in a semi-automated way that requires minimal human involvement

8.6.2 Source

REQ-2015-0527R01

> Note: This use case has been gathered from material of the EU FP7 Project CAMPUS 21 (http://www.campus21-project.eu), in particular from Deliverable 1.1 “Analysis of Existing Business Models and Procurement Schemes” (http://www.campus21-project.eu/media/publicdeliverables/D1-1.pdf)

8.6.3 Actors

- **Holistic Management Service Provider (HM)** : A company that provides holistic management services for energy, material and resource flows for any kinds of facilities. The actor provides the synergetic analytics over all data sources within different dimensions like time, space and context, and provides decision support for advanced facility control operations. This actor cooperates with the facility operator in order to provide holistic data management and control.
  According to oneM2M terminology the **HM** is a M2M Application Service Provider
- **Facility Operator (FO)** : A company that is in charge of the operation of facility. The main focus is the main facility’s metering and control system (e.g. building automation systems) and therefore the operation of the facility in a cost- and energy-efficient manner. This actor will cooperate with third party facility services in order to enable holistic data integration.

It is in charge of the business relations for all actors active within and for the facility.
According to oneM2M terminology the **FO** is a M2M Application Service Provider
- **Third Party Facility ICT provider (TP):** A company which provides an additional sensor/ control/ metering system into the facility operated independently (installed permanently or temporarily, e.g. event ticketing system) from the main facility monitoring system. This actor might have a business relation with the facility operator, and enables access to its data.
According to oneM2M terminology the **TP** is a M2M Application Service Provider

All the above mentioned actors provide oneM2M System compliant M2M Application services.

8.6.4 Pre-conditions

- In order to provide services the Holistic Management Service Provider (HM) needs to get access to M2M data of multiple, independent Third Party Facility ICT providers (TP) in near real time. He needs to prove legitimacy of his request to access these data by some authorization of the Facility Operator (FO)
- The Facility Operator has established a business relationship with the Holistic Management Service Provider
(FO <-> HM)
- The Facility Operator has established business relationships with Third Party Facility ICT providers that provide:
    - The event calendar and ticket sales (TP for event management)
    - ticket sales solutions at the stadium
    - maintenance (temperature- and humidity control, irrigation) of the lawn of the stadium
    - maintenance (filling level, quality control, outflow- and inflow control) of the water reservoir of the stadium

  (FO <-> TP)
- Facility Operator, Holistic Management Service Provider and Third Party Facility ICT providers has established business relationships with the M2M Service Provider.
(FO, HM, TP <-> M2M-SP)

Note, there is no business relationship between the Holistic Management Service Provider and Third Party Facility ICT providers.

8.6.5 Triggers

None

8.6.6 Normal Flow

1. Offline Step:

(a) The Holistic Management Service Provider (HM) requests the Facility Operator (FO) to provide him with data read-access to event calendar, ticketing information, lawn conditions and water reservoir conditions. These data are required with a certain quality/granularity (e.g. twice a day). Moreover actuation-access to the inflow of the water reservoir is requested

(b) The Facility Operator (FO) returns a list of IDs of Third Party Facility ICT providers (TP) whose Applications provide these data

2. The Facility Operator (FO) provides the HM with an electronic token that certifies the FO's consent to allowing the HM's applications to access Third Party Facility ICT provider (TP) data.
   This consent - and the token - is restricted to only
   - The TPs and the data of these TPs that are required for the holistic service
   - The necessary quality/granularity of the data.

   The Facility Operator (FO) can at any time revoke his consent by invalidating the electronic token
3. Based on list of IDs of TPs the M2M Application of the HM discovers relevant applications of the TPs
4. The M2M Application of the HM requests read / write access to the relevant data of the TPs applications. The electronic token provided by the FO is attached to this request to prove its legitimacy.
5. Since the legitimacy of the data access request is proven through the electronic token the TP enables the data access to the HM with the necessary quality/granularity of the data.

8.6.7 Alternative flow

None

8.6.8 Post-conditions

None

8.6.9 High Level Illustration

8.6.10 Potential requirements

3. When an M2M Application (A) has access (read and/or write) to application data of another M2M Application (B) then (A) shall be able to create an electronic means - e.g. a token - that certifies the consent of (A) that a third M2M Application (C) is authorized to access these data too.

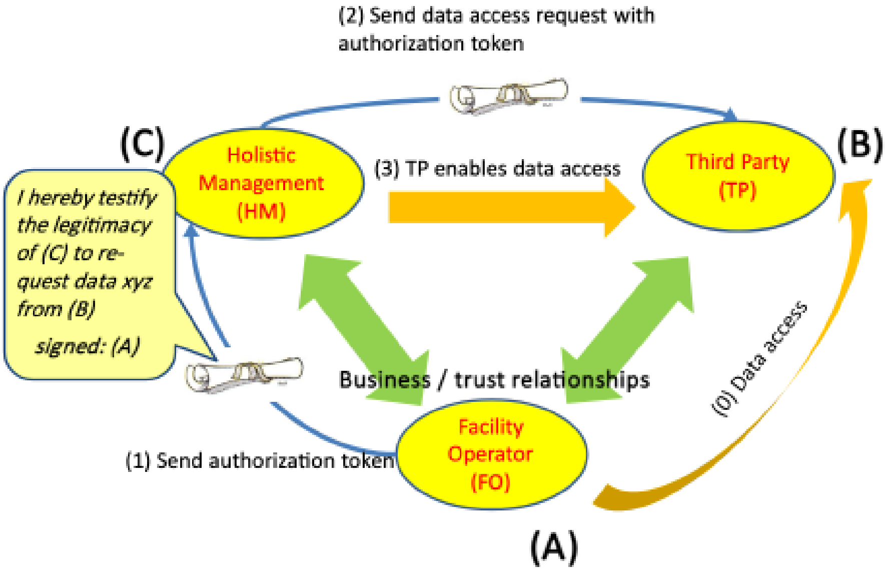

(2) Send data access request with authorization token
(C)
Holistic Management (HM)
(3) TP enables data access
Third Party (TP)
(B)
I hereby testify the legitimacy of (C) to request data xyz from (B)
signed: (A)
Business / trust relationships
(0) Data access
(1) Send authorization token
Facility Operator (FO)
(A)

Figure 37: Figure 8.6.9-1 Holistic Service Provider High Level Illustration

4. The M2M Application (A) shall be able to provide a third M2M Application (C) with this authorization token.
5. The M2M Application (A) shall be able to restrict the consent expressed in the authorization token to specify:
   - the authorized M2M Application (C)
   - the data accessed from a specified M2M Application (B)
   - the type of data access (read and/or write) and time when (how often) data can be accessed.
   - in case of subscription to the data the time granularity of providing data updates
6. An M2M Application (B) shall be able to receive a request to access its data from an M2M Application (C) together with an authorization token that certifies the consent of M2M Application (A) that (C) has been authorized by (A) to access these data.
7. The M2M Application (A) that had issued the authorization token shall be able to revoke the authorization token.
8. When an authorization token has been revoked, then any M2M Application (B) that had granted access to its data based on the presence of this authorization token shall receive notification by the M2M System that the authorization token has been revoked.

8.7 Resource reservation for public services

8.7.1 Description

In a Smart City environment, a central management coordinator interacts with hundreds of devices and vehicles owned and operated by different stakeholders: public service managers and end-user applications, traffic and transportation apps from local companies, stakeholders and users, vehicles and sensors from municipality, universities, etc. Some devices, such as those for public services, allow the central coordinator access to specific resources hosted locally on the device, with access control managed at the device level. In an emergency or special event situation the coordinator needs uninterrupted access (albeit for short periods of time) to specific resources on all these devices, and for their state to be unchanged by other entities. For example, reservation 1 (see Figure 8.7.9-1) will be needed temporarily for shuttles and traffic lights in a specific area, in order to coordinate traffic when emergency public works are performed. Another reservation (2) is needed for resources on end-user's mobile devices to allow for updates with critical event information while temporarily blocking changes, for example, from the bus system.

The usecase requires that entities (such as the management applications) can reserve oneM2M resources on their own behalf or others', including groups of applications, etc. Such actions normally require changes in the ACPs resources in many devices, where the ACPs are distinct from each other. Changing ACPs requires individual RESTful operations to be performed for each change, with a large messaging overhead.

This usecase requires a more dynamic procedure. Pre-provisioned policies for reservation (for the security of the system) are used to enable reservations via simple/dynamic requests such as: "allow THIS specific Originator (which already has privileges in all these heterogeneous and distributed ACPs"), to reserve the resource temporarily, with the existing privileges".

NOTE: In this context, a reservation is a service by the Host of one or more oneM2M resources for a limited time. During the reservation, RESTful requests from some entities (i.e. Privileged Entities) and targeting the reserved oneM2M resources are treated preferentially e.g. may be the only ones to be executed against the reserved resource. At the same time, RESTful requests from other entities (i.e. Non-Privileged Entities) and targeting the reserved oneM2M resources are barred or de-prioritized. A reservation instance is characterized by specific conditions, scope and rules based on which the requests received during a reservation (from either Privileged or Non-Privileged Entities) are processed.

8.7.2 Source

REQ-2018-0061R02 Resource reservation for public services

8.7.3 Actors

- Originator: It is the entity that requests a reservation of resources, either in its own behalf or on behalf of other entities, termed privileged entities (for the duration of the reservation).
- Host: Entity hosting resources and providing services using reservation mechanisms.
- Privileged Entity: Originator of requests targeting the reserved resources at the Host, requests which are granted during a reservation on its behalf.
- Non-Privileged Entity: Originator of requests targeting the reserved resources at the Host, requests which are barred during a reservation

8.7.4 Pre-conditions

- Reservation Policies are created along with Access Control Policies.
- Access Control Policies are enforced at all times.

8.7.5 Triggers

None

8.7.6 Normal Flow

The flow in Figure 8.7.6-1 distinguishes the following steps:

0. Reservation setup: During this step the target resource Host is enabled to provide services using (or based on) reservations by being provided with Reservation Policy information.
1. Reservation request/triggering: During this step a Reservation Instance is created or triggered.
   There may be several types of reservation requests, depending on triggering methods:
   - a. Explicit: A reservation requester provides directly all the reservation information that allows the Host to enforce the reservation of oneM2M resources (on behalf of the requester or another privileged entity)
   - b. Request-based/ Implicit: A RESTful request is used to trigger a reservation, with reservation parameters (scope) provided implicitly, i.e. determined by the Host based on the local information.
   - c. Event-based/ Implicit: A specific event monitored by the Host triggers the reservation, with reservation parameters (scope) provided implicitly, i.e. determined by the Host based on the local information
2. Reservation authorization and creation
   This step is closely linked to the triggering procedure in that the reservation request received is authorized based on the information available at the Host from the setup phase (Reservation Policy). If authorized, it results

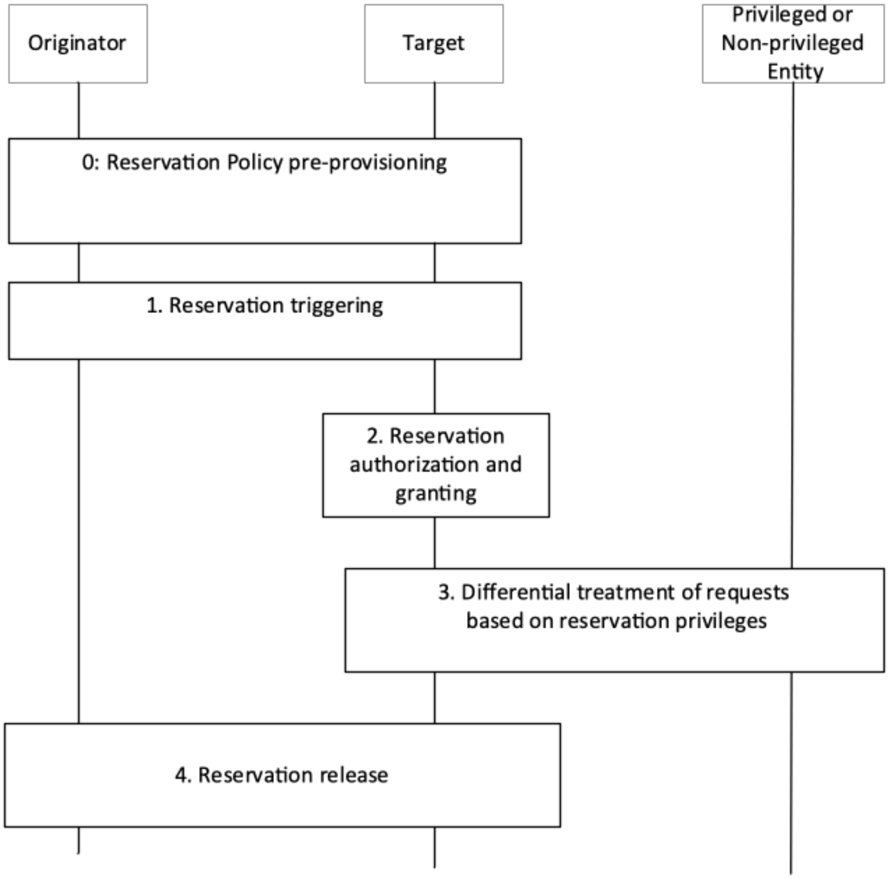

Originator
Target
Privileged or Non-privileged Entity
0: Reservation Policy pre-provisioning
1. Reservation triggering
2. Reservation authorization and granting
3. Differential treatment of requests based on reservation privileges
4. Reservation release

Figure 38: Figure 8.7.6-1 Resource Reservation flow

in a new Reservation Instance being created. The parameters (scope) of the Reservation Instance are based on the Reservation Policy as well as information included in step 1.

3. Management of external requests during reservations:
    - a. From privileged entities
    - b. From non-privileged entities

   During the reservation the Host processes requests based on the reservation rules. The processing of Privileged Requests is different than the processing of Non-Privileged Requests.
4. Reservation stop or release:
   This step is also closely linked to the triggering procedure in that the method for reservation stop or release depends on the triggering method. Differential processing of incoming requests ceases.

8.7.7 Alternative Flow

None

8.7.8 Post-conditions

None

8.7.9 High Level Illustration

8.7.10 Potential requirements

1. The oneM2M System shall support the provisioning and management of policies governing the use of resource reservation mechanisms, including: authorizing resource reservation requests, constraining resource reservation parameters (e.g. maximum reservation duration, maximum aggregated reservation duration, maximum number of resources reserved, maximum number of consecutive reservations granted, etc.)
2. The oneM2M System shall support mechanisms for time-limited reservation of resources at resource hosts, based on pre-provisioned resource reservation policies and reservation requests, subject to access control.

8.8 Manhole Cover Monitoring

8.8.1 Description

Manholes leading to underground supply systems are essential for their maintenance. Without these modern infrastructures our daily life as well as the economic system would collapse. In particular, this concerns: telecommunications networks, water supply networks, gas supply networks and electricity networks. This makes these systems vulnerable to sabotage and terror attacks. Every unsecured manhole represents an easy potential target. In supply networks a very small action at a single point can inflict a huge amount of damage to property and people.

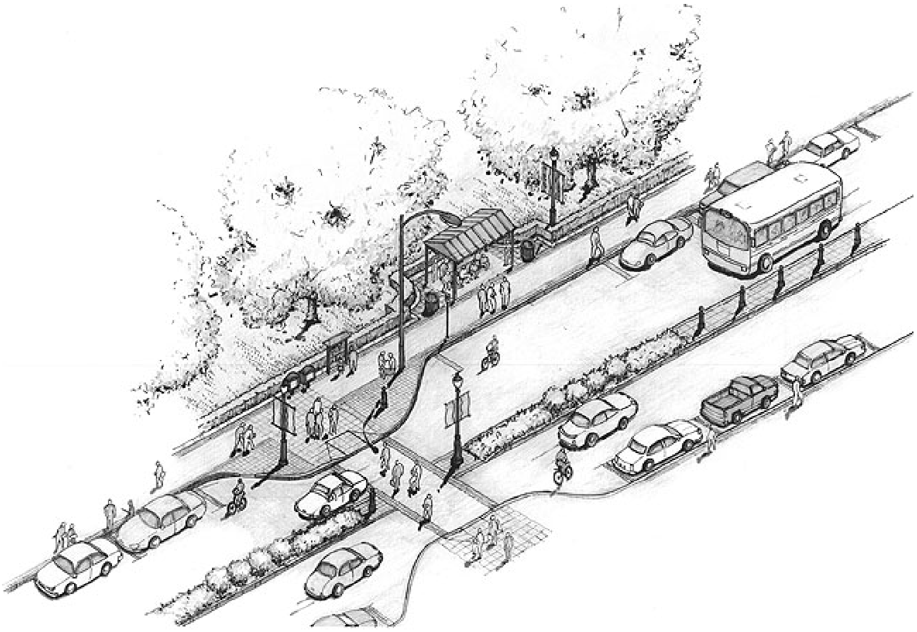


Figure 39: Figure 8.7.9-1 Resource Reservation for Public Services

In smart city, there are many sensors which are used to monitor the manholes cover. The Manhole Monitor sends alarms in real-time and it communicates status information daily whenever a manhole cover is opened or lifted. This can be used to alert the authorities and locate which manhole has been lifted immediately.

8.8.2 Source

REQ-2018-0093R01 - Use case for Manhole Cover Monitoring

8.8.3 Actors

- Manhole Cover Monitoring Device: function to detect if the manhole cover has been moved.
- Manage Server: function to monitor if the manhole cover has been moved.
- Street Authority Application: function to receive the manhole cover event and initiate event task.
- District Authority Application: function to receive the manhole cover event and monitor if the Street Authority has completed event task.

8.8.4 Pre-conditions

Street manager has the ability to subscribe to the Manhole Cover related event.

Street manager and district manager has the ability to receive the Manhole Cover related event notification.

8.8.5 Triggers

None

8.8.6 Normal Flow

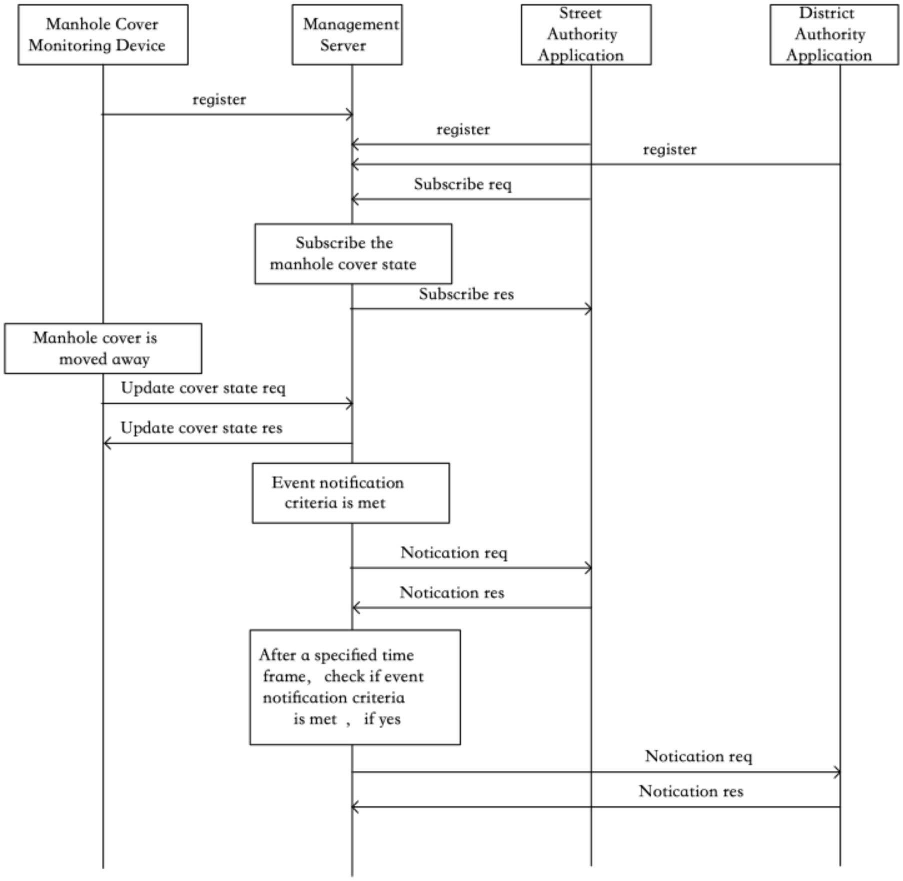

Manhole Cover Monitoring Device
Management Server
Street Authority Application
District Authority Application
register
register
register
Subscribe req
Subscribe the manhole cover state
Subscribe res
Manhole cover is moved away
Update cover state req
Update cover state res
Event notification criteria is met
Notication req
Notication res
After a specified time frame, check if event notification criteria is met , if yes
Notication req
Notication res

Figure 40: Figure 8.8.6-1 Normal flow for monitoring services

1. Manhole Cover Monitoring Device, Street Authority and District Authority register to the Management Server;
2. The Street Authority subscribe to the Manhole Cover Monitoring Device event notifications, where notification receiver includes the Street Authority and District Authority;

3. When the Manhole Cover is moved from stored/closed position, the Manhole Cover Monitoring Device updates the state of Manhole Cover in the Management Server;
4. The Management Server decides that a Manhole Cover event occurred based on the event notification criteria;
5. The Management Server sends event notification to the Street Authority immediately;
6. After a specified time frame, a check occurs, determining if the event notification criteria is met; if yes, the Management Server sends the notification to the District Authority Application.
7. The Management Server receives the notification response from the District Authority Application.

8.8.7 Alternative flow

None

8.8.8 Post-conditions

None

8.8.9 High Level Illustration

8.8.10 Potential requirements

1. The oneM2M system shall support deferred notification for a specified time frame.
2. The oneM2M system shall support sending deferred notifications if based on event notification criteria (e.g. is met after the specified time frame).

9 Residential Use Cases

9.1 Home Energy Management

9.1.1 Description

This use case is to manage energy consumption at home so that consumers can be aware of their daily home energy consumptions and able to control this consumption by remote actions on home appliances. Innovative services can be developed from the data (energy) collection and sent to either the consumers/ equipment or to Business-to-Business market.

The use case focuses on a home Energy Gateway (EGW) that collects energy information from the electrical home network and communicates it to an M2M system for aggregating and processing of the data. Services can then be developed from the collected data.

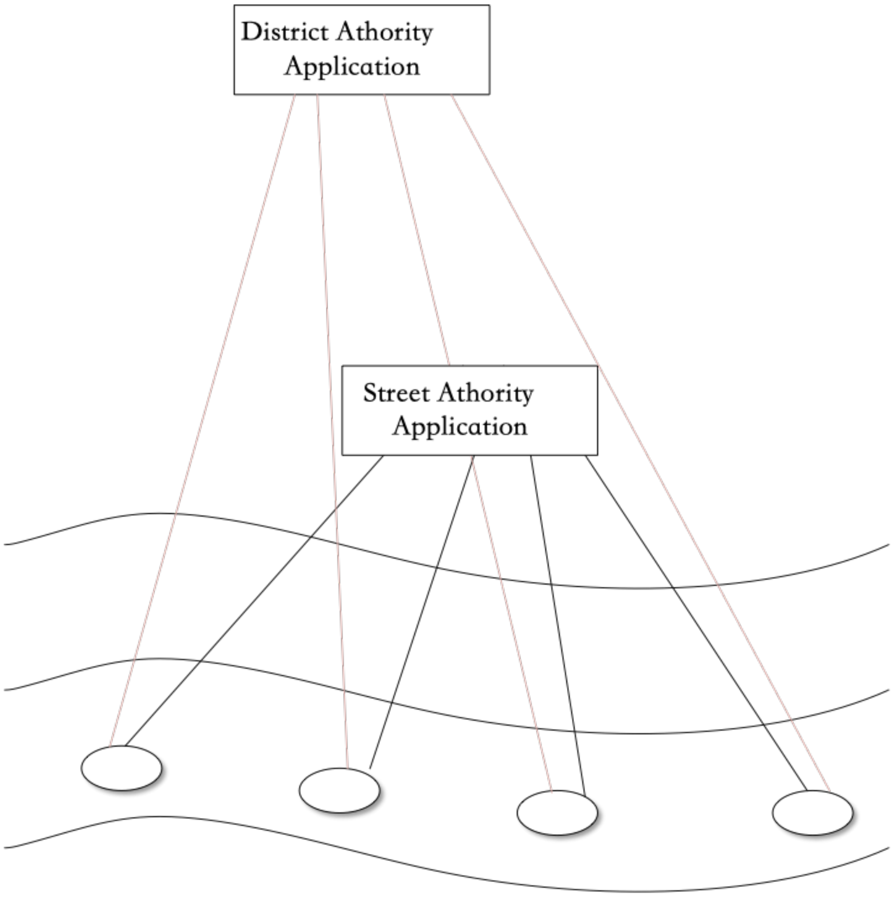


Figure 41: Figure 8.8.9-1 High level illustration for monitoring services

The EGW performs an initial treatment of the data received from various sources (sensors, context) as follows:

- aggregating and processing the obtained information:
- sending some information to the remote M2M system e.g. sending alerts through the M2M system
- using some information locally for immediate activation of some actuators/appliances
- Is connected (wirelessly or via wireline) to home devices, including the home electrical meter, for information on global or individual consumption of the appliances
- Providing displayable consumed energy-related information to the end-user/consumer terminals (PC, mobile phone, tablet, TV screen, etc.)

Ref:[i.6] {HGI-GD017-R3, Use Cases and Architecture for a Home Energy Management Service}

9.1.2 Source

oneM2M-REQ-2012-0058R03 Home Energy Management

Note: from [i.2] ETSI TR 102 935 v2.1.1

9.1.3 Actors

- User: user of home appliance
- Communication operators: in charge of communicating the collected information via any protocol (e.g. ZigBee, PLC, Bluetooth 4.0 . . .) to EGW and from the EGW to the M2M system
- Energy gateway SP: in charge of collecting & transmitting securely energy information from appliances to the M2M system and receiving remote controls/commands from the M2M system
- System operators/providers of service layer platform(s): in charge of providing services/common functionalities for applications (e.g. HEM) that are independent of the underlying network(s); e.g. they are in charge of collecting the status information of home devices and controlling them via the energy gateway.
- Application Service Provider: Provides Home Energy Management (HEM) Application for the user through the M2M system

9.1.4 Pre-conditions

None

9.1.5 Triggers

None

9.1.6 Normal Flow

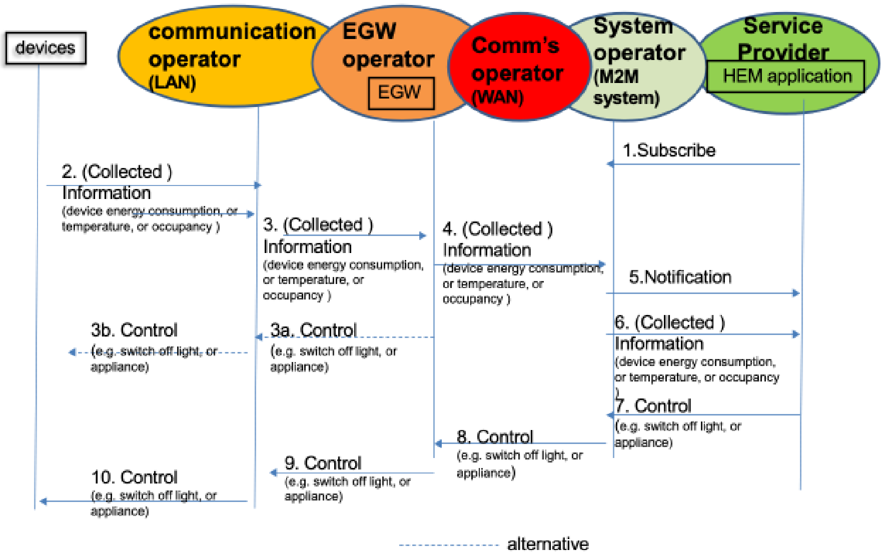

devices
communication operator (LAN)
EGW operator
EGW
Comm's operator (WAN)
System operator (M2M system)
Service Provider
HEM application
1.Subscribe
2. (Collected) Information
(device energy consumption, or temperature, or occupancy)
3. (Collected) Information
(device energy consumption, or temperature, or occupancy)
4. (Collected) Information
(device energy consumption, or temperature, or occupancy)
5.Notification
6. (Collected) Information
(device energy consumption, or temperature, or occupancy)
3b. Control
(e.g. switch off light, or appliance)
3a. Control
(e.g. switch off light, or appliance)
7. Control
(e.g. switch off light, or appliance)
8. Control
(e.g. switch off light, or appliance)
9. Control
(e.g. switch off light, or appliance)
10. Control
(e.g. switch off light, or appliance)
alternative

Figure 42: Figure 9.1.6-1 Home Energy Management Normal Flow

1. HEM application (M2M device) subscribe to System Operator/SP for information from home device(s).
2. Information from devices which could be M2M devices (smart meters, electric lightening, fridge, washing machine etc.) at home is collected by the Energy Gateway Operator (EGW) via communication network operator. . Information may include room, temperature, occupancy, energy consumption.
3. Collected information is stored in the EGW SP and may be processed at energy gateway. As a result, control message may be sent back to device from the energy GW depending on policies stored in the energy gateway.
4. Collected information may also be sent to system operator which contains the M2M service platform for storage via communication network.
5. Subscribed application (HEM) is notified information is available for processing. Its subscribe M2M operator can process the information before sending to HEM application depending on subscription profile.
6. HEM application reacts to the shared /collected information and can send control message (e.g. To switch a home device e.g. light /appliance or washing machine) via the system operator.
7. Control is propagated back through different operator to appropriate M2M device(s).

9.1.7 Alternative Flow

None

9.1.8 Post-conditions

None

9.1.9 High Level Illustration

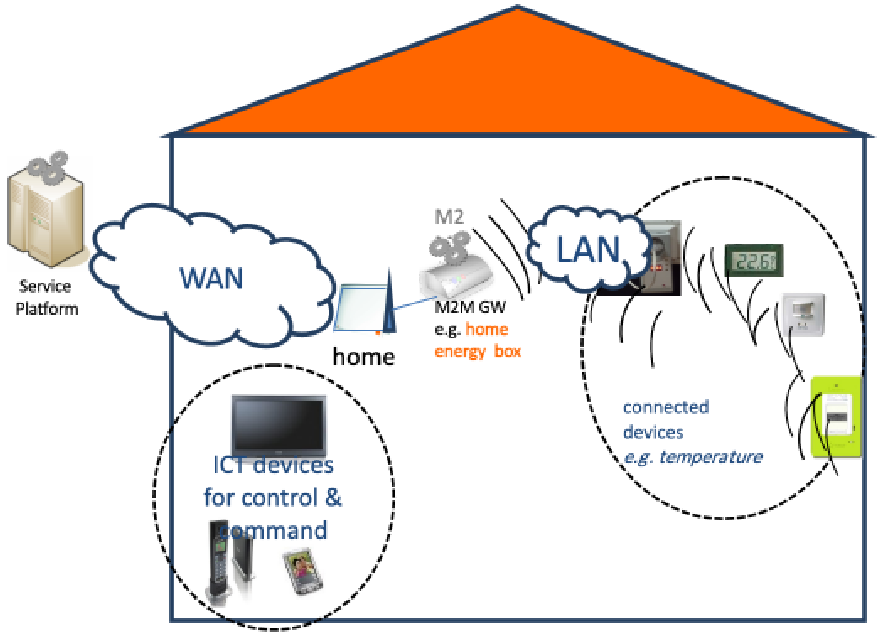


Figure 43: Figure 9.1.9-1 Home Energy Management System High Level Illustration

9.1.10 Potential Requirements

1. Similar to that of WAMS use case summarized as follows:
   - a. Data collection and reporting capability/function
   - b. Remote control of M2M Devices
   - c. Information collection & delivery to multiple applications
   - d. Data store and share
   - e. Authentication of M2M system with M2M devices/ /collectors
   - f. Authentication of M2M devices with M2M applications
   - g. Data integrity
   - h. Prevention of abuse of network connection

- i. Privacy
- j. Security credential and software upgrade at the Application level.
- k. In addition the following requirements are needed:
- l. The M2M system shall support a Gateway
- m. The Gateway can be per home or per multiple homes e.g. a Gateway Concentrator.

2. Configuration Management
3. Pre provisioning of the M2M Devices and Gateways:
    - a. The M2M System shall support mechanisms to perform simple and scalable pre provisioning of M2M Devices/Gateways.
4. Management of multiple M2M Devices/Gateways
    - a. The M2M Application e.g. the HEM application shall be able to interact with one or multiple M2M Devices/Gateways, e.g. for information collection, control, either directly or through using M2M Service Capabilities.
    - b. The HEM application shall be able to share anonymous data with energy partners to provide the consumer with special energy rates.
5. Support for subscribing to receive notification:
    - a. The M2M System shall support a mechanism for allowing applications to subscribe and being notified of changes.
    - b. The M2M System operator shall be is able to support subscription of the HEM application to subscribe.
6. Support for optimizing notification:
   The M2M System shall be able to may support a mechanism for delaying notification of Connected Devices in the case of a congested communication network.
7. Support for store and forward
    - a. The M2M System shall be able to support a mechanism to manage a remote access of information from other Connected Devices. When supported the M2M system shall be able to aggregate requests and delay to perform the request depending on a given delay and/or category e.g. the M2M application does not have to connect in real time with the devices.

9.2 Home Energy Management System (HEMS)

9.2.1 Description

This use case introduces several services based on HEMS technologies.

Home appliances from multiple vendors are connected to a LAN or PAN, and controlled by the gateway device.

The gateway device aggregates functionalities of home appliances by getting their status and sending this to the management server.

The gateway device is also upgradable to host newly released home appliance(s).

The gateway device provides an API for remote control which takes privacy and authorization issues into account.

9.2.2 Source

oneM2M-REQ-2012-0072R05 Use Case Home Energy Management System (HEMS)

9.2.3 Actors

```
- User: user (owner) of the home appliances
- Home Appliance: appliances which may be from multiple vendors and are monitored and/or con
- Gateway Device: a device installed in the user's home and receives remote control commands
- Management Server: the server which is in charge of collecting the status of appliances an
- HEMS Application Server: the server which provides HEMS service for the user through the r
```

9.2.4 Pre-conditions

```
- WAN connectivity to the Gateway Device is installed
- Service contract is required, and authentication credentials for the Management Service an
```

9.2.5 Triggers

New Air Conditioner (for example) is installed

9.2.6 Normal Flow

1. User operates the Gateway Device to identify newly installed Air Conditioner (A/C) on the LAN.
2. The newly installed A/C is identified by the Gateway Device.
3. The Gateway Device requests the Management Server to provide support software for the A/C.
4. The support software is installed on the Gateway Device.
5. The Gateway Device registers the functionalities of the A/C to the Management Server.
6. The Management Server notifies the event of the installation of the A/C to the HEMS Application Server.
7. The HEMS Application Server is reconfigured with the newly installed A/C.
8. The HEMS Application Server receives the latest status of all of the Home Appliances including the newly installed A/C from the Management Server.
9. The HEMS Application Server sends management command(s) to the Management Server to minimize energy consumption.

9.2.7 Alternative Flow

None

9.2.8 Post-conditions

Energy consumption within the home is minimized by monitoring and controlling Home Appliances.

9.2.9 High Level Illustration

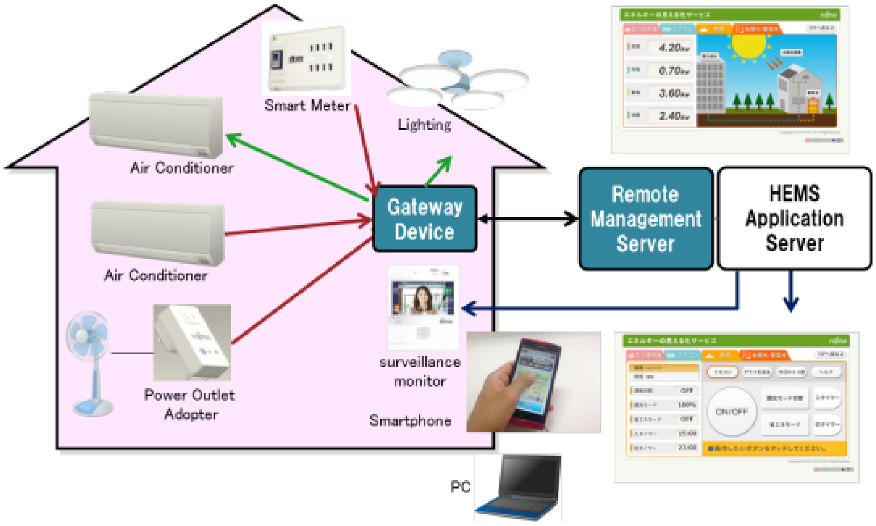


Figure 44: Figure 9.2.9-1 Home Energy Management System High Level Illustration

9.2.10 Potential Requirements

1. Gateway Device shall have the following requirements.
2. To detect the newly installed Home Appliance.
3. To be provided with appropriate pre provisioning configuration which is required to host the Home Appliances?
4. To support Home Appliances from multiple vendors as an abstracted object model.
5. To allow control to be overridden of the Home Appliances by User's direct operation.

9.3 Plug-In Electrical Charging Vehicles and power feed in home scenario

9.3.1 Description

The aim of the Plug-In Electric Vehicle (PEV) Charging and Power feed use case is to show the interaction between the different actors that can be involved in the charging of Electric Vehicle in home scenario. The scenario includes engagement of various actors:

- Electricity-Network Service Provider (Electricity-N/W-SP),
- Dedicated Electric Vehicle Charging SP (EVC-SP) who takes care of special functions like the Demand Response (DR) enablement (cost effective PEV Charging and Power Feed),
- PEV-SP in charge of functions related to PEV service and maintenance (providing a data connection for PEV health purposes such as managing Power Feed cycles, PEV-SW upgrading & remote fault analysis, etc.)
- PEV manufacturer in charge of replacing faulty parts for the PEV

PEV can be considered as a load and also as power storage (DER resource). In the latter case, a Power Feed from the PEV's battery into the Electricity-N/W is required.

The Electricity-N/W-SP is responsible for the residential homes (smart) metering. Depending on local laws, the metering for the (Electrical Vehicle Charging Equipment) EVCE may be independent and might be a physical part of the EVCE.

Depending on the PEV's brand, a parallel wired data connection may be included in the EVCE charging plug to enable the PEV's controller to access its agreed service and maintenance provider (PEV-SP). In case of no wired connection (high data rate, e.g. Ethernet), a short reach link, e.g. via ZigBee® or even Bluetooth® may be established (medium data rate ~2 Mb/s). This connection will then be routed via the EVCE's mobile broadband link to the PEV-SP's control centre in parallel to the charging and power feed control data, which is routed to the EVC-SP's control centre.

Related Standard activities:

- TC 69 committee: working on [i.7] ISO/ IEC 15118 parts 1-4, vehicle to grid communication; currently under development EU standardisation Mandate 486 to CEN, CENELEC and ETSI (for further information refer to [i.8] Mandate 486)
- Open 2G: using [i.9] DIN specification 70121 and [i.7] IEC 15118
- DIN specification [i.9] 70121 defines the requirements for the communications between the electric vehicle (EV) and the charging EVCE).

9.3.2 Source

oneM2M-REQ-2012-0059R02 Plug-In Electric Vehicle Charging (PEV)

Note: from [i.2] ETSI TR 102 935 v2.1.1

9.3.3 Actors

- Electricity Network service provider (Electricity N/W-SP/DSO) is responsible for the residential homes smart metering.
- Electricity vehicle charging service provider (EVC-SP) takes care of special functions like the Demand Response (DR) enablement (cost effective PEV Charging and Power Feed)
- PEV service provider (PEV SP) offering functions in conjunction with PEV service and maintenance (PEV health check and management such as management of power feed cycles, PEV-SW upgrading & remote fault analysis, etc.)
- Communication operator /provider provide the public wireless data service to PEV-SP and EVC SP control centres.

9.3.4 Pre-conditions

Connection from PEV to EVCE through a wired EVCE plug (data communication) or wirelessly (ZigBee or Bluetooth) or any short range technology.

Public communication network from EVCE to PEV SP and EVCE SP control centres.

Public communication between EVCE metering and El. N/W SP

9.3.5 Triggers

Control and pricing announcements from El. N/W SP to for example balance the power N/W

Control and pricing trigger/initiate PEV being charged at a particular time with a specific power feed cycle that is appropriate for consumer (cheaper) and for El. N/W SP (balance power system).

PEV health management through PEV control link to EVCE

e.g. PEV SP initiates health check when PEV is plugged into EVCE for charging; if there is a problem detected or a PEV part status is over a certain limit, this will trigger a corrective measure according to health check result (e.g. PEV SP place an order for a part replacement to PEV manufacturer, or SW upgrade, etc.)

EVCE SP will control and manage EVCE through EVCE control link;

9.3.6 Normal Flow

An example flow to show the interaction between PEV SP (PEV health check), PEV manufacturer (PEV defect part replacement) and EVC SP (metering/charging):

- Red colour to refer to flow related to EVC charging application
- Green colour refer to flow related to PEV SP application
- Blue colour refer to flow related to PEV manufacturer application

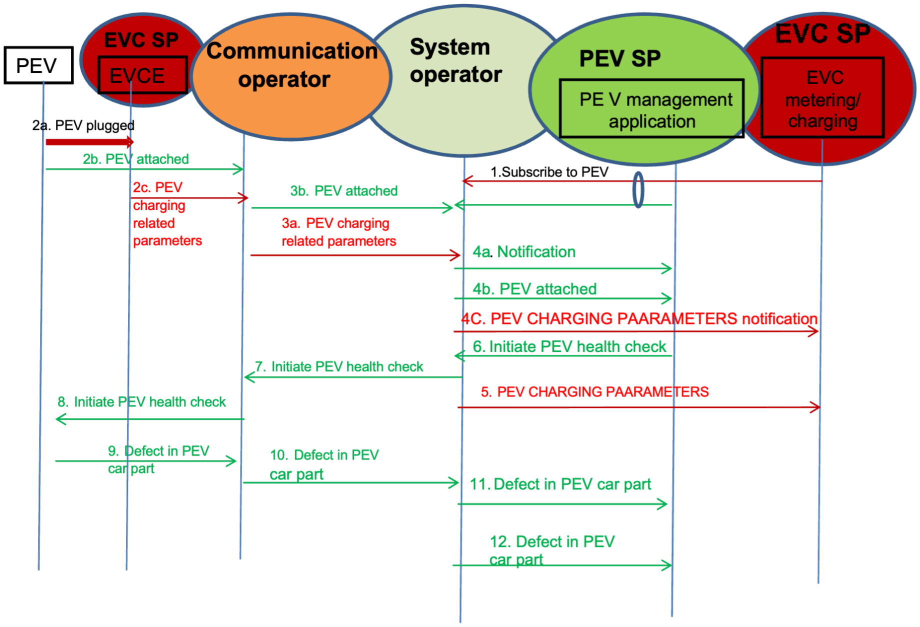

PEV
EVC SP
EVCE
Communication operator
System operator
PEV SP
PE V management application
EVC SP
EVC metering/ charging
2a. PEV plugged
2b. PEV attached
2c. PEV charging related parameters
3b. PEV attached
3a. PEV charging related parameters
1.Subscribe to PEV
4a. Notification
4b. PEV attached
4C. PEV CHARGING PAARAMETERS notification
6. Initiate PEV health check
7. Initiate PEV health check
5. PEV CHARGING PAARAMETERS
8. Initiate PEV health check
9. Defect in PEV car part
10. Defect in PEV car part
11. Defect in PEV car part
12. Defect in PEV car part

Figure 45: Figure 9.3.6-1 PEV Normal Flow

- 1) PEV management application and EVC metering/charging application subscribe to information related to PEV.
- 2)
  - 2a) PEV is plugged to EVCE
  - 2b) PEV related information (e.g. PEV1) is sent to communication operator
  - 2c) PEV charging related information (e.g. .charging period)
- 3) Information sent in step 2 are sent to system operator which trigger the notification in step 4
- 4) Notifications are sent to the subscribed applications.
- 5) PEV charging parameters pulled/pushed to the EVC-SP
- 6) PEV management application sent an initiation of health check message to system operator
- 7) Initiation message is sent by system operator through communication operator to PEV to start the health check

- 8.) - 9) A PEV part defect is detected and a message is sent to the system operator, which triggers the notification of the PEV SP
- 10) System operator is sent a defect Notification to PEV SP application of the car part.
- 11) Which in turn send an order of the defected part to system operator
- 12) System operator sends the order to a PEV manufacturer

9.3.7 Alternative Flow

None

9.3.8 Post-conditions

None

9.3.9 High Level Illustration

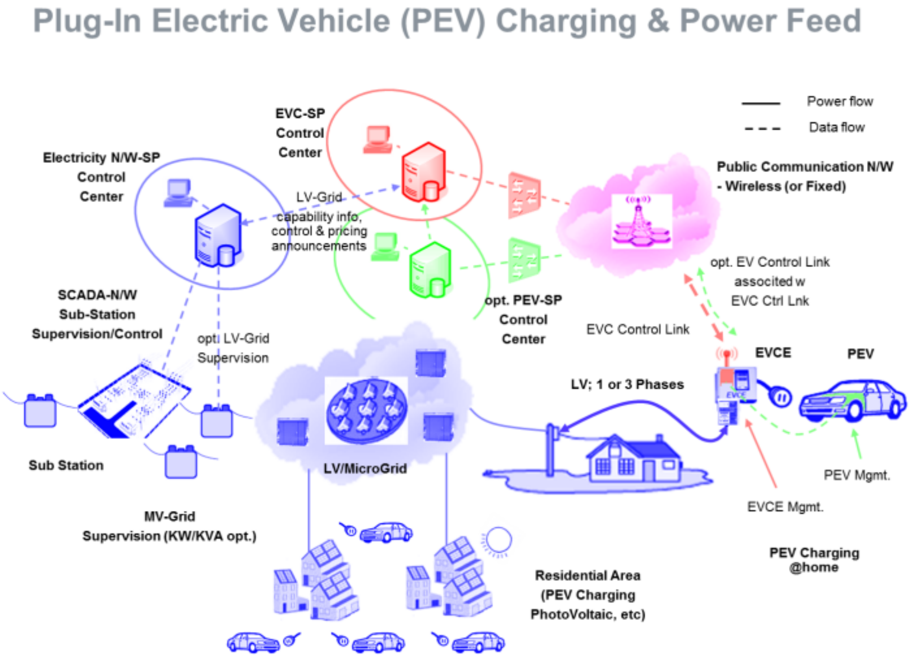

Plug-In Electric Vehicle (PEV) Charging & Power Feed
Power flow
Data flow
EVC-SP Control Center
Electricity N/W-SP Control Center
Public Communication N/W - Wireless (or Fixed)
LV-Grid capability info, control & pricing announcements
opt. EV Control Link associted w EVC Ctrl Lnk
SCADA-N/W Sub-Station Supervision/Control
opt. LV-Grid Supervision
opt. PEV-SP Control Center
EVC Control Link
EVCE
PEV
LV; 1 or 3 Phases
Sub Station
LV/MicroGrid
PEV Mgmt.
EVCE Mgmt.
MV-Grid Supervision (KW/KVA opt.)
PEV Charging @home
Residential Area (PEV Charging PhotoVoltaic, etc)

Figure 46: Figure 9.3.9-1 PEV Charging High Level Illustration

9.3.10 Potential Requirements

1. Secure communication of the following transactions:

   - i. SW upgrade by PEV manufacturer,
   - ii. Collecting PEV status info for health check will trigger control or command (e.g. order new part, trigger to do a car service) to another SP
   - iii. Collecting charging information (metering) from EVCE i.e. power feed cycle and time and charging period to the EVC-SP control centre (the metering could be home owned smart meter or Utility owned)
   - iv. Collection metering info from EVCE (PEV considered as a load or resource), to Electric N/W provider for billing purposes. Controlling EVCE e.g. SW upgrade, part order
   - v. Pricing info from Electricity Network SP to EVC SP
   - vi. Fleet management control centre to collect location information of PEV
2. Potential requirements are similar to those of WAMS:
   - i. Data collection and reporting capability/function including data delivery to multiple applications
   - ii. Remote control of M2M Devices
   - iii. Data store and share
   - iv. Authentication of M2M system with M2M devices/ /collectors
   - v. Authentication of M2M devices with M2M applications
   - vi. Data integrity
   - vii. Prevention of abuse of network connection
   - viii. Privacy
   - ix. Security credential and software upgrade at the Application level.

9.4 Real-time Audio/Video Communication

9.4.1 Description

So far, session control and Real-time audio/video communication are taken as basic capabilities in H2H telecom network. People may think that device does not need to listen or watch something from elsewhere except itself, thus there is no need for M2M system to support such kinds of human oriented capabilities, however, this is not the case. The following are some use cases in which session control for real-time audio/video communication is needed.

Use Case 1: Home Surveillance

One person, when travelling far from home, would like to use the application installed on his/her cell phone or pad computer to monitor his/her house, via the cameras fixed inside or outside his/her house. In the case the person makes a call to the camera through his/her cell phone or pad computer requesting for image/video transmission, the camera can answer the call request and automatically start transmission of images/video captured by the camera.

The camera may be able to initiate an audio/video call or send messages for alarm addressing to the cell phone of the person in the case there are abnormal images captured by the camera, e.g. the image changes or the camera are moved. The cameras can communicate with other M2M devices via wired or wireless network. The communication can be between the M2M application on the M2M device and the M2M application applied in a service centre which provides home surveillance service to the users.

In order to have a clearer look at the images captured by the cameras, some commands can be sent to the camera to adjust some parameters on the cameras, e.g. tilt, zoom in/out, adjust the focus, initiate recording, and so on. For easy and better control of the camera along with the video transmission, the commands can be transported within the same session as for video transmission. It is assumed that standalone session can be created to control the cameras as well.

The cell phone can also start calling the camera automatically according to some predefined rules. For example, the cell phone calls the camera and records the audio/video information automatically every night while the owner is sleeping.

Use Case 2: Doorbell Controller

One person, when he/she is away from home, his/her children or parents may forget to take the keys and lock them from entering into the house. After they push the door bell or door controller with cameras equipped, the application installed on the door bell or door controller may initiate a video call to the person's cell phone in which it shows who are standing before the door, and once the user answers the call reaching his/her cell phone, the door will open.

Also, when the motion detector equipped near the doorbell detects some abnormal movements near the door, the motion detector notifies the doorbell with a camera to start a call to the owner's cell phone. When the owner answers the phone, he/she will be able to make sure if the movements are normal.

Use Case 3: Customized Home Service

One person, when he/she is away from home, he/her may use his/her mobile device to coordinate appointments using calendar application or to search information on internet. His/her mobile device also can trace its location using GPS. By collecting the information, his/her life pattern/context and interests can be analysed.

Using well-analysed information, a service provider can provide user- customized home service with home appliances which have capability of showing video or playing audio like smart television or smart refrigerator.

He/she may come back to home and turn on TV. Channels would be recommended based on analysed data of his/her preference. Then commercial advertisement on TV would be shown regarding of his/her interest and personal information.

9.4.2 Source

oneM2M-REQ-2013-0281R02 Use Case real time audio video communication

oneM2M-REQ-2013-0398R01 Use Case of Additional audio video

9.4.3 Actors

- M2M Service Provider:
  A company that provides M2M service including one or more of the entities e.g. devices with camera, oneM2M platform and service centre for surveillance and alarm reaction.
- Service Centre:
  The service centre provides home surveillance and other corresponding services, e.g. initiating an audio/video call to the host of the home in case there are intruders or initiating a multimedia conference call for consultation for a patient.

9.4.4 Pre-conditions

Before the audio/video call could be set up, the following steps are to be taken:

- The Devices are configured with the number/address to which an audio/video call can be initiated for alarm
- The oneM2M system allocates unique identifiers for the devices
- The devices need to be registered in the oneM2M system

9.4.5 Triggers

None

9.4.6 Normal Flow

1. The device registers in oneM2M system.
2. When receiving request towards or from the device for an audio/video call, the oneM2M system authorizes if the originator is allowed to send the request.
3. If it is allowed, the oneM2M system route the message accordingly and create a connection between the originator and the receiver for real-time audio and video transfer, and even commands for camera control.
4. After the communication is completed, the oneM2M system releases the connection and resources.

9.4.7 Alternative Flow

None

9.4.8 Post-conditions

None

9.4.9 High Level Illustration

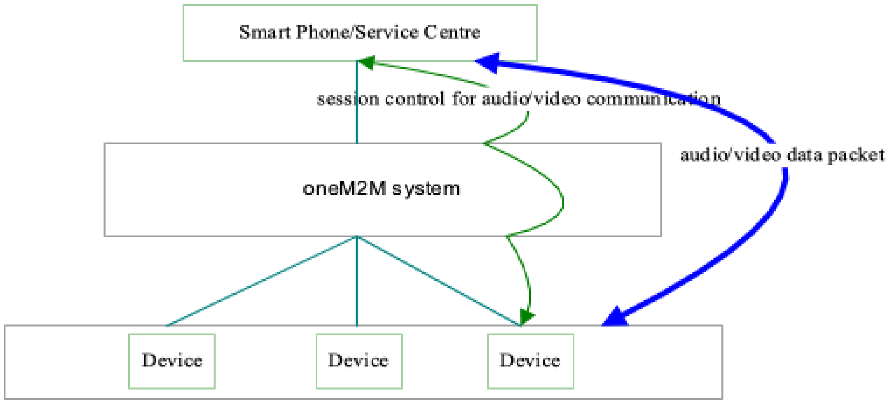

Smart Phone/Service Centre
session control for audio/video communication
audio/video data packet
oneM2M system
Device
Device
Device

Figure 47: Figure 9.4.9-1 High Level Illustration of Real-time Audio/Video Communication

9.4.10 Potential Requirements

1. The oneM2M system shall provide a capability to allocate unique identifiers to devices for identification and session routing in oneM2M system.
2. The oneM2M system shall support to establish and terminate real-time audio/video session between M2M applications.
3. The oneM2M system shall provide a capability for a device to be registered in the system.
4. The oneM2M system shall support authorization if a request to and from the device for real-time audio/video call establishment is allowed.
5. The oneM2M system shall provide a capability for routing a request for real-time audio/video call establishment from or to the device.
6. The oneM2M system shall provide a capability for media control (e.g. negotiation of transcoding, QoS) between the M2M applications for real-time audio/video data packet transmission.

9.5 Event Triggered Task Execution

9.5.1 Description

Gateway Device may be required to configure for executing some tasks which are triggered by pre-defined events.

9.5.2 Source

oneM2M-REQ-2013-0176R03 Event Triggered Task Exec Use Case

REQ-2015-0596 Event Trigger Use Case Revise

9.5.3 Actors

- Management Server,
- Gateway Device which has the characteristic both M2M Gateway (aggregate measured value) and M2M Device (accepting setting change),
- Thermometer and Air Conditioner (M2M Device),
- Data Storage Server,
- User

9.5.4 Pre-conditions

- Gateway Device is configured to work as the gateway for collecting data from some sensor devices installed at home network.
- Sensor Devices are configured to accept the management request from Gateway Device which requests reporting measured data on demand

9.5.5 Triggers

- M2M System is going to configure Gateway Device for scheduling task execution for data collection from sensor devices.

9.5.6 Normal Flow

1. Management Server requests management on scheduling task settings of Gateway Device to fetch the current value of the thermometer, and report collected data from a thermometer (one of the Sensor Devices in this use case) every 30 minutes.
2. Gateway Device establishes the connection to the thermometer, and collects measured data.
3. Gateway Device reports the collected data to Data Storage Server.

9.5.7 Alternative Flow

Alternative Flow 1

1. (after step 2 in normal flow,) Gateway Device stores series of measured data associating with the source Sensor Device.
2. Management Server requests Gateway Device to report the log data which summarize series of measured data by Sensor Devices for one day.

Alternative Flow 2

1. Management Server configures the M2M Application on the Gateway Device to start monitoring energy consumption of Air Conditioner, when the device is turned on, and to stop monitoring when that is turned off.
2. M2M Application on the Gateway Device subscribes requests notification on the power status change of Air Conditioner.
3. When the user turned on the Air Conditioner, the Gateway Device is notified by event notation for the status change.
4. M2M Application on the Gateway Device starts monitoring the energy consumption of the Air Conditioner.
5. When User turned off the Air Conditioner, the M2M Application on the Gateway Device is notified the status change
6. Gateway Device stops monitoring the energy consumption of the Air Conditioner.

Alternative Flow 3

1. Management Server configures the M2M Application on the Gateway Device to report the energy consumption when the total energy consumption exceeded over the 20kW per day.
2. M2M Application on the Gateway Device keeps collecting data about energy consumption from home electronics (i.e. Air Conditioner).
3. When the total energy consumption exceeded over the 20kW per day, the M2M Application on the Gateway sends notify the report to the Data Storage Server.

9.5.8 Post-conditions

Collected data is stored on the Data Storage Server for further use

9.5.9 High Level Illustration

9.5.10 Potential Requirements

1. M2M System Shall support timer triggered data collection on M2M Gateway from M2M Device.
2. M2M System Shall support M2M Gateway which reports collection of data measured by M2M Device.
3. M2M System Shall support to start/stop monitoring measured data by M2M Device triggered by status change of M2M Device to be monitored.
4. M2M System Shall support conditional report from M2M Gateway which reports measured data by M2M Device(s). The condition can be expressed as event notification message which is triggered by M2M Application which is monitoring threshold and/or size of value change.

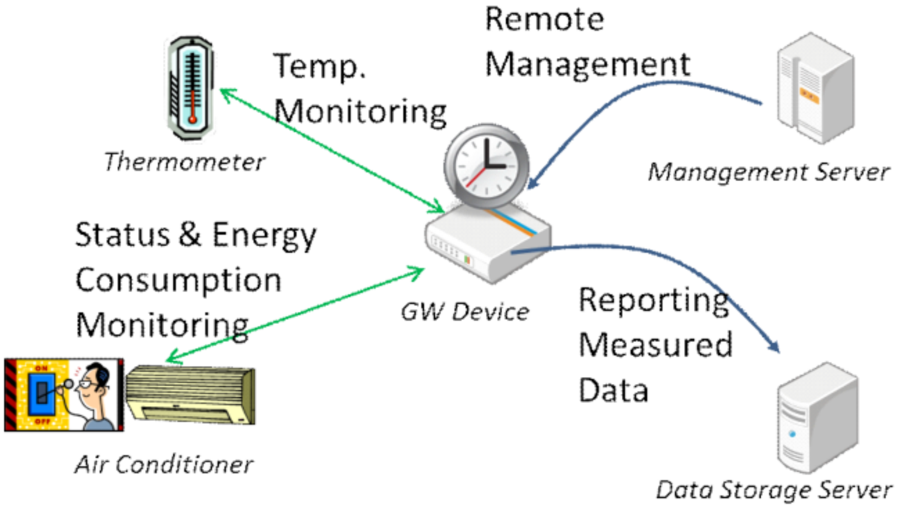


Figure 48: Figure 9.5.9-1 Event triggered Task Execution High Level Illustration

9.6 Semantic Home Control

9.6.1 Description

This use case demonstrates co-operation between two independent M2M applications. The co-operation is made possible because one application can find the other application through semantic information about the application's resources. This semantic information is available in the M2M System.

One application is a building management system (BMS) for a big apartment house. The BMS is operated by a building manager, e.g. the owner of the apartment house. BMS has knowledge about the blueprints of all the apartments in the house, e.g. it knows which heater is located in which room (heaters are assumed to be equipped with temperature sensors/actuators).

The other application is a home energy management system (HEMS). It has been subscribed by the tenant of one of the apartments. HEMS controls the heaters of the apartment (among other purposes).
Because HEMS can find the resources of BMS - e.g. the resource that represents the tenant's apartment and the heaters therein HEMS can configure itself automatically (and can adapt to changes over time) and doesn't require human configuration.
Finding the right resources in the M2M System is made possible through semantic annotation of the resources

9.6.2 Source

oneM2M-MAS-2013-0020 Semantic use cases from ETSI Semantics TR

9.6.3 Actors

- Building manager: is running a Building management system (BMS) for his apartment house.
- Tenant of an apartment: has subscribed to a home energy management system (HEMS) for his apartment.
- M2M service provider: is providing access to the M2M System for both applications, BMS and HEMS.
- Building management system (BMS): is a M2M network application.
- Home energy management system (HEMS): is a M2M network application.

9.6.4 Pre-conditions

The Building management system (BMS) is an M2M application that contains all the information needed to manage a large apartment house. In particular it contains the construction details of the tenant's apartment, where the doors and windows are located, where the heaters are, their capacity, etc. The BMS is used for overall control of the building, but information relevant for individual apartments (e.g. control of the heaters, built-in sensors for windows and doors) can be made available to authorized tenants. In case of fire, the complete blueprint of the house can be made available to fire-fighters.
In the M2M System the BMS makes its information available as M2M resources, similar to as if they were data transmitted by a device. E.g. the complete apartment, individual rooms, their heaters and windows could be represented as M2M resources.

A new tenant is renting an apartment in the house. As he is moving in, he also subscribes to a general-purpose home energy management system (HEMS) that promised a very efficient heater control. E.g. the HEMS always uses the best available electricity tariff and the heating is turned off when windows are open. As part of the subscription, the HEMS is granted access to the respective resources used by the BMS in the M2M system. In particular, the building manager has permitted access of the tenant's HEMS to those resources of the BMS that are needed for energy management of the tenant's apartment (rooms, heaters, door-and window sensors, etc.). Other resources not needed for this task are not exposed to the HEMS.

9.6.5 Triggers

None

9.6.6 Normal Flow

The newly subscribed HEMS will immediately start discovering new devices in the apartment. Once the BMS has granted access, the HEMS will discover the resources of the BMS that are related to the apartment. Using the semantic description of the devices the HEMS can immediately find out about the available rooms, heaters, temperature sensors, etc. With this knowledge it can configure itself without any human intervention.

Since the BMS has configured its devices to be represented in the M2M System as abstract devices, the HEMS can use this information to immediately control the devices using the offered abstract command set. Consequently, HEMS does not have to understand the specifics (e.g. specific protocol) of a particular heater control.

Later, the building manager installs a new device into the tenant's apartment which can help in efficient energy management. This new device is also managed by BMS. Using the selection rule of the HEMS service, the new device will get immediately available to the HEMS. The HEMS will discover the new device and will use it to control the apartment's energy consumption.

9.6.7 Alternative Flow

None

9.6.8 Post-conditions

None

9.6.9 High Level Illustration

None

9.6.10 Potential Requirements

1. The M2M System shall support a common (e.g. per vertical domain) semantic data model (e.g. represented by Ontology) available to M2M application.
2. The M2M System shall provide discovery capabilities that enable the discovery of M2M resources based on their semantic information, e.g. semantic categories and relationship among them. (e.g. all heaters and windows in a room; the room in which a window is located…).
3. The M2M System shall provide representation and discovery functionality of real-world entities (rooms, windows) that are not necessarily physical devices.
4. The M2M system shall be able to map control commands issued towards an abstract device to the concrete commands of a specific device.

9.7 Semantic Device Plug and Play

9.7.1 Description

This use case applies with any verticals, below just take home automation as an example. The use case is about when a device is newly registered in a home, it will find its own character and its relationship with its neighbour devices and Things automatically based on semantic information within the M2M system without the interference of human being. For example, the house owner bought a lamp and a switch to the lamp for his house. Both the lamp and switch is enabled with wireless abilities to be able to communicate with the home automation gateway and other devices. The lamp is for the lobby and accordingly the switch is located near the entrance of the lobby. When the house owner has placed the lamp and the switch properly, a simple power-on would make the lamp and the switch work fine.

9.7.2 Source

oneM2M-MAS-2013-0020 Semantic use cases from ETSI Semantics TR

9.7.3 Actors

- Home automation service provider: is providing home automation service by providing applications running on home automation devices such as gateway, lamp, switch, TV, air-condition etc.
- Home automation management system (HAMS): is a network application.
- Device manufacturer: produces devices as M2M nodes.
- M2M service provider: provides M2M service acts as a platform where all M2M nodes can register to.
- House owner: is a consumer of the home automation service.

9.7.4 Pre-conditions

The house owner has a contract with the home automation service provider for the home automation service. The home automation service provider has a business relationship with the M2M service provider and the device manufacturer. The home automation management system manages all the devices and their relationships registered in the house. Each device has its role and serves fixed services among all home devices.

9.7.5 Triggers

None

9.7.6 Normal Flow

When the house owner buys new devices for his house, the newly bought devices will register to the M2M service provider and expose to the M2M SP its role and functionalities including their semantic descriptions. According to such information, the HAMS will compare the semantic description of the new device with the semantic description of the existing devices in the house and judge their relationships by semantic inference. Then the HAMS will help establish the relationship between the new device and the device in the home and the relationship is maintained in the M2M SP. For example the HAMS finds that the lamp is to be controlled by the switch, it may then bind the status of the switch to the action of the lamp. If the status of the switch is ON, an "ON" command will be sent to the lamp automatically.

9.7.7 Alternative Flow

None

9.7.8 Post-conditions

None

9.7.9 High Level Illustration

None

9.7.10 Potential Requirements

1. The M2M System shall support a semantic data model that is at least common to the vertical industry in which a Thing is used to describe Things registered in the M2M System.
2. The M2M entity shall be able to expose its semantic description to the M2M System.
3. If a Thing is capable to expose semantic information to the M2M System the M2M System shall be able to use that information to represent the Thing.
4. The M2M System shall be able to describe the semantic relationship between Things.

9.8 Triggering in the Field Domain

Void

> Note: This use case can be found in TR-0013 [i.18]

Source: REQ-2014-0447 Use case for Triggering in Field Domain

9.9 Patch the connected home

9.9.1 Description

This use case is to provide a solution to monitor and update the software of the different devices in a house. Many devices are connected to internet through the Home Gateway provided by the Operator. All these devices could be attacked and used to prepare some attacks (e.g. DDoS, cyber attack) if they are not protected and kept up to date against vulnerabilities. The patch could be also necessary to maintain the continutity with the service and the support of new functionalities within the Home.

9.9.2 Source

REQ-2018-0021R04- Use case patch the digital home.

9.9.3 Actors

IoT Device(s), Gateway, device manufacturer, and Operator (Internet Service Provider).

9.9.4 Pre-conditions

None

9.9.5 Triggers

None

9.9.6 Normal Flow

- The Operator, through the Gateway, collects all the software/firmware versions of the devices in the Home network (object management inventory function).
- For each device, the Operator, through the Updates' Coordinator, liaises with the manufacturer and collects information about the up-to-date software/firmware versions.
- The Operator retrieves all the available updates from device manufacturer.
- In accordance with the user consent and the criticity of the updates, the Operator launches software updates for the impacted devices.

9.9.7 Alternative Flow

- The Operator, through the Gateway, collects all the software/firmware versions of the devices in the Home (object management inventory).
- For each device, the Operator, through the Updates' Coordinator, liaises with the manufacturer and collects information about the up-to-date software/firmware versions.
- The Operator retrieves all the available updates information from device manufacturer.
- The Opeartor informs the end user about the necessary updates
- In accordance with the user consent and the criticity of the updates, the deveice manufacturer launches software updates for the impacted devices.

9.9.8 Post-conditions

None

9.9.9 High Level Illustration

The figure below depicts high architecture. Herafter, the high level desctiption of all the steps in the figure:

- (1) Scan the Home network ecosystem controlled by the GW to obtain metadata.
- (2) All valid (i.e. not compromised) devices answer to the request from GW
- (3) GW informs the Coordinator server on current situation
- (4) Coordinator inform the concerned manufacturers and request action (e.g. Detected security breachs by the operator, ask for security patch, ask for update, etc)
- (5) Manufacturer sends back up to date information and OS (e.g. new versions, new features, new)
- (6) Coridinator retrieves the OS and sends it to all concerned GWs
- (7) According to user consent, GW launchs secure installation to dedicated devices. GW could perform integrity and authenticity check of the SW on behalf the device (e.g. for Lightweight device).

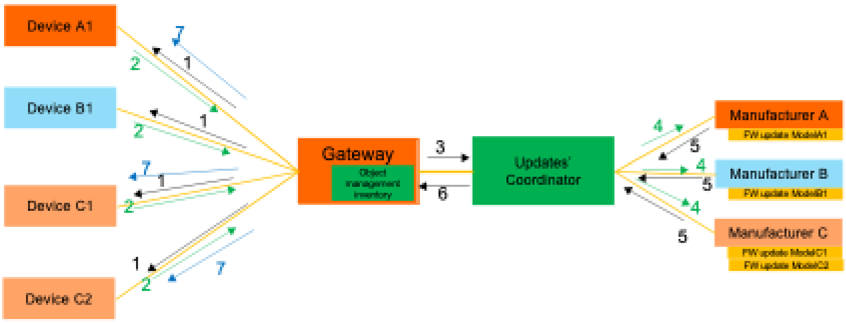


Figure 49: Figure 9.9.9-1 Call flow for the connected home patch

9.9.10 Potential Requirements

- The M2M System shall be able to dynamically obtain metadata (e.g. Firmware version, Manufacturer ID, HW version) from field devices (e.g. located behind a gateway).
- The M2M System shall be able to authenticate metadata (e.g. Firmware version, Manufacturer ID, HW version) from field devices (e.g. located behind a gateway).
- The M2M System shall be able to trigger the secure (e.g. authenticity, integrity, and confidentiality protected) Firmware/Software update of field devices.

9.10 Use case for Disguise Data for Security and Privacy

9.10.1 Description

A smart home can monitor and control everything in various fields such as home appliances (e.g., TV, air conditioner, refrigerator), energy consumption devices (e.g., water, electricity, air conditioning), and security devices (e.g., door lock, surveillance camera) through a communication network.

While it may be convenient to control a smart home from a remote device (such as a smartphone), there are many cases of how critical security devices like locks, alarms, and even baby monitors can be hacked. If the smart home is hacked or the smart home data set is shared with the public, smart home devices like smart plugs or lightbulbs can provide entry points for hackers. For example, hackers can easily predict when the house is vacant by analyzing the data measured by smart home devices.

The k-anonymity algorithm is a basic model for personal information protection and can be used as one of the methods to ensure anonymity, which is one of the personal information protection methods suggested by GDPR. In other words, guaranteeing anonymity means a technology that makes it impossible to identify a specific individual in a dataset containing personal information. A technology that prevents specific personal information from being exposed by creating it is also used. K-anonymity is a technology that makes it impossible to extract personal information or specific information by easily combining different information and ensuring that at least k of the same value exists in a given data set. To this end, in k-anonymity, a part of the data set is modified, or arbitrary data is added so that all data have the same (or indistinguishable) k-1 or more data as themselves. Therefore, it is impossible for an attacker to know which data is being attacked in an unidentified data set.

9.10.2 Source

RDM-2021-0087R01_disguise_data_for_security_and_privacy

9.10.3 Actors

- Smart home sensors: Sensors deployed in smart home.
- IoT platform: An IoT platform that manages data from smart home applications

9.10.4 Pre-conditions

- The cloud IoT platform awares which IoT applications are subject to be protected.

9.10.5 Triggers

- For example, a smart home measures various data from its deployed sensors, e.g., termperature, humidity, status of door. As data from these smart home sensors can reveal user's behavior, the IoT service cloud platform generates a set of fake data that is visible to others except for the home family member.

9.10.6 Normal Flow

Figure 9.10.6-1 illusrates the high-level flows of the generating fake data for security and privacy use case, which consists of the following steps:

- **Step 001** : IoT sensor (i.e., Application #1) in a smart home measuring temperature sends measured data to the IoT platform. The resource for Application #1 is configured to generate a fake data when a new measurement is created.
- **Step 002:** IoT service layer platform creates a resource to store the new measurement. Then IoT service layer platform returns response message to Application #1
- **Step 003:** Application #1 sends a request to create a resource which is a placeholder for new data measurement.
- **Step 00 4 :** As the application resource is configured to generate a fake data when there is a new measurement, a data management function is informed internally.
- **Step 005:** The data management function creates a resorce for a fake data and store a fake value to the resource.
- **Step 006:** IoT service layer returns a response message to Application #1.

###9.10.7 Alternative Flow

None

9.10.8 Post-conditions

None

9.10.9 High Level Illustration

9.10.10 Potential Requirements

The oneM2M System shall be able to generate fake data for security and privacy reason (e.g., hide trends of smart home data change).

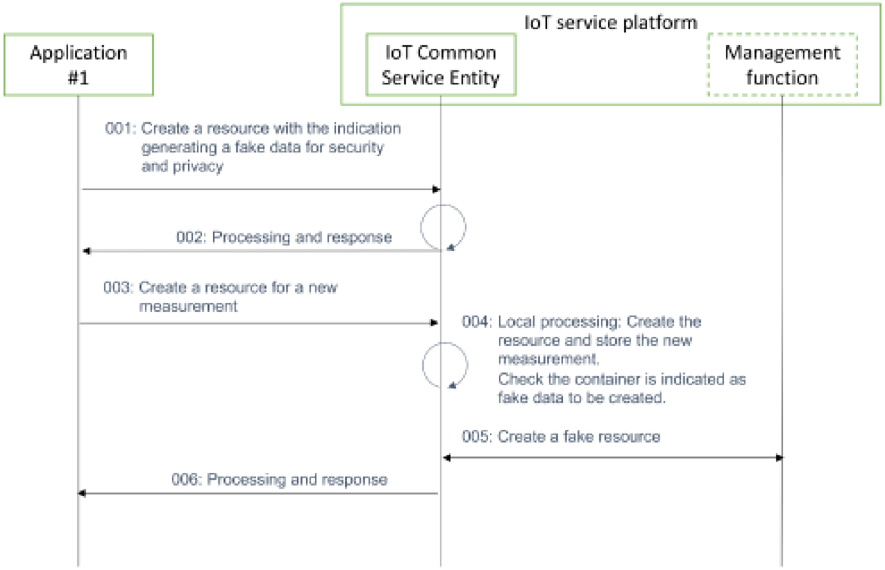

IoT service platform
Application #1
IoT Common Service Entity
Management function
001: Create a resource with the indication generating a fake data for security and privacy
002: Processing and response
003: Create a resource for a new measurement
004: Local processing: Create the resource and store the new measurement.
Check the container is indicated as fake data to be created.
005: Create a fake resource
006: Processing and response

Figure 50: Figure 9.10.6-1 A normal flow for creating fake data when a new measurement is created

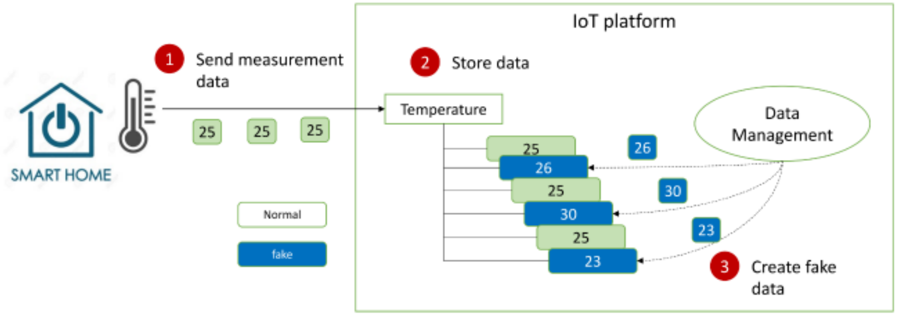


Figure 51: Figure 9.10.9-1 Conceptual diagram of hiding trends of data over time using fake data

10 Retail Use Cases

10.1 Vending Machines

10.1.1 Description

In some situations, vending machine providers need to limit the network access for vending machines based on their geographic location. The providers do NOT want the vending machine user to move the machine from the specified area to other locations (potentially for better sales), so that the providers can control the geographic distribution of their vending machines and make decisions based on data statistics and analysis (e.g. which are the best-selling areas? How many products are sold in specified areas during specified time? (and so on).

10.1.2 Source

REQ-2014-0466R05 Use case for vending machine

10.1.3 Actors

- Vending machine, which can automatically sell products and report data information to the application platform through M2M service platform
- The M2M service platform, which can control the vending machine device and its access to the network
- Vending machine application platform, which can accept the data report from vending machine, monitor its status, and perform data analysis.

10.1.4 Pre-conditions

The location information of the Vending machine is provided to the M2M Service platform by the Underlying network.

10.1.5 Triggers

- Vending machine restarts and registers to M2M service platform
- Vending machine reports data information (e.g., each sale transaction or products selling information and so on).

10.1.6 Normal Flow

- The vending machine restarts and registers to M2M service platform.
- The M2M service platform checks the geographic location policy. If current geographical location of the vending machine is in the permitted area, it allows the vending machine to register. Otherwise, it denies access.
- After vending machine successfully registers, it reports data information (for example, the product selling information and the stock information) periodically or for each product sale to the vending machine application platform through M2M service platform.

- The M2M service platform checks the geographic location policy. If the current geographic location of the vending machine is in the permitted area, it allows for the data report. Otherwise, it will be denied.
- The vending machine application platform receives the data information report, records the information and performs data analysis.

10.1.7 Alternative Flow

None

10.1.8 Post-conditions

None

10.1.9 High Level Illustration

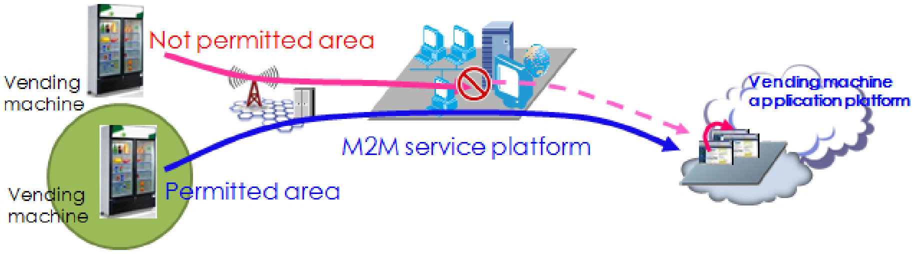


Figure 52: Figure 10.1.9-1 - High level illustration of Vending Machines use case

10.1.10 Potential Requirements

1. The M2M service platform shall be able to support the geographic location-based network access policy. (see also requirement OSR-047)
2. The M2M service platform shall be able to support a geographical boundary within a network access policy. (see also requirement OSR-047)

11 Transportation Use Cases

11.1 Vehicle Diagnostic & Maintenance Report

Void

Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2012-0067R03 Vehicle Stolen and Vehicle Diagnostics

11.2 Remote Maintenance Services

Void

Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2013-0188R06 Use Case Remote Maintenance

11.3 Traffic Accident Information Collection

Void

Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2013-0264R05 Use Case Traffic Accident Information Collection

Note: From [i.10]ETSI TR 102 638

11.4 Fleet Management Service using DTG (Digital Tachograph)

Void

Note: This use case can be found in TR-0026 [i.21].

Source: oneM2M-REQ-2013-0219R01 Use case - Fleet management using DTG

11.5 Electronic Toll Collection (ETC) Service

Void

Note: This use case can be found in TR-0026 [i.21].

Sources:

REQ-2014-0431R03 Use cases for Electronic Toll Collection (ETC) service
REQ-2014-0449R02 Use cases for Electronic Toll Collection (ETC) service

11.6 Taxi Advertisement service

Void

Note: This use case can be found in TR-0026 [i.21].

Source: REQ-2014-0467R02 Use case for taxi advertisement

11.7 Vehicle Data Service

Void

Note: This use case can be found in TR-0026 [i.21].

Source: REQ-2014-0472R06 Use Case on Vehicle Data Services

11.8 Smart Automatic Driving

Void

Note: This use case can be found in TR-0026 [i.21].

Source: REQ-2015-0554-Smart Automatic Driving

11.9 Vehicle Data Wipe Service

Void

Note: This use case can be found in TR-0026 [i.21].

Source: REQ-2015-0589R04 Use case on vehicle data wipe service

12 Other Use Cases

12.1 Extending the M2M Access Network using Satellites

12.1.1 Description

This Use Case demonstrates a scenario that extends the M2M access network using satellite communications. It serves to emphasize that satellite communication is a key component of the network domain to be incorporated in future requirements work at OneM2M on Smart Metering and other M2M use cases.

In locations that are difficult to reach with fixed-line or cellular communications, a machine-to-machine (M2M) satellite solution extends terrestrial coverage and provides access to devices that require remote monitoring and control. Satellite-based communication networks provide communications that integrate seamlessly with any remote IP based application. Satellite networks offer IP connectivity, ubiquitous real time coverage, robust security, high availability compared to cellular networks. Satellite M2M solutions are also much more cost-effective than some years due to advances in satellite technology.

Traditional satellite communications has had a stigma of being expensive and requiring large, power-hungry terminals too complex to integrate with applications. Modern satellite networking, however, provides competitive price solutions, ubiquitous coverage, and a high level of availability which compliment terrestrial networks. For this reason, it is important to consider satellite services for Supervisory Control and Data Acquisition (SCADA) applications, low data rate (LDR) solutions, and other remote, unmanned machine-to-machine (M2M) services.

12.1.2 Source

oneM2M-REQ-2012-0061R02 Use Case Smart Metering with Satellite Communications

12.1.3 Actors

- Service Providers for M2M

12.1.4 Pre-conditions

The following additional functionalities or sub scenarios are explained in a high level format, to relate to electricity, gas, heating, and water.

1. Distribution Automation
   Deploying satellite M2M services along power distribution lines, as a supporting link, allows electrical utility providers to connect to their data centres and extend their network reach to the boundaries of their entire service territory, improving decision-making and operational efficiencies. A single, two-way IP data connection provides automated monitoring and control of re-closers, switches, or other distribution devices - anywhere - enabling utility providers to maintain continuous surveillance and control of their distribution network for voltage fluctuations, outages and service demands.
2. Substation Connectivity
   M2M Satellite communications provide services for electricity substations in locations that may be difficult to reach with fixed-line or cellular communications.
   M2M Satellite communications contains the flexibility to cope with both low-volume high-frequency traffic and bursts of high-volume, low-frequency traffic. If a primary link breaks down, satellite communications can automatically provide backup communications at any substation.
3. Disaster Recovery
   Business continuity is vital for utilities that provide essential services such as electricity, water and gas to millions of people as they need to be able to recover immediately from natural or manmade disasters. When a catastrophic event causes terrestrial networks to fail, utilities companies can rapidly deploy satellite terminals to provide an alternative communications path, enabling them to maintain communications, diagnose issues quickly, and run critical applications.

12.1.5 Triggers

The need to access M2M user devices (UDs) that may not be reachable with terrestrial and wireless networks.

12.1.6 Normal Flow

An example of a M2M communication using satellite service is Smart Metering (valves, electricity meter, gas meter, water meter, and heat meter). Smart Metering devices over a small area connect to aggregation points or Smart Meter Concentrators via a local, meshed wireless network. These aggregation points, or concentrators, collect usage data and distribute control data to and from consumers in a limited geographical area, transmitting it back to the utility's data centre (Figure 12.1.9-1).

The satellite connectivity backhauls Smart Meter data from a satellite antenna mounted on an Advanced Metering Infrastructure (AMI) concentrator to the utility's data centre. Each AMI concentrator links to multiple smart meters via a local wireless network.

In this configuration example, satellite communications co-locate with the primary gateway communication to aggregate meter data at the gateway, extending the network reach across a utility's entire service.

12.1.7 Alternative Flow

None

12.1.8 Post-conditions

None

12.1.9 High Level Illustration

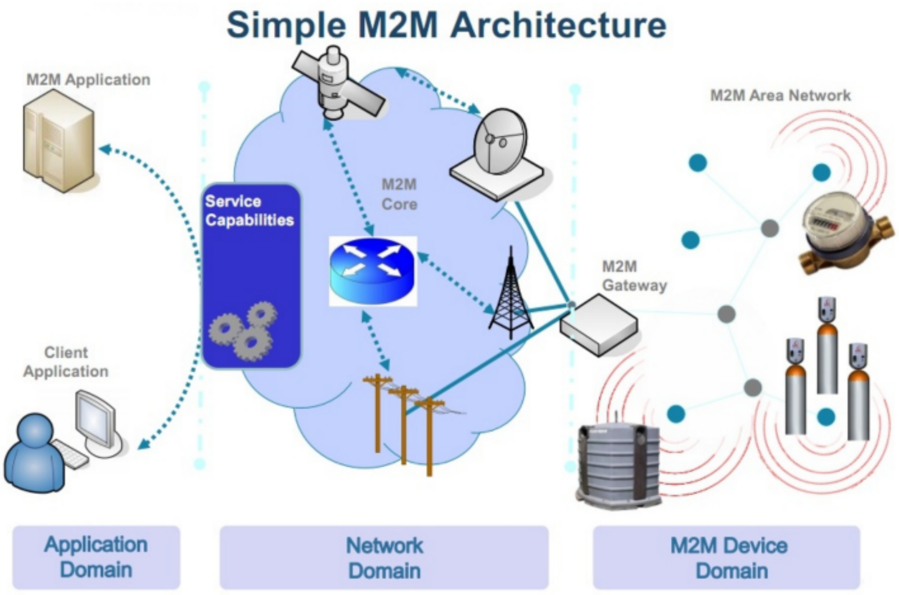


Figure 53: Figure 12.1.9-1 Extended Smart Metering Configuration (source: ETSI)

12.1.10 Potential Requirements

1. Satellite access shall be considered in all M2M network domain architectures.

12.2 M2M Data Traffic Management by the Underlying Network Operator

12.2.1 Description

According to the data traffic condition, e.g. current traffic congestion status, in underlying networks, the underlying network operators (e.g. mobile network operators) would like to manage the M2M data traffic in their networks in conjunction with M2M service platform and/or M2M application server providers in order to avoid losing the M2M communication data packets in the networks.

The M2M service platform and/or M2M application server providers will change their configuration such as data transmission interval or stop sending data over the underlying networks for some duration after receiving the notification from underlying networks.

This use case illustrates handling of M2M data transmission based on the data traffic condition information of underlying network and interworking among the M2M service application server, M2M platform and the underlying network.

12.2.2 Source

oneM2M-REQ-2013-0175R03 Use Case on M2M data traffic management by underlying network operator

12.2.3 Actors

- The M2M application server providing data transmission control according to the data traffic condition of underlying network
  The application server has functions to receive data traffic condition information from the M2M platforms and/or the underlying networks, and control M2M data transmissions according to the received information.
- The M2M service platform providing data transmission control according to the data traffic condition information of underlying networks
  The M2M service platform has functions to receive the data traffic condition information from the underlying networks, and/or control M2M data transmissions according to the information.
- The underlying network providing the data traffic condition information
  The underlying network has functions to send the data traffic condition information to M2M application servers, M2M service platforms, and/or M2M devices. The data traffic condition information includes required transmission interval, required maximum data rate, required maximum

data volume, current traffic congestion status, congested network area information etc.

- The M2M device providing data transmission control according to the data traffic condition information
  The M2M device to receive the data traffic condition information from the underlying networks or M2M service platforms, and control M2M data transmissions.

12.2.4 Pre-conditions

The underlying network monitors the status of the data traffic, analyse the status, define the traffic condition and provides the data traffic condition information to M2M application servers, M2M platforms and/or M2M devices.

12.2.5 Triggers

None

12.2.6 Normal Flow

Normal Flow 1:

1. The mobile network sends the data traffic condition information to the M2M service platform and/or M2M application server.
2. After the M2M service application server receives the data traffic condition information from the underlying network in step1, and it controls M2M data transmission accordingly.
3. After the M2M application service platform receives the data traffic condition information from the underlying network in step 1 via the M2M service platform, it and controls M2M data transmissions accordingly.
4. The M2M service platform may send M2M data transmission configuration information to the M2M device.
5. After the M2M device may receive M2M data transmission configuration information from the M2M service platform in step 4, it and may controls M2M data transmissions accordingly.

Normal Flow 2:

1. The underlying mobile network sends the data traffic condition information to the M2M device as well as M2M service platform.
2. Upon receiving the information, the M2M device re-configures the application behavior, e.g. the interval extension of communication, by M2M service layer capability. The re-configuration profile may be statically stored or can be overwritten by control from the M2M service platform.
3. Upon receiving the information, the M2M service platform controls M2M data transmission accordingly in cooperation with M2M service application server described in step 1 to step 3 in normal flow 1.

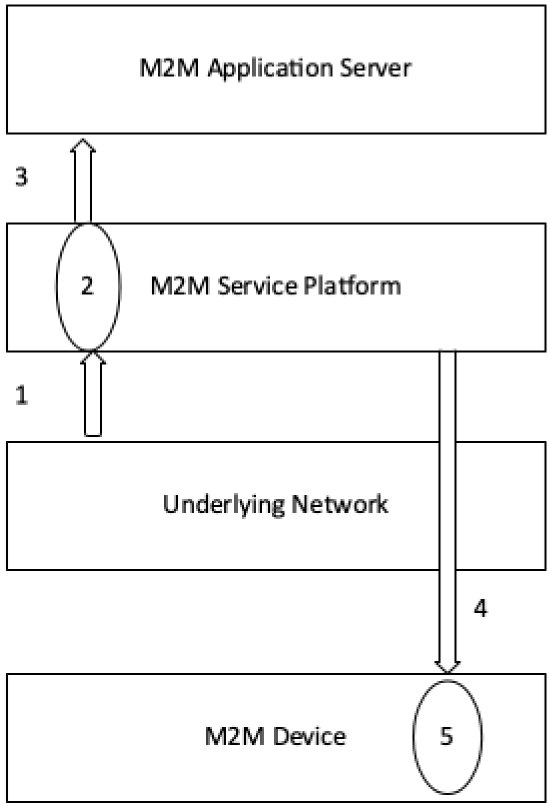


Figure 54: Figure 12.2.6-1 Normal Flow 1 of Data Traffic Management by Underlying Network Operator

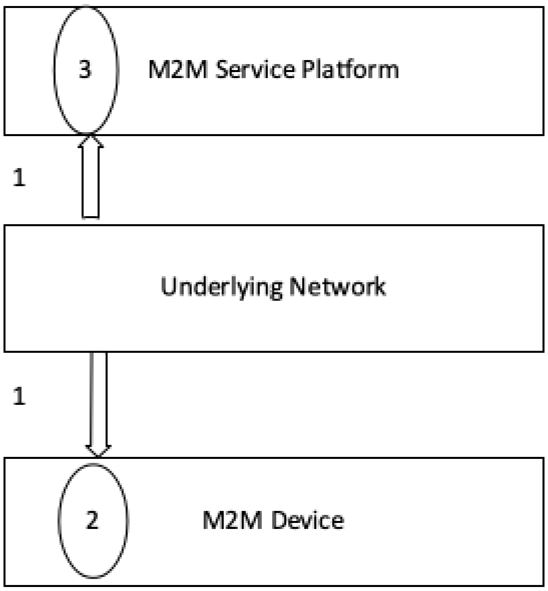


Figure 55: Figure 12.2.6-2 Normal Flow 2 of Data Traffic Management by Underlying Network Operator

12.2.7 Alternative Flow

None

12.2.8 Post-conditions

None

12.2.9 High Level Illustration

12.2.10 Potential Requirements

1. The M2M service platform SHALL be able to receive the data traffic condition information from the Underlying network and notify it to the M2M application server. The M2M application server SHALL be able to control M2M data transmission based on the Underlying Network data traffic condition.
2. The M2M service platform MAY SHALL be able to control M2M data transmission based on the Underlying Network data traffic condition.
3. The M2M device SHALL be able to control M2M data transmission based on the Underlying Network data traffic condition.
4. The M2M device SHALL control M2M application behavior implemented on top of M2M service layer when the M2M device received notification

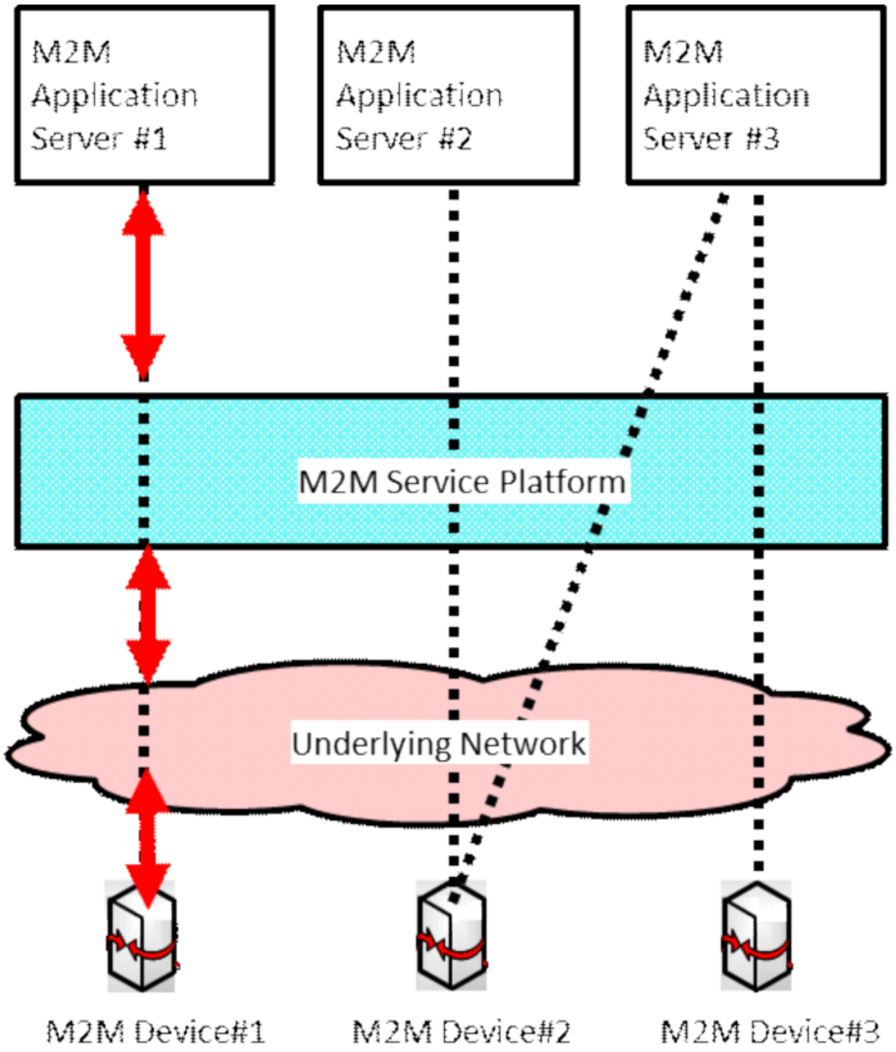

M2M Application Server #1
M2M Application Server #2
M2M Application Server #3
M2M Service Platform
Underlying Network
M2M Device#1
M2M Device#2
M2M Device#3

Figure 56: Figure 12.2.9-1 High Level Illustration of Data Traffic Management by Underlying Network Operator

regarding Underlying Network data traffic condition from the Underlying Network.

12.3 Optimized M2M interworking with mobile networks (Optimizing connectivity management parameters)

12.3.1 Description

Background on the use case and current state in 3GPP.

M2M Services, due to their nature (generally not involving human conversations), will most likely create much lower Average Revenue Per User (ARPU) to an Underlying mobile Network than ordinary Human-to-Human traffic.

Since M2M services, and in particular the oneM2M standard, relies on Underlying Networks (often mobile networks) the success of M2M will inevitably depend on the fact that M2M traffic in the underlying network will compete with human-to-human traffic; both, technically (use of resources) and economically (ARPU).

If M2M traffic in the Underlying Network would not be competitive with human-to-human traffic then a significant sector of M2M services - i.e. those with low ARPU - could not be realized.

To enable economically feasible M2M business e.g. 3GPP seeks to reduce the costs - impact of traffic to the network and the consumption of radio resources - that M2M devices will create for their networks.

E.g. already as early as in 2008 3GPP has created a first set of requirements on Machine Type Communications (MTC) in [i.11] TS 22.368. These were finally approved in 3GPP Rel-10 (2010).

However, due to the (at the current point in time) low priority of M2M business for 3GPP Networks only limited work has been done in 3GPP architecture, radio- and protocol groups until now.

E.g. only 2 out of 4 building blocks: MTCe-SDDTE (Small Data and Device Triggering Enhancements) and MTCe-UEPCOP (UE Power Consumption Optimizations) have been prioritized by SA2 to be handled in current 3GPP Rel-12.

SA2 (architecture) normative work can be found in [i.12] TS 23.682, the architecture study in [i.13] TR 23.887

We believe - and hope - that when in a few years 3GPP Rel-12/13 networks will be in operation then M2M traffic will have a significant share in 3GPP networks. Therefore it is crucial that oneM2M expresses its needs and potential impact to 3GPP now.

OneM2M, representing a high level of expertise in M2M business, needs to actively offer support to 3GPP and other Underlying Network technologies.

Overview of the use case

Many mobile data applications are characterized by transmission of small data packets. Frequent small data transmission may cause the network load by the mobile terminal changing frequently between idle and connected state, if the terminal returns to idle mode soon after the data transmission. On the other hand, when the mobile terminal is kept connected state unnecessarily (if normal operation involves only small data transmission), it has impact on mobile terminal power consumption and radio resources consumption.

In order to reduce both, the control load related to the state transition and the consumption of radio resources, the mobile network (e.g. 3GPP) needs to adjust configuration parameters (the connect keep timer, the radio reception interval, etc.) based on the data transmission interval (frequent or infrequent) of the mobile terminal.

It is important for a mobile network to be informed about a change of data transmission interval of a M2M device which is handled or monitored on service layer. However, such a change of data transmission interval is not easily detected by the mobile network.

This use case illustrates detection of a change of data transmission interval on service layer and notification to the mobile network by interworking between the M2M service platform and the mobile network.

12.3.2 Source

oneM2M-REQ-2013-0231R02 Use Case on Mobile Network interworking-connectivity

12.3.3 Actors

- An M2M Application, hosted on an application server, provides services for creating flood warnings by making use of (and communicating with) an M2M Device that is measuring water levels of a river.
  - If the M2M Application detects that the water level becomes hazardous by the measurement data of the M2M device it sends a request to change the communication mode (normal->abnormal) to the M2M device (the water sensor), and sends current data transmission interval (frequent communication) of the M2M device to the M2M service platform.
  - The data transmission interval includes interval level (normal or frequent), interval value (5min, 30 min, 1h) etc.
- The M2M service platform provided by the M2M service provider
  - The M2M service platform has functions to get the data transmission interval from the application server, analyse the information to detect the change of the transmission interval of the M2M device and send

    the current data transmission interval of the M2M device to the mobile network if any changes are discovered.

- The mobile network provided by the mobile network operator
    - The mobile network has functions to get the current data transmission interval of the M2M device from the M2M service platform and inform the mobile network about it.
- The M2M device
    - The M2M device (the water level sensor) has functions to collect the measurement data and send it the application server.
    - The M2M device has two communication modes.
        * The normal communication mode (the water level is within a safe range): the data transmission interval is infrequent (e.g. once an hour).
        * The abnormal communication mode (the water level exceeds the normal range (hazards)): the data transmission interval is frequent (e.g. every minute).
    - The M2M device has function to change into abnormal communication mode (the data transmission interval is frequent) by a request to change the communication mode (normal->abnormal) from the application server.

12.3.4 Pre-conditions

- The water level of the river is safe. It means the data transmission interval of the M2M device (the sensor) is infrequent (the communication mode is normal).
- The configuration parameters of the mobile network about the M2M device
    - The connection keep time :Short

12.3.5 Triggers

The water level of the river changes to hazardous through heavy rain. It means the data transmission interval changes to frequent (the communication mode is abnormal) from normal (the communication mode is normal).

12.3.6 Normal Flow

1. The application server checks the measurement data from the M2M device (the water sensor).
2. If the application server detects that the water level becomes hazardous by the measurement data, sends a request to change the communication mode (normal->abnormal) to the M2M device (the water sensor), send current communication interval (frequent) of the M2M device to the M2M service platform.
3. The M2M service platform detects the change of the data transmission interval (infrequent->frequent) of the M2M device based on the current

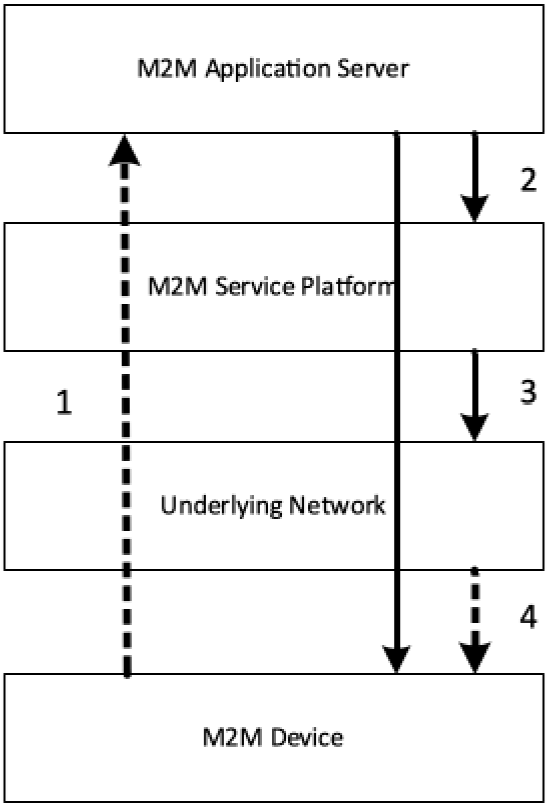


Figure 57: Figure 12.3.6-1 Normal Flow - Optimizing connectivity management parameters

communication interval (frequent), and sends the current data transmission interval of the M2M device to the mobile network.

4. The mobile network adjusts configuration parameters of the mobile network about the M2M device based on the current data transmission interval of the M2M device if necessary.

E.g. the configuration parameters of a 3GPP network may include the connection keep time (e.g. the inactivity timer, the idle (dormant) timer), the radio reception interval (e.g. the DRX (discontinuous reception) timer) etc.

12.3.7 Alternative Flow

None

12.3.8 Post-conditions

The configuration parameters of the mobile network about the M2M device

- The connection keep time :Long

12.3.9 High Level Illustration

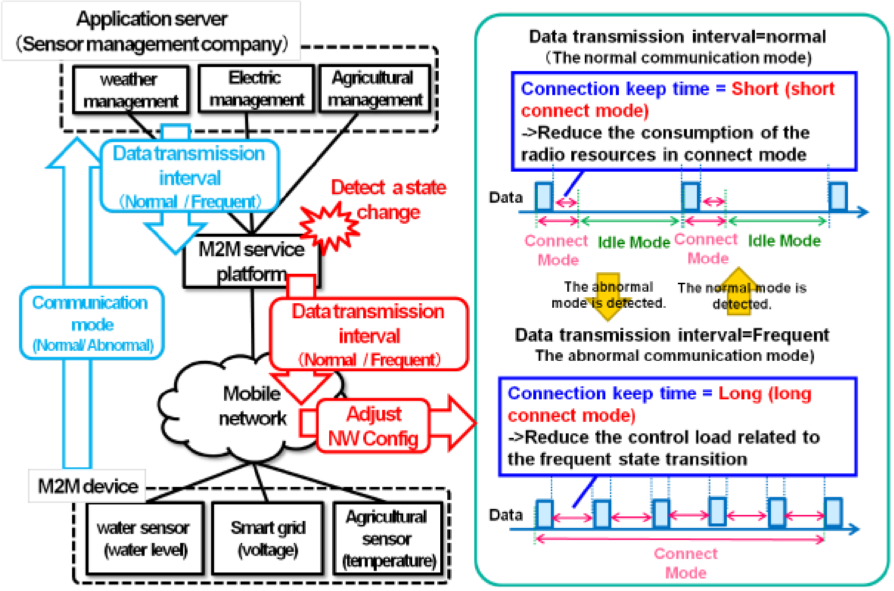

Application server
(Sensor management company)
weather management
Electric management
Agricultural management
Data transmission interval
(Normal / Frequent)
Detect a state change
M2M service platform
Communication mode
(Normal/ Abnormal)
Data transmission interval
(Normal / Frequent)
Mobile network
Adjust NW Config
M2M device
water sensor (water level)
Smart grid (voltage)
Agricultural sensor (temperature)
Data transmission interval=normal
(The normal communication mode)
Connection keep time = Short (short connect mode)
->Reduce the consumption of the radio resources in connect mode
Data
Connect Mode
Idle Mode
Connect Mode
Idle Mode
The abnormal mode is detected.
The normal mode is detected.
Data transmission interval=Frequent
The abnormal communication mode)
Connection keep time = Long (long connect mode)
->Reduce the control load related to the frequent state transition
Data
Connect Mode

Figure 58: Figure 12.3.9-1 High Level Illustration - Optimizing connectivity management parameters

12.3.10 Potential Requirements

1. The M2M service platform SHALL be able to provide the Underlying Network with information related to M2M devices that allows optimizations in the Underlying Network with regard to M2M traffic.
    - An example of such useful information to a cellular network is the current (or change of the) set of data transmission scheduling descriptors including interval times (5min, 30 min, 1h), time ranges (10pm-6pm) etc. of the M2M Device
    - How to utilize such information by the cellular network is the cellular operator implementation dependent and outside the scope of oneM2M.
2. The M2M service platform MAY be able to compute the information with which the Underlying Network should be provided by analysing the information received from the M2M application before providing to the Underlying Network. > Note: The interface to convey such information to the Underlying Network will depend on the type (e.g. 3GPP, 3GPP2, fixed) of the Underlying Network.

12.4 Optimized M2M interworking with mobile networks (Optimizing mobility management parameters)

12.4.1 Description

Background on the use case and current state in 3GPP

M2M Services, due to their nature (generally not involving human conversations), will most likely create much lower Average Revenue Per User (ARPU) to an Underlying mobile Network than ordinary Human-to-Human traffic.

Since M2M services, and in particular the oneM2M standard, relies on Underlying Networks (often mobile networks) the success of M2M will inevitably depend on the fact that M2M traffic in the underlying network will compete with human-to-human traffic; both, technically (use of resources) and economically (ARPU).

If M2M traffic in the Underlying Network would not be competitive with human-to-human traffic then a significant sector of M2M services - i.e. those with low ARPU - could not be realized.

To enable economically feasible M2M business e.g. 3GPP seeks to reduce the costs - impact of traffic to the network and the consumption of radio resources - that M2M devices will create for their networks.

E.g. already as early as in 2008 3GPP has created a first set of requirements on Machine Type Communications (MTC) in [i.11] TS 22.368. These were finally approved in 3GPP Rel-10 (2010).

However, due to the (at the current point in time) low priority of M2M business for 3GPP Networks only limited work has been done in 3GPP architecture, radio-

and protocol groups until now.

E.g. only 2 out of 4 building blocks: MTCe-SDDTE (Small Data and Device Triggering Enhancements) and MTCe-UEPCOP (UE Power Consumption Optimizations) have been prioritized by SA2 to be handled in current 3GPP Rel-12.

SA2 (architecture) normative work can be found in [i.12] TS 23.682, the architecture study in [i.13] TR 23.887

We believe - and hope - that when in a few years 3GPP Rel-12/13 networks will be in operation then M2M traffic will have a significant share in 3GPP networks. Therefore it is crucial that oneM2M expresses its needs and potential impact to 3GPP now.

OneM2M, representing a high level of expertise in M2M business, needs to actively offer support to 3GPP and other Underlying Network technologies.

Overview of the use case

For optimizing traffic handling it is important for a mobile network to know about the mobility characteristics (e.g. low mobility) of a M2M device to adjust configuration parameters (the traffic (paging) area, the location registration interval, etc.). Such mobility characteristics are not easily detected by the mobile network itself but depend on the M2M service and need to be provided by the service layer.

Currently e.g. the assumption in 3GPP is that such mobility characteristics are relatively static and do not change for the device. However in reality one and the same device (e.g. device in a car) may at one time be stationary - low mobility characteristics when the car is parked - and at other times be mobile - high mobility characteristics when driving.

Therefore it becomes important for the mobile network to be informed about mobility characteristics (and changes of it) of a M2M device. However such information can only be provided on service layer and not by the mobile network itself.

This use case illustrates detection of a change of mobility characteristics on service layer (through the M2M Application) and notification (through the oneM2M Service Capabilities) to the mobile network by interworking between the M2M service platform and the mobile network.

12.4.2 Source

oneM2M-REQ-2013-0137R02 Use Case on Mobile Network interworking-mobility

12.4.3 Actors

- The application server providing an application for a fleet management company

The application server has functions to get the mobility related M2M information from the M2M device and send the current mobility characteristics based on the mobility related M2M information to the M2M service platform.

- The M2M service platform provided by the M2M service provider
  The M2M service platform has functions to get the current mobility characteristics from the application server, analyse the information to detect the change of the mobility characteristics of the M2M device based on the current mobility characteristics and send the current mobility characteristics of the M2M device to the mobile network if any changes are discovered.
  The mobility characteristics include mobility status (high mobility, low mobility, no mobility), direction and speed, etc.
- The mobile (transport) network provided by the mobile network operator
  The mobile network has functions to get the current mobility characteristics of the M2M device from the M2M service platform and adjust the configuration parameters of the mobile network about the M2M device based on the current mobility characteristics of the M2M device.
  The configuration parameters of the mobile network include the traffic (paging) area, the location registration interval, etc.
- The M2M device
  The M2M device has functions to collect the mobility related M2M information from sensors within the vehicle and send it to the application server.
  The mobility related M2M information includes engine on/off, navigation system on/off, and GPS data etc.

12.4.4 Pre-conditions

An M2M Application, hosted on an application server, provides services for fleet management by making use of (and communicating with) an M2M Device that is mounted on a vehicle of the fleet.

- The vehicle is running on the road. It means the mobility characteristics of the M2M device (the vehicle) is high mobility (the engine is on)
- The configuration parameters of the mobile network about the M2M device
  - The traffic (paging) area: Wide
  - The location registration interval: Short

12.4.5 Triggers

The vehicle stops at a parking lot. It means the mobility characteristics of the M2M device (the vehicle) changes from high mobility (the engine is on) to no mobility (the engine is off).

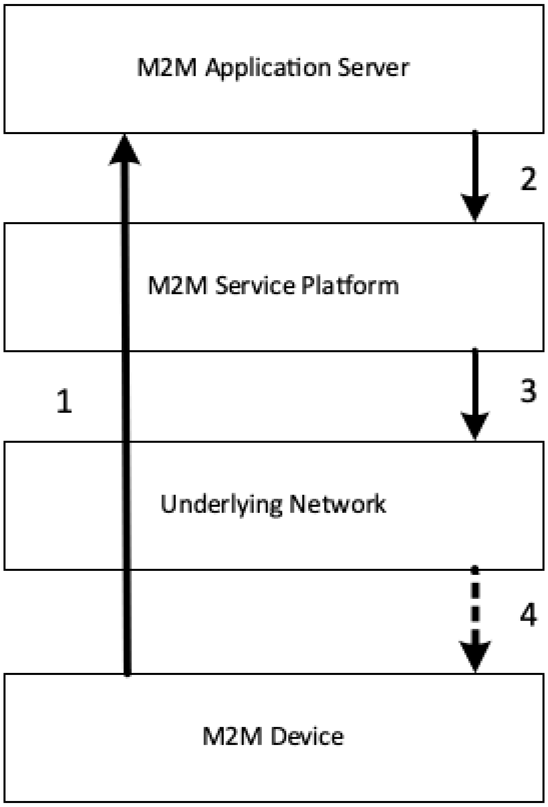


Figure 59: Figure 12.4.6-1 Normal Flow - Optimizing mobility management parameters

12.4.6 Normal Flow

1. The M2M device collects the mobility related M2M information (the engine is off) from sensors within the vehicle and sends it to the application server.
2. The application server gets the mobility related M2M information of the M2M device (the vehicle) and sends the current mobility characteristics (high mobility) based on the mobility related M2M information to the M2M service platform.
3. The M2M service platform detects the change of the mobility characteristics (high mobility->no mobility) of the M2M device based on the current mobility characteristics (high mobility), and sends the current mobility characteristics of the M2M device to the mobile network.
4. The mobile network adjusts configuration parameters of the mobile network about the M2M device based on the current mobility characteristics of the M2M device if necessary.
    - The changed configuration parameters of the mobile network are the traffic area (Wide->Small), the location registration interval (Short->Long).
    - The mobile network may additionally need to adjust configuration parameters in the mobile M2M device.

12.4.7 Alternative Flow

None

12.4.8 Post-conditions

The configuration parameters of the mobile network about the M2M device

- The traffic (paging) area: Small
- The location registration interval: Long

12.4.9 High Level Illustration

12.4.10 Potential Requirements

1. The M2M service platform SHALL be able to provide the Underlying Network with information related to M2M devices that allows optimizations in the Underlying Network with regard to M2M traffic
   An example of such useful information to a cellular network is the current (or change) of the mobility characteristics include moving range (e.g. high mobility, low mobility, no mobility, or speed range), moving direction and moving speed, etc. of the M2M device.
2. How to utilize such information by the cellular network is the cellular operator implementation dependent and outside the scope of oneM2M.
3. The M2M service platform MAY be able to compute the information with which the Underlying Network should be provided by analysing the information received from the M2M application before providing to the

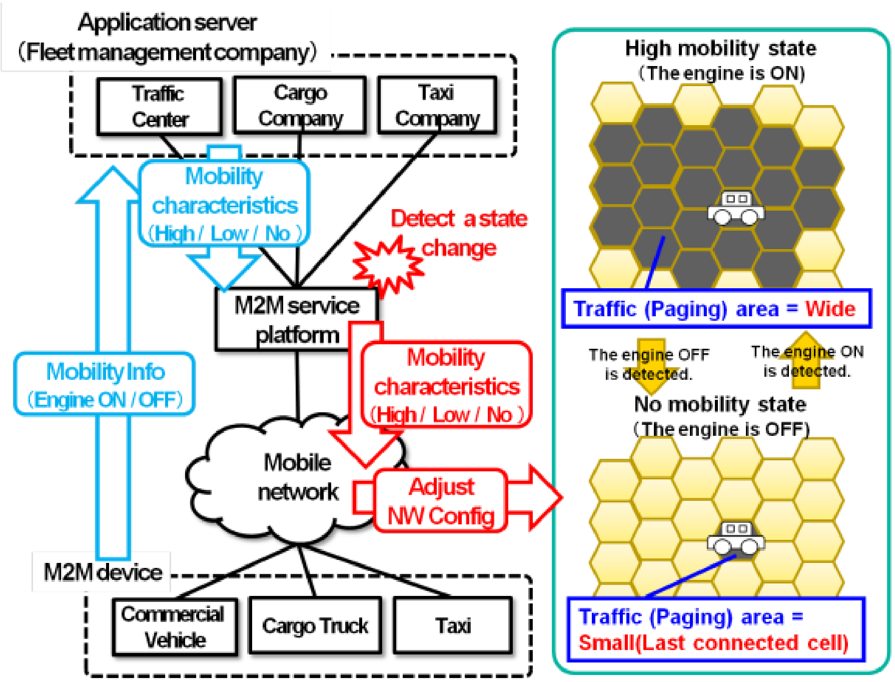

Application server
(Fleet management company)
Traffic Center
Cargo Company
Taxi Company
Mobility characteristics (High / Low / No)
Detect a state change
M2M service platform
Mobility Info (Engine ON / OFF)
Mobility characteristics (High / Low / No)
Mobile network
Adjust NW Config
M2M device
Commercial Vehicle
Cargo Truck
Taxi
High mobility state
(The engine is ON)
Traffic (Paging) area = Wide
The engine OFF is detected.
The engine ON is detected.
No mobility state
(The engine is OFF)
Traffic (Paging) area = Small(Last connected cell)

Figure 60: Figure 12.4.9-1 High Level Illustration - Optimizing mobility management parameters

Underlying Network. >Note: The interface to convey such information to the Underlying Network will depend on the type (e.g. 3GPP, 3GPP2, Fixed) of the Underlying Network.

12.5 Sleepy Nodes

12.5.1 Description

Many e-Health applications involve the use of medical devices which may be connected to a monitoring service. The device user or the user's care providers may periodically need to observe measurements or interact with the device to optimize treatment.

Communications capabilities with multiple entities may be required. For example, communications may be needed between the device and a service/application that collects and analyses the monitored information. In another application communications to allow some control over the device. In one such case the communications may be between the device and the user's care provider(s) and in another case the communication may be with the device manufacturer. Short range communications capability that operates through other devices such as Smartphone or home gateway is assumed to conserve battery life.

One example of such a device is a diabetes management system that includes an insulin pump and a blood glucose monitor.

An insulin pump is used to deliver the insulin. Two types of insulin are commonly used one is fast acting the other slow. The fast acting is usually administered in conjunction with a meal, while the slow acting is used throughout the day.

When and how often the blood glucose level monitor needs to take a reading varies with the daily routine as well as the user's condition.

The need to report the monitored information could vary from an instantaneous reading ordered by the user's care provider to a record of readings at varying intervals over different time periods.

Usually, the monitored information is stored on the device for a period of time before being periodically downloaded. In some cases, the data is sent to a monitoring service, which may perform analysis of the information in preparation for reporting to the user's care providers.

This device can automatically operate the above mentioned functions when needed. Programming of some of these functions can be varied depending on the condition of the user. Sometimes during a daily routine automated operation is preferred (e.g. while traveling or sleeping). Automation is more important for some device users, such as infants, which cannot operate the device manually.

Occasionally, there may be a need to download new firmware to a device to correct a software problem or provide new programming.

The proper functioning of the device is important to maintaining the user's health. The device needs to be operational when needed (i.e. reliable). Optimizing the devices battery life contributes to its reliable functioning. To maximize the life of the device's battery requires putting certain of its functions to sleep for different time intervals (i.e. sleep cycles) when not needed.

Sleep mode device handling is a fundamental issue/requirement for the M2M system. Although there are several requirements in this domain, currently there is no use case clearly addressing this functionality.

12.5.2 Source

oneM2M-REQ-2013-0261R03 Sleepy Node Use Case

12.5.3 Actors

- Sleepy Node (SN)
  A device that spends a large amount of its lifetime disconnected from the network, mainly to save power, or just because it's not capable of storing the energy required for its reliable operation. The device wake up may be based on a variety of methods including but not restricted to: local physical interrupts or triggers, alarms, notifications, etc.
  Sleepy node devices may own and host a set of resources that need to be made available to the other network participants as if it were a typical, always connected device. In some cases low-power, low-range communication technologies (e.g. ZigBee or Bluetooth) may be used to establish connections with relays or gateways capable of longer-range communication (e.g. the user's home Wi-Fi router or smartphone). In this use case several devices used for medical treatment (e.g. insulin pump and blood glucose monitor) embody sleepy node functionality.
- Medical Device Monitoring & Management Service (MDMMS)
  This service periodically collects medical information from the user's monitoring device. Such a service usually provides analysis of the device information for use by medical professionals (e.g. user's care providers). This service can also initiate communication with the device (to send it a command, to re-program it, to update its firmware, etc.). Additional services could be provided to other actors through the collection and analysis of additional information such as device reachability, connection and synchronization requirements, battery status, etc.
- Care Provider (CP)
  Care Providers refers to medical professionals responsible for evaluating and directing treatment for an illness or disease. In this use case the Care Providers are M2M Application Service Providers that interact with the user's medical device. The Care Providers require access to the data provided by the device as well as to applications and functions residing on the device.

- Medical Device Manufacturer (MDM)
  The medical device manufacturer will occasionally require to access and control the device to, for example, download a firmware update or to re-program the device.

12-5-4 Pre-conditions

In this use case the user (e.g. patient) is assumed to be wearing a medical device that operates as a Sleepy Node. However, other similar use cases may involve a medical device that has been surgically implanted within the user, which places an even higher degree of emphasis on its power conservation characteristics. The device has been provisioned for communication using the oneM2M System and is capable of establishing a data connection for communicating with the MDMMS.

12-5-5 Triggers

A variety of triggers might be associated with the overall use case:

- Scheduled transfer of information from SN to MDMMS
- Command from MDMMS to SN (initiated by CP)
- Alarm condition at SN requiring interaction with MDMMS
- Update of SN firmware (by MDMMS or MDM)
- sStatus update or servicing of the SN (by CP, MDMMS or MDM)

To be noted: triggers for device wake up are different than the use case triggers and may be based on a variety of methods such as: local physical interrupts or triggers, alarms, notifications, etc. Communications between SN and the MDMMS may be triggered by either entity.

12.5.6 Normal Flow

- A. Initial setup of SN to MDMMS communications
  1. The device is first installed /powered up.
  2. Network connectivity with the oneM2M System will be established.
  3. Communications between SN and MDMMS are initiated by either entity, depending on individual requirements. Device, capability, service, subscription, user, etc. information is exchanged.
  4. The SN and MDMMS may exchange SN specific information such (power cycles, allowable communication wake-up triggers, etc.)
  5. The device may receive commands from the MDMMS.
  6. The device completes any received commands and communicates status as appropriate.
  7. The device returns to a sleep state.
- B. SN to MDMMS transfer of information
  1. The device wakes up from a sleep cycle. The wake up may occur based on any number of asynchronous events.
  2. The device initiates communication with the MDMMS. Because the device has been in a sleep condition that does not support any network

connectivity, it is possible that a data connection with the oneM2M System will need to be re-established.

3. Once a data connection is established, the device transfers its accumulated information payload to the MDMMS.
4. The device may receive commands from the MDMMS that are either sent directly during the established communication session or have been sent previously and stored in an intermediate node.
5. The device completes any received commands and communicates status as appropriate.
6. The device returns to a sleep state.

- C. Command from MDMMS to SN
    1. Care Provider initiates command to the device (e.g. change in insulin delivery rate) via MDMMS.
    2. MDMMS may schedule delivery of the command based on any relevant scheduling information (such as service and application requirements, notification types, network congestion status, SN power cycle status, SN reachability, etc.). Several commands may be aggregated, ordered or queued and delivered to the SN or an intermediary node.
    3. Command(s) are delivered by the intermediary node or MDMMS to the SN after its wake up.
    4. The device completes any received commands and communicates status as appropriate.
    5. The device returns to a sleep state.
- D. Alarm condition at SN requiring interaction with MDMMS
    1. The device wakes up outside of its sleep cycle due to an alarm condition (e.g. blood glucose levels below a predetermined threshold).
    2. The device initiates communication with the MDMMS. Because the device has been in a sleep condition that does not support any network connectivity, it is possible that a data connection with the oneM2M System will need to be re-established.
    3. Once a data connection is established, the device communicates the alarm condition to the MDMMS.
    4. The device may receive commands from the MDMMS that are either sent directly during the established communication session or have been sent previously and stored in an intermediate node.
    5. The device completes any received commands and communicates status as appropriate, but also maintains the communication session until the alarm condition is cleared or otherwise resolved.
    6. The device returns to a sleep state.
- E. Update of SN firmware
    1. MDMMS is notified by MDM that the device firmware must be updated.
    2. MDMMS schedules the firmware update.
    3. The device wakes up and receives a notification that firmware update is requested. This may require additional action by the user (e.g. plugging the device into a power source during the update process) and

by the MDMMS to establish a communication channel between the MDM and the device to perform the data transfer and/or execute the update process.
4. The device returns to a sleep state.

- F. SN status update or servicing
  1. Various SN status and/or parameters (battery status, reachability state, etc.) are requested via MDMMS
  2. MDMMS notifies the SN.
  3. The device initiates communication with the MDMMS. Because the device has been in a sleep condition that does not support any network connectivity, it is possible that a data connection with the oneM2M System will need to be re-established.
  4. Upon device wake up
- G. The device returns to a sleep state

12.5.7 Alternative Flow

None

12.5.8 Post-conditions

In most cases, the SN will resume sleep as detailed in the flow clause, but the state of wakefulness is determined by other factors such as device, application, service or subscription requirements.

12.5.9 High Level Illustration

None

12.5.10 Potential Requirements

The following is a list of previously submitted requirements with impact on SN functionality, which is now re-submitted for consideration for this scenario.

Table 5: Table 12-1

Temp req. no.	Submitted req. number	Initial submitter	Requirement
SNR-001	HLR-118	Telecom Italia	The M2M System may be aware of the reachability state of the Applications.

Temp req. no.	Submitted req. number	Initial submitter	Requirement
SNR-002	HLR-024	Telecom Italia	The M2M System shall be able to support a variety of different M2M Devices/Gateways types, e.g. active M2M Devices and sleeping M2M Devices, upgradable M2M Devices/Gateways and not upgradable M2M Devices/Gateways.
SNR-003	HLR-055	Telecom Italia	The M2M System should support time synchronization. M2M Devices and M2M Gateways may support time synchronization. The level of accuracy and of security for the time synchronization can be system specific.

Temp req. no.	Submitted req. number	Initial submitter	Requirement
SNR-004	HLR-114	Telecom Italia	The M2M System shall support testing the connectivity towards a selected set of Applications at regular intervals provided the Applications support the function.
SNR-005	HLR-095	Fujitsu	The M2M System shall be able to support a mechanism for delaying notification of Connected Devices in the case of a congested communication network.

Temp req. no.	Submitted req. number	Initial submitter	Requirement
SNR-006	HLR-096	Fujitsu	The M2M System shall be able to support a mechanism to manage a remote access of information from other Connected Devices. When supported the M2M system shall be able to aggregate requests to perform the request depending on a given delay and/or category e.g. the M2M application does not have to connect in real time with the devices.
SNR-007	HLR-097	Telecom Italia	The M2M System may support a mechanism for delaying notifying a Connected Objects.

Temp req. no.	Submitted req. number	Initial submitter	Requirement
SNR-008	HLR-098	Telecom Italia	The M2M System may support a mechanism to manage a remote access of information from Applications and shall be able to aggregate requests and delay to perform the request depending on a given delay and/or category.
SNR-009	HLR-115	Telecom Italia	The Applications and their resources operational status shall be monitorable.
SNR-010	HLR-161	ALU, Huawei	The M2M System shall be capable of retrieving information related to the environment (e.g. battery, memory, current time) of a M2M Gateway or Device

Informative annex to Potential Requirements

Requirements TS content related to Sleepy Node functionality

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-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-015
The M2M system shall support different communication patterns including infrequent communications, small data transfer, large file transfer, streamed communication.

MGR-001
M2M System shall support management and configuration of resource constrained devices.

Other agreed requirements related to Sleepy Node functionality

(HLR-005)
The M2M System shall support M2M applications accessing the M2M system by means of a non-continuous connectivity.

(HLR-006)
The M2M System shall be able to manage communication towards a device which is not continuously reachable.

(HLR-047)
The M2M System shall be able to manage the scheduling of network access and of messaging.

(HLR-137)
The M2M System shall provide the capability to notify M2M Applications of the availability of, and changes to, available M2M Application/management data on the M2M Device/Gateway, including changes to the M2M Area Network.

12.6 Collection of M2M System data

12.6.1 Description

M2M Service Providers have a need to provide the Application Service Providers with data and analysis related to the behavior of the M2M System as well as the service provider supplied components of the M2M System (e.g. Device Gateway) M2M Operators face two problems.

M2M Service Providers can utilize the methods of Big Data by collecting M2M System data for the behavior of the M2M System as well as data from M2M System components provided by the Service Provider.

In this scenario, the data is collected from M2M Gateways and Devices provided by the M2M Service Provider. The M2M System data that is collected from the M2M Devices and Gateways can be described as:

- M2M System Behavior

- Component Properties

M2M System Behavior: Data related to the operation of the M2M Applications within the M2M System.

Types of data that is to be collected includes information related Messages transmittal and reception (e.g. bytes, response times, event time).

Component Properties: Data related to the Service Provider supplied components as the component is in use by the M2M System (e.g. location, speed of the component, other anonymous data).

With this data, the M2M Service Provide can provide:

1. Analysis of the data without knowledge of content of the Application's data.
2. Insights into the operation of the M2M Applications. For example, the M2M Service Provider can infer the "correct" state of the application or the network status changes, by the analysis of the data, and then trigger some kinds of optimization mechanisms.

12.6.2 Source

oneM2M-REQ-2013-0279R04 Collection of non-application data

12.6.3 Actors

- Front-end data-collection equipment (e.g. M2M Devices and Gateways) :
- Management Platform (e.g. M2M Service Provider's Platform)
- Monitor Centre (e.g. M2M Application's Platform)
- M2M System Data Collection Centre

12.6.4 Pre-conditions

None

12.6.5 Triggers

- Time trigger: collecting data at a specific time;
- Position trigger: collecting data when position changed;
- Behavior trigger: collecting data when certain behavior happened

12.6.6 Normal Flow

1. The M2M Device and Gateway collects M2M System data.
2. Once a trigger is activated, the M2M Devices and Gateway sends the M2M System data to the M2M System Data Collection Centre.

12.6.7 Alternative Flow

None

12.6.8 Post-conditions

None

12.6.9 High Level Illustration

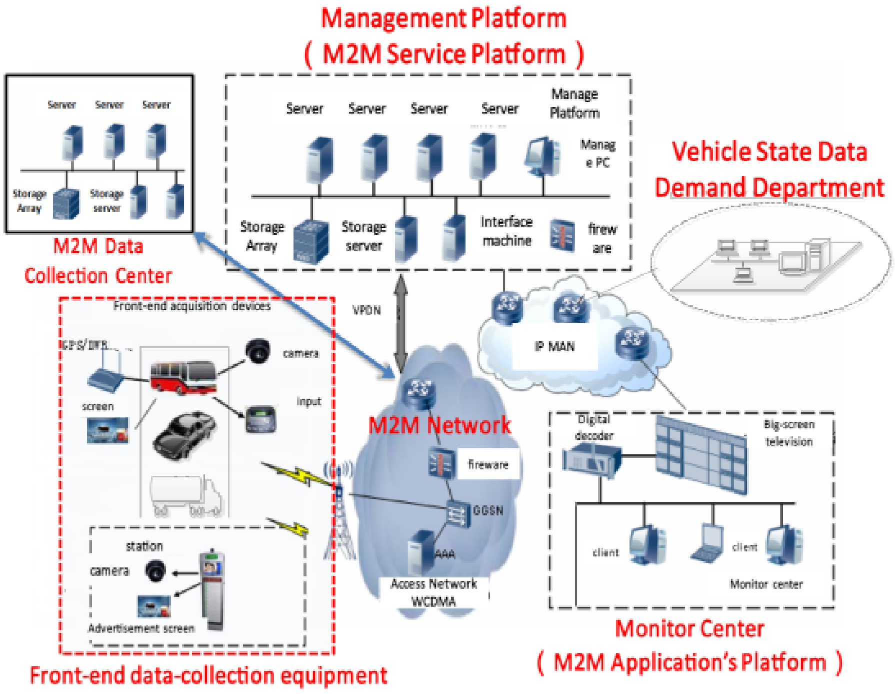


Figure 61: Figure 12.6.9-1 Vehicle Operation Management System

- Vehicle Operation Management System provide users a new telecommunications business with remote collection, transmission, storage, processing of the image and alarm signals.
- Front-End Data Collection Equipment include Front-End 3G camera, Electronic Station, Car DVR, costumed car GPS, WCDMA wireless routers and other equipment.
- Management Platform with business management function, include:
  - Forwarding, distribution, or storage of images
  - Linkage process of alarms
  - Management and maintenance of the vehicle status data.

- Monitor Centre: consists of TV wall, soft / hardware decoder, monitor software, etc.
- Vehicle State Data Demand Department: such as auto 4S shop, vehicle repair shop, vehicle management centre, automobile and parts manufacturers, government regulatory platform, etc.
- M2M System Data Collection Centre: use built-in data collectors resided in Network Equipment, M2M Platform, Costumed M2M Modules and Costumed M2M Terminal Devices to collect M2M System data.

12.6.10 Potential Requirements

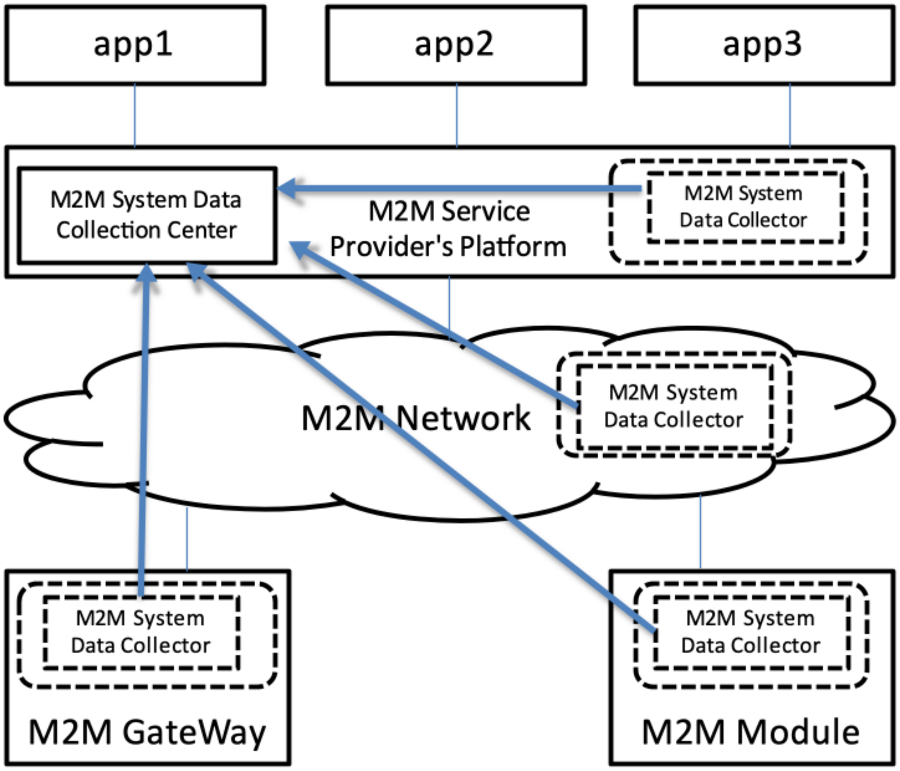

app1
app2
app3
M2M System Data Collection Center
M2M Service Provider's Platform
M2M System Data Collector
M2M Network
M2M System Data Collector
M2M System Data Collector
M2M GateWay
M2M System Data Collector
M2M Module

Figure 62: Figure 12.6.10-1 M2M System Data Collection Processing Flow

1. M2M System should support M2M System data collection.
   As illustrated in Figure 12.6.10-1, we suggest that M2M System data collector should reside in:
   - M2M Service Providers' Platform
   - M2M Network Equipment
   - M2M Devices and Gateways
   - M2M Communication Module

12.7 Leveraging Broadcasting/ Multicasting Capabilities of Underlying Networks

12.7.1 Description

This use case illustrates that an automotive telematics (Application) service provider XYZ Ltd. alerts vehicles around where a traffic accident has just happened. The alerted vehicles could go slow or go another route to prevent a second accident and to avoid the expected traffic jam.

In this case, the automotive telematics service provider XYZ Ltd. takes advantage of broadcasting/multicasting capability of underlying communication networks. Some kinds of communication networks (in particular, a mobile communication network) have the capability to broadcast/multicast a message in specific areas. Utilizing this capability, XYZ Ltd. can alert at once all the relevant vehicles within a specific region. This approach can avoid burst traffic in the communication network and provides a simple and cost-efficient way for XYZ Ltd. to implement this neighbourhood alerting mechanism.

> Note: Ordinary unicast messaging mechanism is inadequate here. The alert messages shall be delivered in a timely manner to all the relevant vehicles within a specific region. XYZ Ltd. therefore needs to select the relevant vehicles that should receive the alert messages according to their current registered location (It needs continuous location management of vehicles). Moreover the underlying communication network has to route large number of unicast messages with very short delay.

However it is hard for XYZ Ltd. to utilize broadcasting/multicasting functionality of underlying networks directly which can vary with kinds of communication networks (e.g. 3GPP, 3GPP2, WiMAX or Wi-Fi).

A oneM2M service provider ABC Corp. facilitates this interworking between XYZ Ltd. and a variety of communication network service providers (or operators). ABC Corp. exposes unified/standardized interfaces to utilize broadcasting (or multicasting) capability of communication networks. ABC Corp. authenticates the requester (=XYZ Ltd.), validates and authorizes the request, then calls the corresponding function of the appropriate communication networks.

> Note: There are many other scenarios in which broadcasting/multicasting capability of underlying communication networks provides significant benefit in a M2M system. For example,
> - Warning about a crime incident - When a security firm detects a break-in at a house, it sets off all neighbourhood burglar alarms and alerts the M2M Application on the subscribed users' cellular phones around there. - Monitoring a water delivery system - When a water-supply corporation detects a burst of a water pipe, it remotely shuts off the water supply valves in that block, and alerts the M2M Application on the subscribed users' cellular phones around there.

The potential requirements in this contribution cover the above and all similar use cases, too.

12.7.2 Source

oneM2M-REQ-2013-0260R02 Leveraging Broadcasting - Multicasting Capability of Underlying Networks

12.7.3 Actors

- The automotive telematics service provider: XYZ Ltd.
  It provides automotive telematics service as a M2M application.
- The oneM2M service provider: ABC Corp.
  It provides a common platform to support diverse M2M applications and services.
- The communication network service providers (or operators): AA Wireless, BB Telecom and CC Mobile
  They operate communication networks.
  Some of them have the capability to broadcast/multicast a message in specific areas. The broadcasting/multicasting capability is available for external entities.
- The vehicles:
  They have communication capability as M2M devices, and have user interfaces (e.g. displays, audio speakers) or actuators to control driving.

  Note: roles are distinct from actors. For example, the oneM2M service provider role may be performed by any organization that meets the necessary standardization requirements, including MNOs.

12.7.4 Pre-conditions

The vehicles are able to communicate in one or more communication networks.

12.7.5 Triggers

The automotive telematics service provider XYZ Ltd. detects a traffic accident. How it detects the accident and captures details of the accident is out of scope of this use case.

12.7.6 Normal Flow

1. XYZ Ltd. estimates the location and impact of the accident to specify the area in which all the relevant vehicles should be alerted.
2. XYZ Ltd. requests oneM2M service provider ABC Corp. to alert subscribed vehicles in the specified area.
   - That request encapsulates the alert message (payload) and alert parameters (options).

    - The request contains the payload to be delivered to vehicles. It can contain for example the alert level (how serious and urgent), the location and time of the accident, and directions to the driver (e.g. go slow or change routes).
    - The request also defines targeted receivers of the message and specifies alert options. They can contain for example the area to be covered, the type of devices to be alerted, the option whether the alerting should be repeated, the repetition interval, and stopping conditions.

3. ABC Corp. receives the alert request from XYZ Ltd. It authenticates the requester (=XYZ Ltd.), validates and authorizes the request. When the request from XYZ Ltd. does not have alert parameters, ABC Corp. analyses the alert message to determine broadcast parameters. Then it chooses appropriate communication network service providers (or operators) to meet the alert request from XYZ Ltd.
4. ABC Corp. requests AA Wireless and CC Mobile to broadcast the alert message in the specified area.
    - That request encapsulates the alert message (payload) and broadcast parameters.
        - The alert message is the payload to be delivered to vehicles. The contents are the same as from ABC Corp. but the format and encoding of the message may be different from AA Wireless and CC Mobile.
        - The broadcast parameters define targeted receivers of the message and specify broadcast options. They can contain for example the area to be covered, the type of devices to be alerted, the option whether the broadcast should be repeated, the repetition interval, and stopping conditions. The format of the parameters can be different between AA Wireless and CC Mobile.

    ABC Corp. may need to cover a part of the broadcasting functions for some communication network service providers. For example, if CC Mobile does not have the functionality to repeat broadcasting periodically, ABC Corp. repeatedly requests CC Mobile to broadcast the message, in order to meet the request from XYZ Corp.

12.7.7 Alternative Flow

None

12.7.8 Post-conditions

The vehicles around where the traffic accident has just happened are properly alerted about the accident.

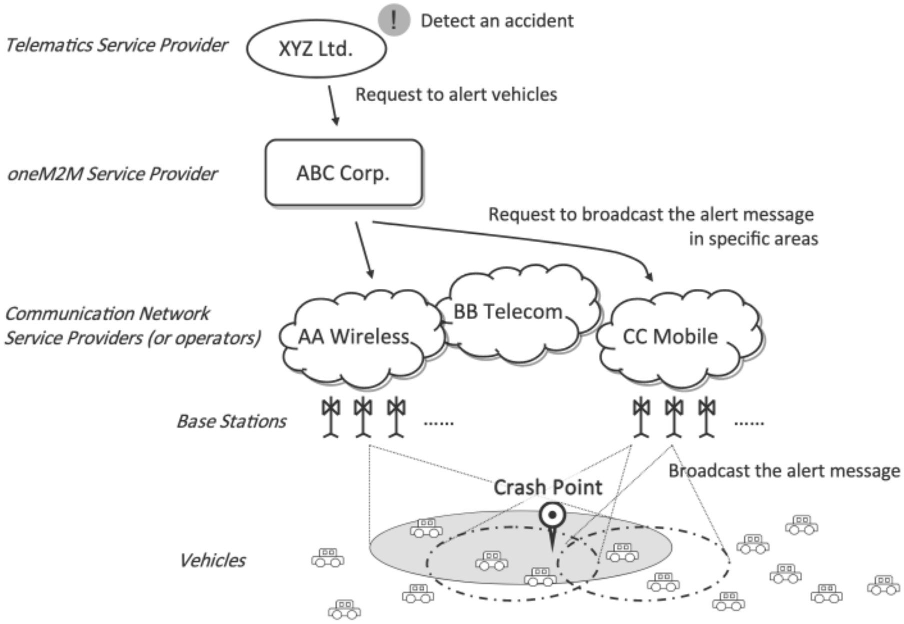

Detect an accident
Telematics Service Provider
XYZ Ltd.
Request to alert vehicles
oneM2M Service Provider
ABC Corp.
Request to broadcast the alert message in specific areas
Communication Network Service Providers (or operators)
AA Wireless
BB Telecom
CC Mobile
Base Stations
......
......
Broadcast the alert message
Crash Point
Vehicles

Figure 63: Figure 12.7.9-1 High level illustration 1

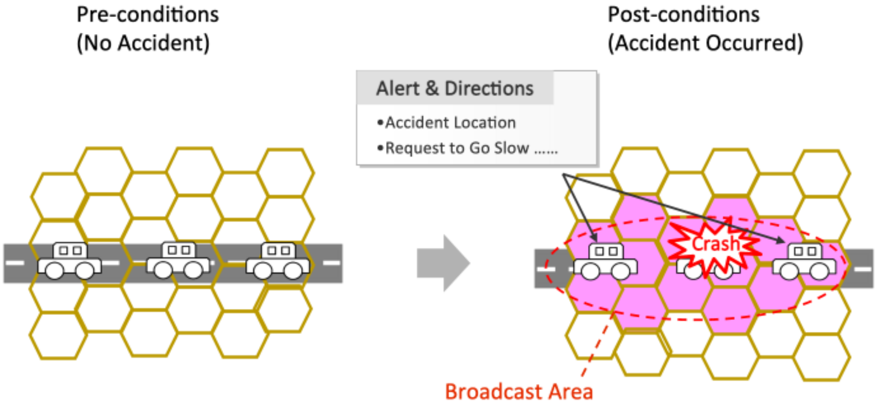


Figure 64: Figure 12.7.9-2 High Level Illustration 2

12.7.9 High Level Illustration

12.7.10 Potential Requirements

1. oneM2M System SHALL be able to leverage broadcasting and multicasting capability of Underlying Networks.
2. oneM2M System SHALL enable a M2M Application to request to broadcast/multicast a message in specific geographic areas.
    - That request SHALL encapsulate the message (payload) from the M2M Application, relevant parameters (options) and optionally credentials for authentication and authorization.
    - The M2M System SHALL support that request to be independent of the types of the Underlying Networks.
3. oneM2M System SHALL support mechanisms for Authentication, Authorization and Accounting of an M2M Application to request to broadcast/multicast a message.
    - oneM2M System SHALL authenticate the M2M Application.
    - oneM2M System SHALL validate and authorize the request.
    - oneM2M System SHALL support accounting on handling the request.
4. oneM2M System SHALL be able to select appropriate underlying networks to broadcast/multicast a message in specified geographic areas according to capability/functionality of those networks.
5. oneM2M System SHALL be able to receive information on broadcasting/multicasting capability/functionality of each underlying network.
6. oneM2M System SHALL be able to indicate towards the Underlying Network that a message needs to be broadcasted/multicasted and to determine its broadcast parameters (or multicast parameters), e.g. the area to be covered, the type of devices to be alerted, the option whether the broadcast should be repeated, the repetition interval, and stopping conditions.
7. oneM2M System SHALL be able to analyse a message from a M2M Application to determine broadcast parameters.
8. Interfaces to address the above requirements SHALL be standardized by oneM2M.

    Note: roles are distinct from actors. An actor may play one or more
    roles and the economic boundary conditions of a particular market
    will decide which role(s) will be played by a particular actor.

12.8 Leveraging Service Provisioning for Equipment with Built-in M2M Device

12.8.1 Description

Some industrial equipment is so complicatedly designed that it’s difficult for users themselves to maintain, such as construction engineering equipment, air compressor, large medical instrument and so on. Vehicles with online service can also be seen as one kind of such equipment. Therefore, equipment vendors build back-end applications to monitor and maintain them remotely. They also collect data from them for analysis in order to improve service level and product quality. We call such service provided by equipment providers as “equipment remote maintenance service”.

Equipment providers can integrate remote communication unit into equipment directly. But often, they get M2M device from other providers, which mainly provide remote communication capability. They embed one M2M device into one equipment.

More and more equipment begin to use mobile network to communicate with the back-end application because of the convenience and low-cost of the current mobile network. In this case, SIM Card or UIM Card should be put into the M2M device. epic [i.16] can be one of the best choices.

This contribution mainly focuses on M2M service provisioning in the above case. M2M service consists of the service provided by M2M service platform and network service provided by the mobile network. Therefore, full M2M service provisioning consists of M2M service provisioning and network service provisioning. The former is to allow M2M device to talk with M2M service platform. The latter is to make M2M device access mobile network.

M2M service platform is operated by M2M Service Providers (M2M SP). With M2M SP’s help, Equipment Providers don’t need to manage mobile-network specific identifiers, such as IMSI, MSISDN or MDN. They just use Equipment ID / Equipment Name and Device ID / Device Name to identify equipment and device. M2M Service Platform can hide the complexity of the underlying mobile network.

For devices managed by M2M Service platform, there are two kinds of M2M Service status. One is administrative status. The other is operational status. The former is to tell whether M2M Service has been allowed to be running by M2M SP for a device. “active” means it’s allowed. “de-active” means it’s not allowed. The latter is to tell whether M2M Service is available now for a device. “available” means it function correctly now. “unavailable” means it doesn’t function correctly now. For example, if related IMSI has been deactivated by MNO, M2M Service operational status of the device is unavailable.

For network identifiers, Network Service administrative status is to tell whether network service has been allowed to be running for a network identifier by MNO. “active” means it’s allowed. “de-active” means it’s not allowed.

12.8.2 Source

oneM2M-REQ-2013-0171R03 M2M Service Provisioning for Equipment with Built-in M2M Device

12.8.3 Actors

- Equipment Provider (EP)
  Vendors who make equipment with built-in remote communication capability, sell and install equipment, and provide equipment remote maintenance service
- Equipment User
  Customers who use equipment
- M2M Device Provider (M2M DP)
  Vendors who make M2M Device with built-in remote communication capability and other M2M service capability
- M2M Service Provider (M2M SP)
  Service provider who provide M2M service which including network service
- Mobile Network Operator (MNO)
  Service provider who provide mobile network service
- Equipment Provider Back-end Application (EPBA)
  One kind of M2M Applications by which EPs can monitor, control, and collect data from their equipment. It is normally located in EP's office.
- M2M Service Platform (MSP)
  Platform which is operated by M2M SP and provides M2M Service
- Equipment
  It is made by EP, which can do some specific work in some specific areas, such as concrete machinery, hoisting machinery and air compressor.
- M2M Device
  Device embedded into equipment, which serves the function of communication between equipment and EPBA. It also talks with MSP to use M2M service.

12.8.4 Pre-conditions

Equipment User uses equipment remote maintenance service provided by EP.

Equipment Provider uses M2M Service provided by M2M SP.

M2M Service provided by M2M SP includes Network Service. That is to say, M2M service provider chooses which MNO's network to be used.

12.8.5 Triggers

None.

12.8.6 Normal Flow

Equipment's lifetime can be summarized as following figure:

M2M service provisioning for equipment with built-in M2M device mainly consists of the following scenarios:

- Pre-provisioning Scenario

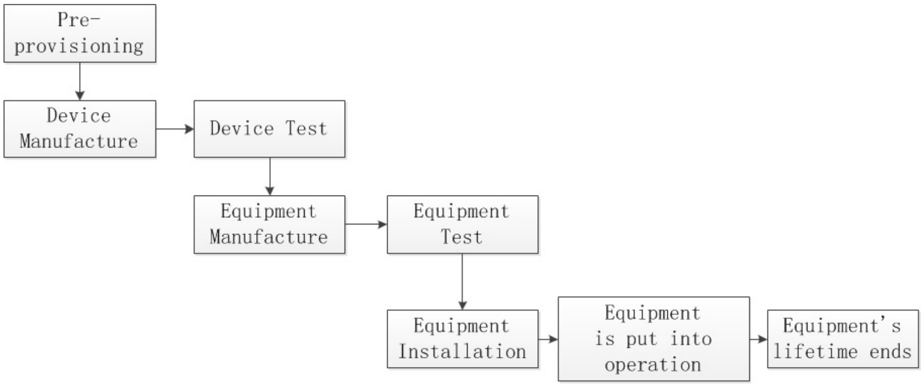


Figure 65: Figure 12.8.6-1 Equipment lifetime

- Manufacture and Test Scenario
- Installation Scenario
- EP Suspends / Resumes / Stops Equipment Remote Maintenance Service Scenario
- M2M SP Suspends / Resumes M2M Service Scenario
- MNO Suspends / Resumes Network Service Scenario
- Replacing-device Scenario

1. Pre-provisioning Scenario
   At first, M2M SP prepares a batch of SIM/UIM cards from MNOs and registers the information of these cards in MSP, such as ICCID, IMSI and so on

2. Manufacture and Test Scenario
   Device Manufacture Phase: M2M DP gets SIM/UIM card from M2M SP, and puts it into the module, and integrates the module into the device. Then, M2M DP configures the device ID parameter in device.
   Device Test Phase: After that, M2M DP tests the device. Before and after the test, M2M DP or M2M SP sets M2M Service administrative status of specific ICCID as “active” or “de-active”, which allows MSP to talk with underlying mobile network to activate or deactivate the network service administrative status of the corresponding IMSI. In the test process, M2M Device reports its device ID and ICCID/IMSI to MSP. Thus, MSP knows such binding info.
   Equipment Manufacture Phase: After that, EP gets the device and puts it into their equipment. Then, EP configures the equipment ID parameter in device.
   Equipment Test Phase: EP also tests the equipment. Before and after the test, EP or M2M SP sets the M2M Service administrative status of specific device as “active” or “de-active”, which allows MSP to talk with underlying mobile network to activate or deactivate the network service administrative

status of the corresponding IMSI. In the test process, Equipment reports its device ID and equipment ID to EPBA.

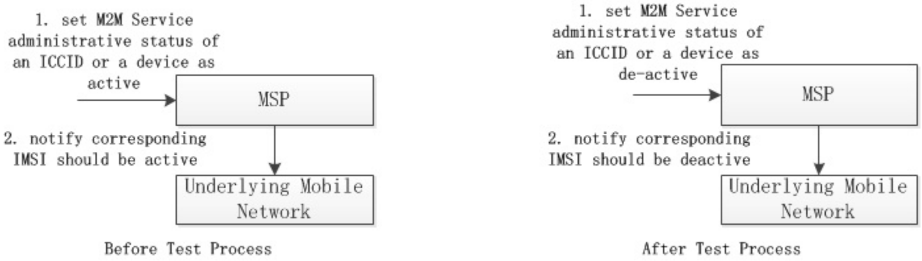

1. set M2M Service administrative status of an ICCID or a device as active
MSP
2. notify corresponding IMSI should be active
Underlying Mobile Network
Before Test Process
1. set M2M Service administrative status of an ICCID or a device as de-active
MSP
2. notify corresponding IMSI should be deactive
Underlying Mobile Network
After Test Process

Figure 66: Figure 12.8.6-2 Manufacture and Test Scenario

Figure 12.8.6-2 Manufacture and Test Scenario

3. Installation Scenario
   Before the installation, EP sets equipment remote maintenance service of specific equipment as “active”, and it talks with MSP to set M2M service administrative status of the corresponding device as “active”, and which also allows MSP to notify underlying mobile network to set network service administrative status of the corresponding IMSI as “active”. Then, EP continues to install the equipment. After that, the equipment can be put into operation.

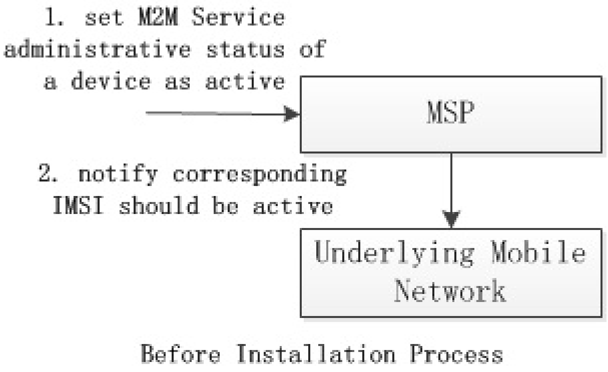

1. set M2M Service administrative status of a device as active
MSP
2. notify corresponding IMSI should be active
Underlying Mobile Network
Before Installation Process

Figure 67: Figure 12.8.6-3 Installation Scenario

Figure 12.8.6-3 Installation Scenario

4. EP Suspends / Resumes / Stops Equipment Remote Maintenance Service Scenario
   EP may suspend, resume, or stop equipment remote maintenance service of specific equipment. For suspending and resuming scenario, EP sets equipment remote maintenance service of specific equipment as “de-active”

or “active”, which may trigger MSP to set M2M service administrative status of the corresponding device as “de-active” or “active”, and which also may trigger MSP to notify underlying mobile network to set network administrative status of the corresponding IMSI as “de-active” or “active”. But, in some cases, the above administrative statuses don’t correlation together. It’s up to different business model and management policy.

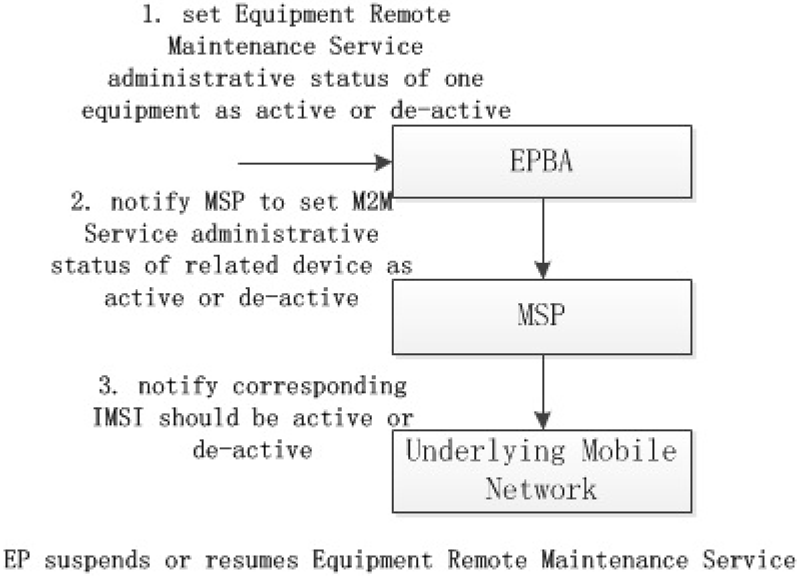

1. set Equipment Remote Maintenance Service administrative status of one equipment as active or de-active
EPBA
2. notify MSP to set M2M Service administrative status of related device as active or de-active
MSP
3. notify corresponding IMSI should be active or de-active
Underlying Mobile Network
EP suspends or resumes Equipment Remote Maintenance Service

Figure 68: Figure 12.8.6-4 EP Suspends / Resumes / Stops Equipment Remote Maintenance Service Scenario

Figure 12.8.6-4 EP Suspends / Resumes / Stops Equipment Remote Maintenance Service Scenario

For stopping scenario, EP sets equipment remote maintenance service of specific equipment as “stopped”, which may trigger MSP to set M2M service administrative status of the corresponding device as “stopped”, and which also may trigger underlying mobile network to reclaim the corresponding IMSI.

5. M2M SP Suspends / Resumes M2M Service Scenario
   M2M SP may suspend or resume M2M service of specific device, which may let MSP talk with underlying mobile network to deactivate or activate network service administrative status of the corresponding IMSI. After that, MSP should notify EPBA of such M2M service administrative status change of the device if EPBA has registered such notification, which allows EPBA to do some operations.

   Figure 12.8.6-5 SP Suspends / Resumes M2M Service Scenario

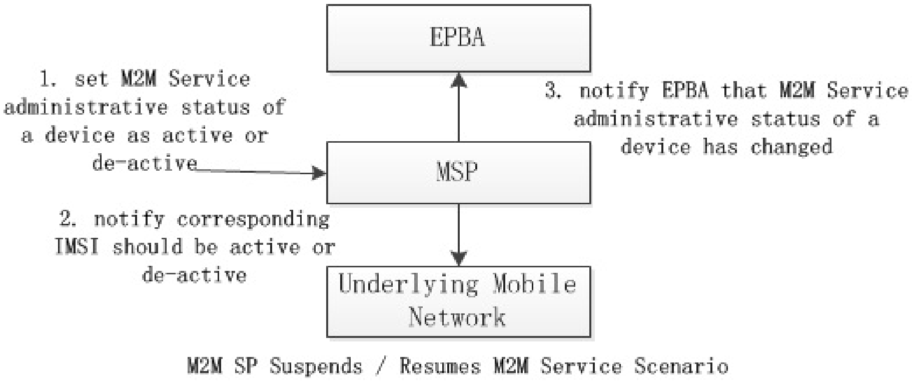

EPBA
1. set M2M Service administrative status of a device as active or de-active
3. notify EPBA that M2M Service administrative status of a device has changed
MSP
2. notify corresponding IMSI should be active or de-active
Underlying Mobile Network
M2M SP Suspends / Resumes M2M Service Scenario

Figure 69: Figure 12.8.6-5 SP Suspends / Resumes M2M Service Scenario

6. MNO Suspends / Resumes Network Service Scenario
   MNO may suspend or resume network service of specific IMSI. If that happens, underlying mobile network may notify MSP the change of specific IMSI. Then, MSP may change the M2M service operational status of the corresponding device to "unavailable" or "available". After that, MSP may also notify EPBA of the M2M service operational status change of the corresponding device if EPBA has registered such notification.

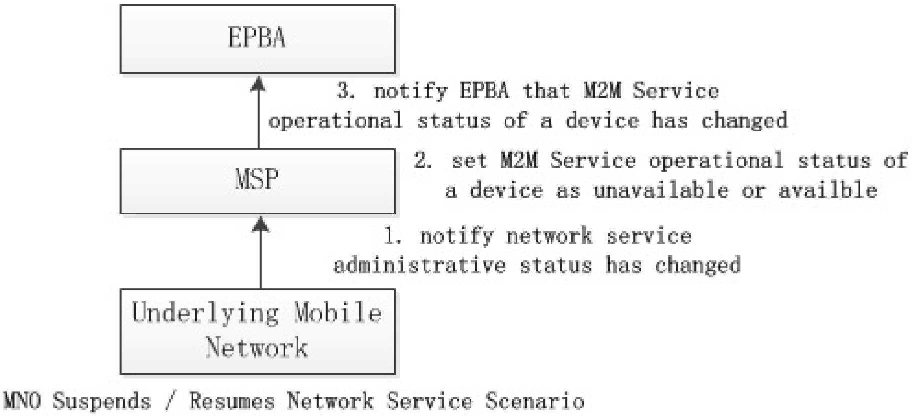

EPBA
3. notify EPBA that M2M Service operational status of a device has changed
MSP
2. set M2M Service operational status of a device as unavailable or availble
1. notify network service administrative status has changed
Underlying Mobile Network
MNO Suspends / Resumes Network Service Scenario

Figure 70: Figure 12.8.6-6 MNO Suspends / Resumes Network Service Scenario

Figure 12.8.6-6 MNO Suspends / Resumes Network Service Scenario

7. Replacing-device Scenario
   In some cases, EP may decide to replace bad device with new one in the equipment. EP sets equipment remote maintenance service of specific equipment as "replaced", which triggers MSP set M2M service administra-

tive status of the corresponding device as “stopped”, which also may trigger MSP to notify underlying mobile network to reclaim the corresponding IMSI.
The following procedure is the same as the Equipment Manufacture Phase in Manufacture and Test Scenario

12.8.7 Alternative Flow

None

12.8.8 Post-conditions

None

12.8.9 High Level Illustration

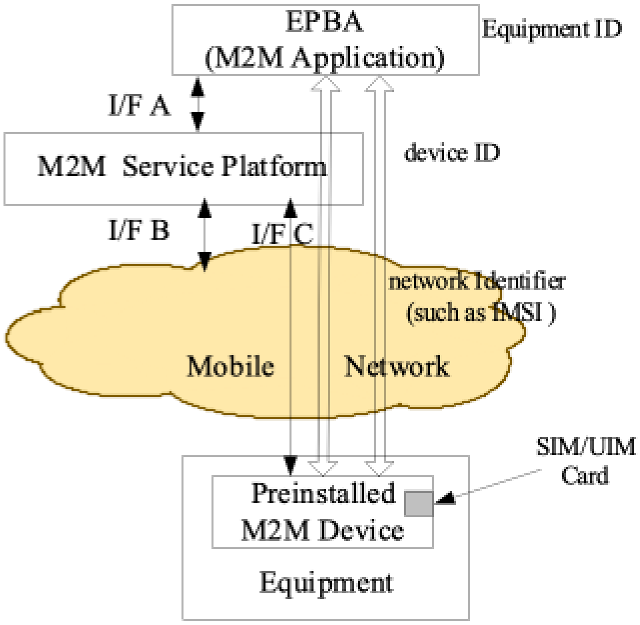


Figure 71: Figure 12.8.9-1 High Level Illustration

Service Model

Equipment Provider (EP) provides equipment remote maintenance service to Equipment User. M2M SP provides M2M service to EP. MNO provides network service to M2M SP.

Equipment remote maintenance service consists of M2M service which is provided by M2M SP and other service provided by EP.

M2M service consists of network service which is provided by MNO and other service provided by M2M SP. M2M service operational status will be de-active if network service administrative status is de-active.

Entity Model

EPBA uses equipment ID to identify specific equipment.

EPBA and MSP uses device ID to identify specific device. MSP and underlying mobile network use network identifier such as IMSI, MSISDN, MDN or External id to identify specific user in its network.

One equipment has only one M2M device in it at one time. EP can replace old M2M device in equipment with new one.

One M2M device has only one SIM/UIM card in it.

12.8.10 Potential requirements

1. The M2M System shall identify and manage M2M Service status of devices.

   > Note: There are two kinds of M2M Service status. One is administrative status. The other is operational status. The former is to tell whether M2M Service has been allowed to be running by M2M SP for a device. "active" means it's allowed. "de-active" means it's not allowed. The latter is to tell whether M2M Service is available now for a device. "available" means it function correctly now. "unavailable" means it doesn't function correctly now. For example, if related IMSI has been deactivated by MNO, M2M Service operational status of the device is unavailable.

2. The M2M System should identify Network Service administrative status of device-related network identifiers such as IMSI, MSISDN, MDN, or External id.

3. > Note: Network Service administrative status is to tell whether network service has been allowed to be running for a network identifier by MNO. "active" means it's allowed. "de-active" means it's not allowed. The M2M System should support the correlation of service identifier of a device in service layer and related mobile network identifier such as IMSI, MSISDN, MDN, or External id in underlying network layer.

   > Note: Different MNOs may expose different kinds of network identifiers to the M2M System. It's up to MNO.

4. System should notify underlying mobile network that Network Service administrative status of related mobile network identifier should be changed when M2M Service administrative status of a device changes if underlying mobile network can receive such notification and has subscribed such notification.

5. The M2M System shall notify M2M Application when M2M Service administrative status of a device changes if M2M Application has subscribed such notification. The M2M System should notify M2M Application when M2M Service operational status of a device changes if M2M Application has subscribed such notification.
6. The M2M System should change M2M Service operational status of the corresponding device to available or unavailable when it receives the notification from the underlying mobile network that Network Service administrative status of a mobile network identifier has changed to active or de-active, if the underlying mobile network can send such notification to the M2M System.
7. The M2M System should support M2M Application to activate or deactivate M2M Service administrative status of a device.

12.9 Semantics query for device discovery across M2M Service Providers

12.9.1 Description

This use case describes discovery of a device based on metadata of the device such as the type of device or its location. It is similar to the use case "Use Case on Devices, Virtual Devices and Things" in clause 8.2 however in the present use case the discovery may be extended to the domains of different M2M service providers.

12.9.2 Source

REQ-2014-0005R01 Semantics query for device discovery across M2M Service Providers

12.9.3 Actors

- M2M Application Provider
  The M2M Application Provider provides an application which can employ a device that has already been installed and is operated by a different M2M Application Provider. However, the M2M Application Provider does not have any information (ID, URI, etc.) that can identify the device, the M2M service provider and the M2M Application Provider which the device belongs to.
- M2M Service Provider 1
  M2M Service Provider 1 is a service provider with whom the M2M Application Provider has a contractual relationship.
- M2M Service Provider 2
  M2M Service Provider 2 is a service provider with whom the M2M Application Provider does not have a contractual relationship. The M2M Service Infrastructure of M2M Service Provider 1 can communicate with the M2M

Service Infrastructure of M2M Service Provider 2 via an inter-provider interface.

- The device which M2M Application Provider wants to employ is connected to M2M Service Provider 2.

12.9.4 Pre-conditions

An M2M Device (e.g. a surveillance camera in a public space, a thermometer for agriculture in a field, etc.) has been installed and is operated in the domain of M2M Service Provider 2.

The M2M Application Provider has found the device in the real world (in the public space, the agriculture field, etc.) and wants to make use of the device within his application. The M2M Application Provider, however, does not have any information (ID, URI, etc.) that can identify the device. Further, the M2M Application Provider does not know which M2M Service Provider the device belongs to.

The M2M Application Provider has a contractual relationship with M2M Service Provider 1.

M2M Service Providers 1 and 2 have databases that contain information on their devices. The databases include location information (where each device is currently located) and the device type.

12.9.5 Triggers

Using a suitable interface (e.g. a web-page) of the M2M Application the M2M Application Provider creates a request for using the device. The request contains location information about the device and possibly a device type.

12.9.6 Normal Flow

0. The M2M Application launches a query within the domain of M2M Service Provider 1 to find and identify the device. The query is invoked with location information on the device and information on the device type.
1. The database of M2M Service Provider 1 is searched whether the requested device is connected to his domain or not.
2. If the requested device is connected to M2M Service Provider 1, M2M Service Provider 1 returns to the M2M Application the information to identify the device (ID, URI, etc.) and terms of use for the device.
3. If the requested device is not connected to M2M Service Provider 1 then M2M Service Provider 1 forwards the query to other M2M Service Providers to which M2M Service Provider 1 has an inter-provider system interface. Forwarding may depend on whether some criteria of the query are known to be supported / not supported by a certain Service Provider (e.g. if it is known that the devices of a Service Provider only operate in a certain geographical region and the query looks for a device in a different region).

4. The query is executed in the domains of the other M2M Service Providers.
5. If the requested device is connected to M2M Service Provider 2 then M2M Service Provider 2 returns to M2M Service Provider 1 the information to identify the device (ID, URI, etc.) and terms of use for the device.
6. M2M Service Provider 1 returns to M2M Application Provider the information to identify the device (ID, URI, etc.) and terms of use.

12.9.7 Alternative Flow

None

12.9.8 Post-conditions

M2M Application Provider can start to employ the device on the basis of the terms of use sent by M2M Service Provider 1.

12.9.9 High Level Illustration

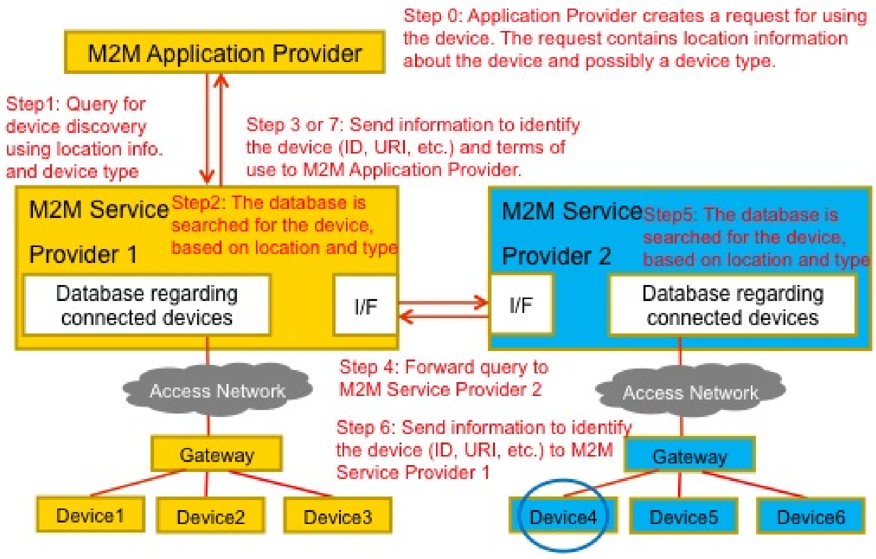

M2M Application Provider
Step 0: Application Provider creates a request for using the device. The request contains location information about the device and possibly a device type.
Step1: Query for device discovery using location info. and device type
Step 3 or 7: Send information to identify the device (ID, URI, etc.) and terms of use to M2M Application Provider.
M2M Service Provider 1
Step2: The database is searched for the device, based on location and type
Database regarding connected devices
I/F
M2M Service Provider 2
Step5: The database is searched for the device, based on location and type
I/F
Database regarding connected devices
Step 4: Forward query to M2M Service Provider 2
Step 6: Send information to identify the device (ID, URI, etc.) to M2M Service Provider 1
Access Network
Access Network
Gateway
Gateway
Device1
Device2
Device3
Device4
Device5
Device6

Figure 72: Figure 12.9.9-1 High Level Illustration of Semantics discovery across M2M Service Providers

12.9.10 Potential Requirements

The following requirements extend the requirement SMR-004 from clause 6.3.2 (Semantic Requirements) of [i.16]:

SMR-004: The M2M System shall provide capabilities to discover M2M Resources based on semantic descriptions.

1. The M2M System shall provide a capability to an M2M Application to search (semantic query) within the domain of the application's M2M Service Provider to discover M2M Devices, Virtual Devices and Things on the basis of their semantic descriptions and meta-data such as device location or a device type.
2. The M2M System shall provide a capability to a M2M Service Provider to automatically forward such a semantic query via standardized inter-provider interfaces to the domains of other M2M Service providers in order to extend the search to these domains.

   Note: Based on Service Provider's policies forwarding can depend on whether some criteria of the query are known to be supported / not supported by a certain Service Provider (e.g. if it is known that the devices of a Service Provider only operate in a certain geographical region and the query looks for a device in a different region).

If M2M Devices, Virtual Devices and Things that match the criteria are found within the domain of a M2M Service Provider to which the semantic query had been forwarded then the search results may be returned via standardized inter-provider interfaces to the domain of the M2M Service Provider that had forwarded the query. The search result shall contain sufficient information to identify the device and the term of use for the device.

3. The M2M System shall provide the capability to return to the M2M Application that had issued the semantic query the results of the query from the M2M Service Provider's domain and from M2M Service Provider domains to which the query had been forwarded.

The supported formats for semantic queries shall be described in the oneM2M standard.

12.10 Underlying network service activation and deactivation

12.10.1 Description

- Background of the use case
  Currently, for flexible M2M service deployments and low network service subscription cost, some underlying network operators have developed their private network service activation and deactivation APIs and opened them to M2M application providers. The M2M systems may need to support reusing the network service activation and deactivation capability provided by underlying network via transforming these network APIs and opening for M2M applications.

- Overview of the use case
  In the M2M device, a network service module (e.g. SIM card) will be embedded to support the network communication. For some potential

requirements, the network service module need be activated or deactivated by remote or local M2M applications via M2M platform.

In the context of this use case, an *active network service module* means that the network service module enables the M2M device to send / receive M2M traffic. An *inactive network service module* does not allow the M2M device to send / receive M2M traffic, however the service module, together with the M2M device, is capable to exchange signalling with M2M platform according to network operator's policy.

The network entity of underlying network can activate/deactivate network service module according to network policy and network service activation/deactivation request.

The following scenarios are given to show above requirements.

- Factory acceptance test
  During the factory acceptance test of the M2M device, the network service module need be activated for M2M service testing. After the test, the network service module need be deactivated for saving the network subscription cost.
- Starting usage
  When the M2M device are sold and the user starts to use it, the network service module need be activated to support the M2M service. The network service module may be activated via M2M platform by local M2M applications in the case that the local M2M applications detects the M2M device in use or by remote M2M applications in the case that the user requests the M2M application server to active the M2M device.
- Abandon
  When the M2M device is abandoned by user, the network service of the M2M device need to be deactivated for reducing network service subscription cost. In this case, the network service module will be deactivated via M2M platform by remote M2M applications.
- Lost
  When the M2M device is lost or stolen, the network service of the M2M device need be deactivated for reducing network service subscription cost. In this case, the network service module will be deactivated via M2M platform by remote M2M applications.
- Abused
  When the M2M device is misused by user (e.g. used for certain forbidden services), the remote M2M application server intends to stop providing M2M service and deactivate the network service of target M2M device via M2M platform.
  Similarly, if a M2M device is used outside a specific geographic area in which the M2M device is supposed to operate (e.g. a vending machine is removed from its assigned place) then a location enabled M2M device may deactivate the network service module.

12.10.2 Source

REQ-2014-0446R02 Underlying network service activation and deactivation use case

12.10.3 Actors

- Underlying network operator
- M2M service provider
- M2M Application server (operated by a M2M Application Service provider)
- M2M platform (operated by the M2M service provider)
- M2M device (containing a network service module)
- Network service module (operated by the Underlying network operator)

12.10.4 Pre-conditions

- The mobile network operator opens the service interface, i.e. network API, for remote activation and deactivation of underlying network service.

12.10.5 Triggers

The following triggers could initiate exchange of information.

Trigger A:

The M2M application on M2M device initiates the activation request. In this case, the M2M device is in use, and the M2M application intends to activate / deactivate the network service of the corresponding M2M device via an M2M platform.

(Note that even if the network service of the M2M device is deactivated, the M2M device may still be able to connect to target M2M platform according to the policy of network operator.)

Trigger B:

The M2M application server initiates the activation/deactivation request. In this case, the M2M application intends to activate / deactivate the network service of the target M2M device via M2M platform.

12.10.6 Normal Flow

Trigger A:
When the M2M device is in first use, network service activation request will be triggered by local M2M application on M2M device (Trigger A).

1. The M2M application on M2M device initiates the activation request to M2M platform.

2. The M2M platform uses the network service activation API provided by the underlying network operator to active the network service module of the corresponding M2M device and feedback the activation information.

Trigger B:
When the user intends to reuse the M2M device, network service activation request will be triggered by remote M2M application, and when the M2M device is misused by users, network service deactivation request will be triggered by remote M2M application. (Trigger B).

1. The M2M application server initiates the activation/deactivation request to M2M platform.
2. The M2M platform uses the network service activation/deactivation API provided by the underlying network operator to activate/deactivate the network service module of target M2M device and feedback the activation/deactivation information to the M2M application server.

12.10.7 Alternative Flow

None

12.10.8 Post-conditions

Trigger A:
The M2M device can send / receive M2M traffic if the network service module is activated successfully according to network activation request.

Trigger B:
The M2M device cannot send / receive M2M traffic but may be able to exchange signalling with M2M platform if the network service module is deactivated successfully according to network deactivation request.

12.10.9 High Level Illustration

Fig. 12.10.9-1 and Fig. 12.10.9-2 describe the normal flow of this use case for Trigger A and Trigger 2 from high level aspect.

12.10.10 Potential requirements

1. The M2M systems shall support the capability of reusing the network service activation and deactivation capability in underlying network via Mcn reference point.

12.11 On-demand data collection for factories

Void

Note: This use case can be found in TR-0018 [i.19].

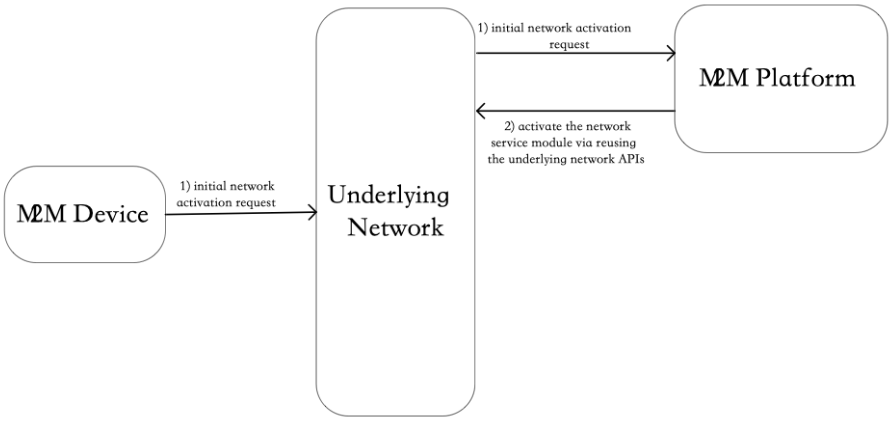

1) initial network activation request
M2M Platform
2) activate the network service module via reusing the underlying network APIs
M2M Device
1) initial network activation request
Underlying Network

Figure 73: Figure 12.10.9-1 - Normal flow description for Trigger A

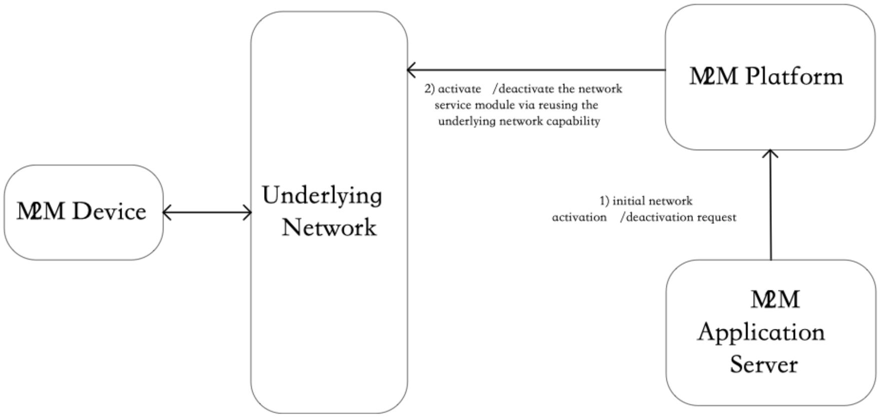

M2M Platform
2) activate /deactivate the network service module via reusing the underlying network capability
M2M Device
Underlying Network
1) initial network activation /deactivation request
M2M Application Server

Figure 74: Figure 12.10.9-2 - Normal flow description for Trigger B

Source: REQ-2014-0487R03: A use case for industry: On-demand data collection for factories

12.12 Smart Irrigation System

12.12.1 Description

The use case describes a smart irrigation system in which all the valves and sensors deployed around the farmland are centrally controlled and managed by Irrigation Administration Centre. The sensors include temperature, humidity, illumination and soil moisture level. The Irrigation Administration Centre collects data from those sensors and decides if it's time to irrigate the farmland. Because the soil condition and the plant are different depend on the area of the farmland. The timing of the irrigation may be different. According to the pre-configured policies, and the Irrigation Administration Centre decides which valves to open, which valves to close as well as how much the value opens to irrigate the farmland.

12.12.2 Source

REQ-2015-0528R03 Use case on transactions (Smart Irrigation System).

12.12.3 Actors

- Irrigation Administration Centre (IAC): The application that analyses the data collected by sensors and control the valves to irrigate the farmland.
- Smart Irrigation Service Provider: The Smart Irrigation Service Provider provides special sensors and valves to implement irrigation system. The Smart Irrigation Service Providers also own the database on the policies of how to irrigate certain plant based on the data collected by sensors. The Smart Irrigation Service Provider helps the customer of its system to deploy the irrigation system which includes the deployment of gateways, sensors and valves into the farmland. Prepare the channel and pipes to let the water flow to every corner of the farmland. The installation and configuration of the Irrigation Administration Centre. And make sure the system is working fine before the finishing of its service.
- M2M Service Provider: The M2M Service Provider provides M2M platform, M2M Gateway and standard ways to connect devices with each other. The Smart Irrigation Service Provider subscribes the service provided by M2M Service Provider to deploy its own service.
- Farmer: The customer that purchases the service from Smart Irrigation Service Provider. After the installation of the Smart Irrigation System, the farmer will no longer worry about the irrigation of its farmland.
- Sensors and Valves: Sensors and Valves deployed by Smart Irrigation Service Provider. The Valves are connected by channels or pipes. The sensors are scattered around the farmland include temperature sensor, humidity sensor, light sensor, soil moisture sensor.

- Channels and Pipes: Channels and pipes are jointly connected by valves from the source of the water to every corner of the farmland. Channels are half closed and may be overflowed if the water cannot be released in time. Pipes are closed and have standard pressure limit. If the downstream valve cannot be opened in time, may cause irregular pipe pressure which may result in fall of the junction valve or leak of water.
- M2M Gateway: M2M Gateways are deployed by M2M Service Provider to connect with sensors and valves around the farmland. M2M Gateway collects data from sensors and reports the data to M2M Platform. M2M Gateway also distribute control message from M2M Platform to valves.
- M2M Platform: M2M Platform is deployed by M2M Service Provider. It stores sensor data and valve conditions which are read or written by Irrigation Administration Centre application.

12.12.4 Pre-conditions

The subscription relationships between farmer, Smart Irrigation Service Provider, M2M Service Provider are carefully contracted.

Channels and Pipes are connected with valves from the source of water to every corner of the farmland.

Sensor are scattered around the farmland and connected with gateway and finally connected with the M2M Platform.

Irrigation Administration Centre is registered with M2M Platform and can successfully read or write sensor and valve state data.

To irrigate one part of the farmland, it may need to open several valves at the same time or in a certain order. If failed to do so, it may cause water overflow of the channel or irregular pressure of the water pipes. This may then result in unexpected irrigation or water leak.

12.12.5 Triggers

Based on the sensors data read by the Irrigation Administration Centre, the Irrigation Administration Centre decides to irrigate one part of the farmland.

12.12.6 Normal Flow

1. IAC read sensors data from M2M Platform of Area_A of the farmland.
2. IAC detects that according to current condition, Area_A needs to be irrigated half an hour later.
3. IAC detects that to irrigate Area_A, Valve_1, Valve_3 and Valve_7 need to be opened at the same time. Valve needs to be opened to 10%, Value_3 needs to be opened to 50% and Valve_7 needs to be opened to 100%.
4. IAC then sends request to M2M Platform to indicate to switch the valves to corresponding percentage in half an hour.

5. Valve_1, Valve_3 and Valve_7 responded with success information immediately.
6. Valve_1, Valve_3 and Valve_7 adjusted its open percentage after half an hour. Irrigation starts.
7. IAC detects that according to current condition, the water in Area_A would be sufficient.
8. IAC then sends request to M2M Platform to indicate to switch the valves off in 5 min.
9. Valve_1, Valve_3 and Valve_7 responded with success information immediately.
10. Valve_1, Valve_3 and Valve_7 is shut off in 5 min. Irrigation stopped.

12.12.7 Alternative flow

The alternative flow is about the scenario that something error happened during the operation of the valves.

1. IAC read sensors data from M2M Platform of Area_A of the farmland.
2. IAC detects that according to current condition, Area_A needs to be irrigated half an hour later.
3. IAC detects that to irrigate Area_A, Valve_1, Valve_3 and Valve_7 need to be opened at the same time. Valve needs to be opened to 10%, Value_3 needs to be opened to 50% and Valve_7 needs to be opened to 100%.
4. IAC then sends request to M2M Platform to indicate to switch the valves to corresponding percentage in half an hour.
5. Valve_1 and Valve_7 responded with success information immediately but Valve_3 responded with a failure.
6. IAC requests to Valve_1 and Valve_7 the cancellation of the operation.
7. Valve_1 and Valve_7 responded the success cancellation.
8. Irrigation failed, the IAC will try some time later again for the irrigation.

12.12.8 Post-conditions

None

12.12.9 High Level Illustration

12.12.10 Potential requirements

1. The oneM2M system shall support distributed transactions to multiple devices or applications where the transaction includes the characteristics of atomicity, consistency, isolation and durability.
2. sThe 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.

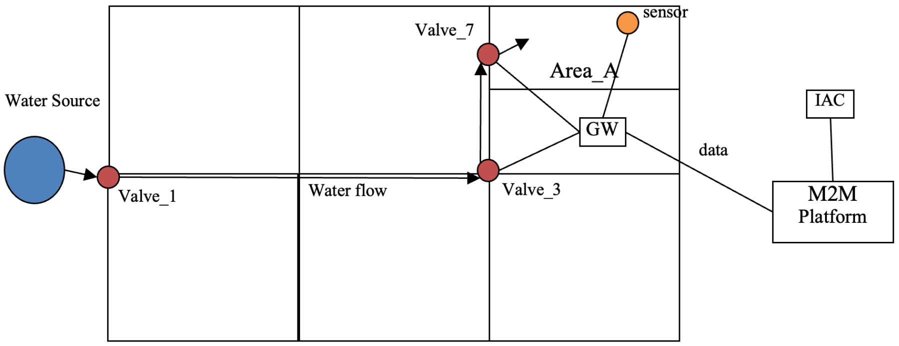


Figure 75: Figure 12.12.9-1 Smart Irrigation System

12.13 Group Registration Management

12.13.1 Description

A user's smart phone hosts several workout tracking applications and several home automation applications.

The workout tracking applications were provided with the user's gym membership. When in the gym, the workout applications are used to reserve and monitor the availability of workout equipment (e.g., treadmills) and track the user's workout performance. While at home, the workout tracking applications are used to track the user's workout performance.

The home automation application are used to control smart devices in the home while the user is at home or on the road.

When the user is at home, both the workout and home automation applications register with the user's home automation gateway so that they can communicate with smart devices and workout equipment in the home. While on the road, the home automation applications register with an M2M Server that can be used to monitor and control devices in the home via the home automation gateway. The workout applications also register with the M2M Server and take advantage of a location tracking service that the M2M Server offers. The location tracking service will be used by the workout application to detect when the host devices enters a gym.

Upon entering the gym, the workout applications register with an M2M Gateway that is owned by the gym. The geographical availability of new services triggers the workout applications to search for a new service layer and a registration to a new service layer.

12.13.2 Source

REQ-2015-0561 Use case group registration

12.13.3 Actors

- Workout Applications
- Home Automation Applications
- Home Gateway
- Gym Gateway
- M2M Server

12.13.4 Pre-conditions

The Home GW is registered with the M2M Server

12.13.5 Triggers

Location change

12.13.6 Normal Flow

- 0a. The Device is registered with the home GW (i.e. via Wi-Fi).
- 0b. The workout and home automation applications AEs are registered with the ASN-CSE
- 1a. The user leaves the home, thus losing its network connection to the Home Gateway.
- 1b. The device (smart phone) performs service discovery and determines that the M2M Server can be reached (i.e. via cellular).
- 1c. The device registers with the M2M Server (i.e. via cellular).
- 2a. The user enters the gym.
- 2b. The device performs service layer discovery and determines the availability of the gym as registration point. Alternatively M2M Server notifies the device of the new registration point available at the gym. The cellular connection continues to be available.
- 2c. The device re-registers at Gym Gateway (e.g. via Wi-Fi)and announces the workout applications AE1 and AE2.The device does not announce applications which cannot be serviced by the gym gateway (e.g. home automation AE3)
- 3. The device notifies the home automation application AE3 of the availability of the M2M Server as registration point and AE3 re-registers directly with the M2M Server

12.13.7 Alternative flow

Depiction of alternative flows is not relevant

12.13.8 Post-conditions

The workout applications (AE1 and AE2) are being serviced by the Gym Gateway via a Wi-Fi connection. The home automation applications (AE3) is now registered to the M2M Server via a cellular connection.

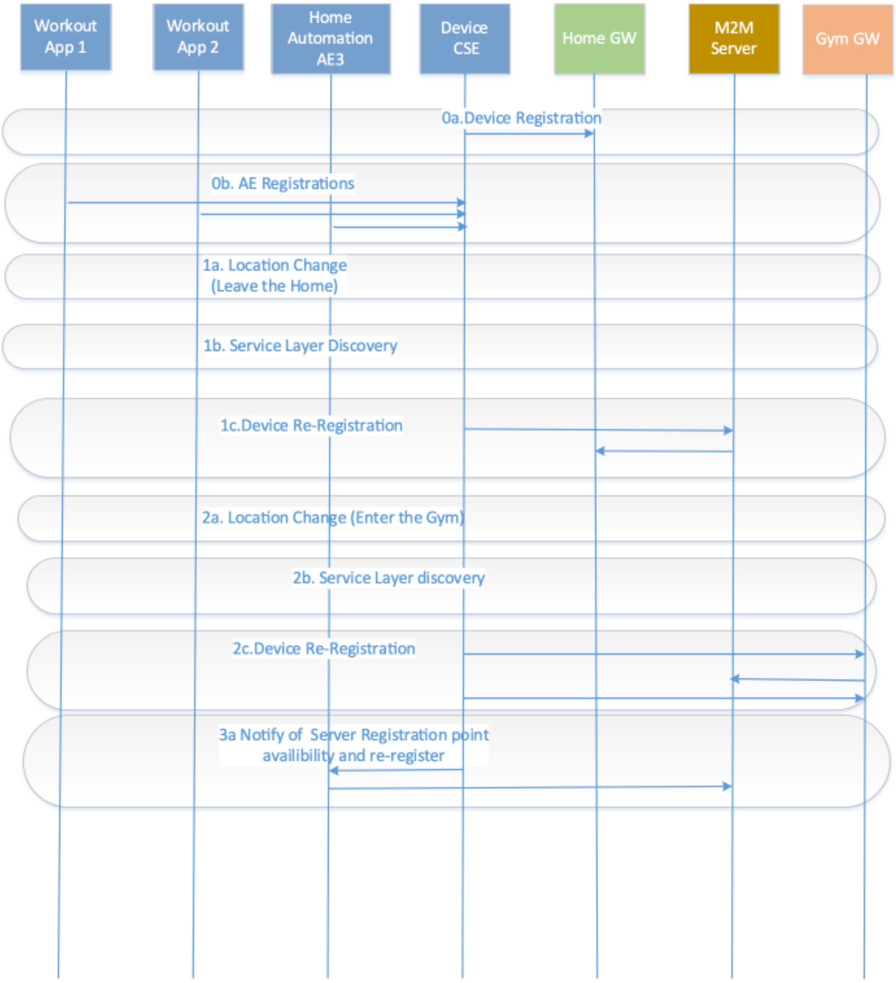

Workout App 1
Workout App 2
Home Automation AE3
Device CSE
Home GW
M2M Server
Gym GW
0a.Device Registration
0b. AE Registrations
1a. Location Change (Leave the Home)
1b. Service Layer Discovery
1c.Device Re-Registration
2a. Location Change (Enter the Gym)
2b. Service Layer discovery
2c.Device Re-Registration
3a Notify of Server Registration point availibility and re-register

Figure 76: Figure 12.13.6-1 Group Registration Management

12.13.9 High Level Illustration

See high level flow

12.13.10 Potential requirements

1. The oneM2M System shall provide the capability to notify a device hosting a group of applications that it should perform discovery when alternative registration points are available (e.g., via different underlying networks) based on the service requirements of each of the applications hosted.
2. The oneM2M System shall provide the capability to register applications in group or independently, based on their service requirements.

12.14 Multicast using group

12.14.1 Description

In the smart metering scenario, meters are reporting their collected data to the server in a predefined frequency. If it is decided to change the frequency, the server will have to change the policy to every meter by unicast manner. It's preferred that the system may utilize the broadcast or multicast mechanism to send out the configuration message to all the eligible devices at one time to save the network resources.

12.14.2 Source

REQ-2015-0557R01-Use Case multicast using group

12.14.3 Actors

- Metering Company: The Company that provides metering service to collect metering data from all the meters deployed across the city.
- M2M SP Platform: The platform provided by the M2M Service Provider to collect metering data from all meters.
- Meter: The meter device that is equipped with a wireless of wired network capability that connects with the M2M SP Platform to report their metering data.

12.14.4 Pre-conditions

The Metering Company and M2M Service Provide has signed contract about delivering the M2M Service.

The Metering Company deploys Meters with pre-configuration on the frequency of reporting the data.

The Meters connect and register with the M2M SP Platform and periodically reports metering data.

12.14.5 Triggers

The Metering Company decided to change the report frequency.

12.14.6 Normal Flow

1. The Metering Company creates a group on the M2M SP Platform and include all the meters as group members.
2. After the successful creation of group, the Metering Company then sends a policy configuration message to all meters through the group.
3. The M2M SP Platform determines if the connection of the meters supports broadcast/ multicast.
4. The M2M SP Platform then makes the best use of the broadcast/ multicast mechanism to fan out configuration messages.
5. After the receiving of the policies, meters start to report the metering data using the new frequency.

12.14.7 Alternative flow

None

12.14.8 Post-conditions

None

12.14.9 High Level Illustration

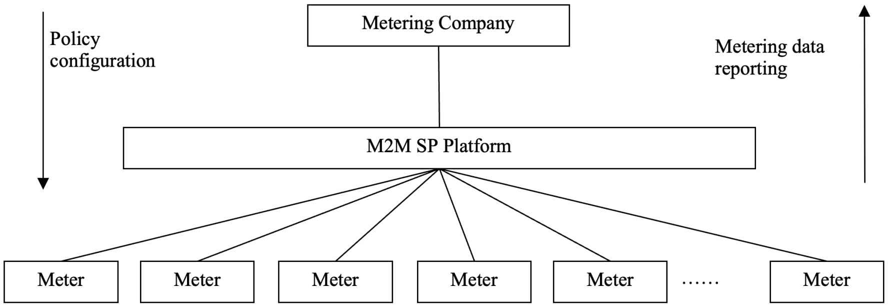


Figure 77: Figure 12.14.9-1 Multicast using group

12.14.10 Potential requirements

1. 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.[OSR-052]

2. The M2M System shall be capable of collecting asynchronous responses pertaining to the broadcasted messages.

12.15 Access control using group

12.15.1 Description

The Parking Management System of the building is in charge of collecting the number of the available parking slot by the sensor that was set above each slot. The Parking Management System publishes the information on the M2M Platform for vehicles which is destined to the building to acquire. However, the information is only disclosed to vehicles that has proper access rights. The Parking Management System uses a group to organize the vehicles that has the correct access rights.

12.15.2 Source

REQ-2015-0556R01-Use Case access control using group

12.15.3 Actors

- Parking Management System: The Parking Management System uses the M2M SP to host its parking slot reservation service. The Parking Management System reports the available number of parking slots to the M2M platform for vehicles to acquire.
- M2M SP: The M2M Service Provider provides M2M platform as well as the connection between the platform, vehicles and the Parking Management System.
- Vehicle: The Vehicle acquires the available parking slot number of the building and decides if to reserve one from the Parking Management System or choose another nearby parking area.

12.15.4 Pre-conditions

The Parking Management System, the M2M SP and the Vehicles have established business relationship with each other.

Some Vehicles has been authorized by the Parking Management System to read the available parking slot information while some others are not.

The Parking Management System created a group on the platform of the M2M SP to organize all the Vehicles that are authorized.

12.15.5 Triggers

One Vehicle attempts to acquire the available parking slot number from the platform.

12.15.6 Normal Flow

1. The Vehicle that is destined to the building acquires the available parking slot from the platform.
2. The platform inspects if the Vehicle is among the group that is authorized to retrieve such information.
3. The platform finds that the Vehicle is a member of the group.
4. The platform responds back the information to the Vehicle.

12.15.7 Alternative flow

1. The Vehicle that is destined to the building acquires the available parking slot from the platform.
2. The platform inspects if the Vehicle is among the group that is authorized to retrieve such information.
3. The platform finds that the Vehicle is not a member of the group.
4. The platform rejects the acquire attempt from the Vehicle.

12.15.8 Post-conditions

None

12.15.9 High Level Illustration

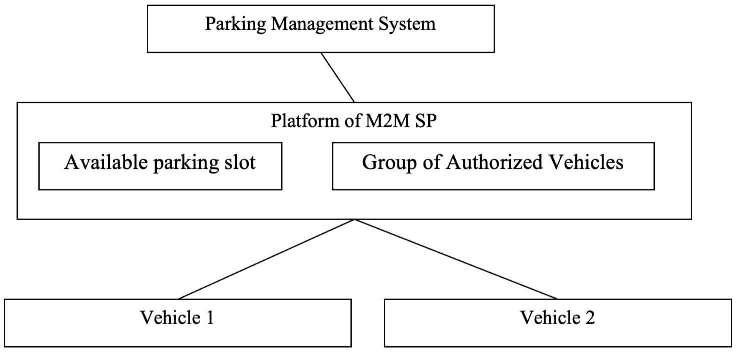


Figure 78: Figure 12.15.9-1 Access control using group

12.15.10 Potential requirements

1. The M2M System shall support grouping of M2M applications that have the same access control rights towards specific resources, so that access control can be performed by validating if the M2M application is a member of certain group.

12.16 Personal data management mechanism based on user's privacy preference

12.16.1 Description

Because the data collected by the M2M platforms may include personal information or sensitive information of data providers, the access to such data should be controlled appropriately. This use case shows the data management mechanism based on data provider's privacy preferences, which is developed as a PPM (Privacy Policy Manager). Because access from application service providers to the collected data at M2M service platform is controlled based on the privacy preferences that are configured by the data providers, unnecessary and unwanted access to the collected data is blocked appropriately.

12.16.2 Source

REQ-2015-0576-Use case of PPM

12.16.3 Actors

- Front-end data-collection equipment (M2M devices): This actor collects various kinds of data and sends the data to a management platform. The collected data may include sensitive or privacy information of data providers.
- Management platform (M2M Service Provider's Platform): The management platform stores the data collected by M2M devices. This also has authorization function that manages the access control to the stored data.
- Data provider: A data provider is a user of services from application service providers. The user subscribes services, and the management platform starts to collect data related to the user and its services. In case that a service requires personal information of a user, such data are collected by the management platform. So the user becomes the data provider. The data that are provided by the data provider may include sensitive or private information. The data provider can configure his/her privacy preference for the collected personal data. If the data provider would not like to permit the application service provider to collect or access specific kinds of data, the data provider can configure the privacy preference of the service to control the data collection or access. The management platform control the data collection from the M2M devices and the data access from the application service providers to the collected personal data based on the privacy preferences.
- PPM: A PPM function manages privacy preferences of the data providers. The data providers configure their privacy preferences while subscribing application services. The application service providers present the data providers which kinds of data are collected and used by the application service, and the data providers configure their privacy preferences to give access permissions to several kinds of collected data. Although an applica-

tion service provider may use many kinds of data from a data provider, the data provider can permit the subset of listed data by configuring the privacy preference for its application service. A PPM function also has mechanism to record the usage of the collected data. When application service providers access to the collected data from data providers, its accesses are logged to the PPM. If the data providers would like to refer the past usage of their personal data, they can check it by accessing the PPM. The data provider can request the application service providers to delete the collected data based on the record of access log.

- Application service providers: This actor provides many kinds of services to service users. In case the application service providers use the data stored in the management platform, they access to the data via authorization function. Because this function provides access control to the data, the function asks a PPM and decides whether the application service provider has access permission to the accessing data or not.

12.16.4 Pre-conditions

None

12.16.5 Triggers

- Service subscribing trigger: configuring privacy preference of data providers for each service
- Data collection trigger: collecting data at M2M modules
- Data access trigger: accessing collected data from application service providers
- Data usage reference trigger: referring usage of collected data from application service providers
- Data deletion trigger: requesting deletion of accessed and stored data in application service providers

12.16.6 Normal Flow

The following normal flow is described based on a figure in High Level Illustration (Figure 12.16.9-1).

- a) Configuration of privacy preference by data provider
    1. When a user starts to subscribe a service of application service provider, the user checks the privacy policy of service. The privacy policy explains what kinds of data will be accessed to provide the service. If the user permits the application service provider to access the collected data by M2M management platform, the user becomes the data provider.
    2. The data provider can select the kinds of data that the application service provider can use by using the PPM. If the data provider would not like to permit the application service provider to access specific

kinds of data, the data provider can configure the privacy preference to enable this situation. In other words, because this access permission can be defined item by item, the data provider can restricts the access to the part of collected data.

- b) M2M data collection

  1. The M2M Service Provider's platform collects data related to the data providers by using M2M devices. In this phase, unwanted and unused data are not collected by configuring privacy preference in PPM appropriately.

- c) M2M data access from application service providers

  1. When application service providers access to the collected data in M2M Data, they access M2M Service Provider's Platform. The authorization function in the platform controls access to the M2M Data based on the privacy preference stored in the PPM. The authorization function retrieves privacy preference to the target data from the PPM.
  2. If the access is permitted, the target data are transferred to the application service provider. If the access is not permitted, the authorization function responds to the application service provider with the notification of access denied with reasons.

- d) Traceability of personal data usage

  1. When the application service providers access to the collected data in M2M Data, all the access and its result (access permitted, access denied) are recorded and stored at the PPM.
  2. If the data provider would like to check the status of data usage by application providers, the data provider access to the PPM. The data provider can recognize that which application provider accessed to what kinds of collected data.
  3. If the data provider would like to delete the collected data that were stored in the application service providers, the data provider can request the application service providers to delete the transferred data by specifying access record in the PPM.

12.16.7 Alternative flow

None

12.16.8 Post-conditions

None

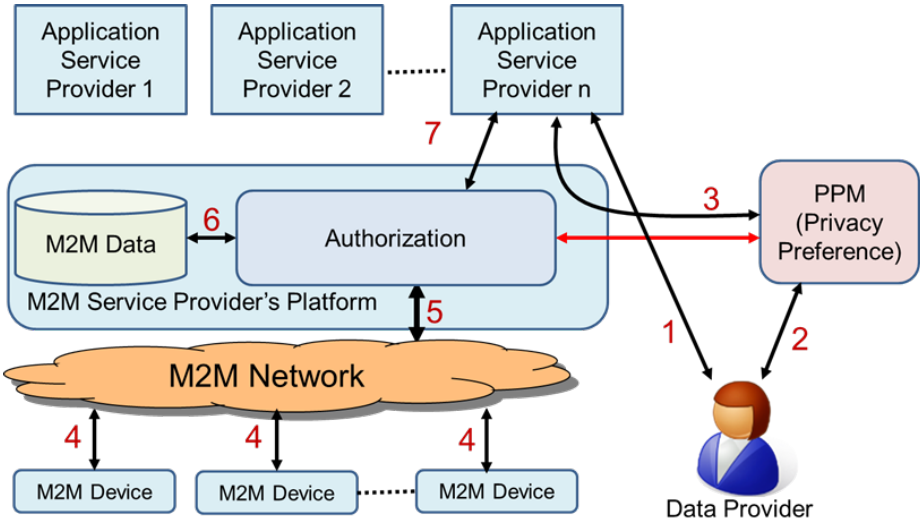

Application Service Provider 1
Application Service Provider 2
Application Service Provider n
7
M2M Data
6
Authorization
3
PPM (Privacy Preference)
M2M Service Provider's Platform
5
1
2
M2M Network
4
4
4
M2M Device
M2M Device
M2M Device
Data Provider

Figure 79: Figure 12.16.9-1 Overview of Personal Data Management mechanism using PPM

12.16.9 High Level Illustration

12.16.10 Potential requirements

1. The M2M system shall support the capability of managing the data collection and access to the collected data by using authorization mechanism to avoid unnecessary and unwanted personal information access based on the privacy preference defined by the data provider.
2. The M2M Service Provider's Platform system shall provide an interface that enables access control for personal data of a data provider by using access control policy defined by the data provider as privacy preference.

12.17 Quality of Sensor Data

12.17.1 Description

It is quite popular to transmit observation values of the sensor as a form of time series data in social infrastructure, i.e. factories, power plants, water systems, or railroad systems. In these handling of sensor values, observation value is transmitted with "quality bit", which represents quality of data, i.e. the observation value is valid or not by reference to predefined normal operating condition of the sensor.

The quality bit is used as a quality indicator of observation value of sensor. In other words, it is used as a basis for considering whether the value is usable or not, or how the value should be used.

Here we consider an example case where water is stored in a tank and is conveyed by a pump. The water level of a tank is observed by a sensor, and data collection policy (named data catalogue) is utilized at oneM2M MN to transmit average of 2 observation values. The observation value is not adequate to be utilized when there is any abnormality in the electric power source of the sensor or in controller. The average value is not adequate to be utilized when one of observation values is not adequate. Therefore, information such as "the observation value of sensor of water level lacks quality" is added in order to make the application work as intended.

12.17.2 Source

REQ-2015-0599R03 Sensor Data Quality

12.18.3 Actors

- Tank1: Tank stores water
- Pump1: Pump conveys water
- Water level sensor1: It observes water level of a tank1 and transmit the observation value d1 to PLC/DCS1 at fixed time intervals
- Electric power source of water level sensor1: It supplies electric power which is required for the water level sensor1 to work correctly
- PLC(Programmable Logic Controller)/DCS(Distributed Control System)1: PLC/DCS receives two observation values, i.e. water level of tank1 and status signal of electric power source of water level sensor1, and transmit a form of water level data d1 with a quality bit q1 at fixed time intervals. When the electric power source of water level sensor1 is abnormal or PLC/DCS1 itself has some abnormality, the water level observation value d1 is considered to be incorrect and the quality bit q1 is set to "not good."
- Tank2: Tank stores water
- Pump2: Pump conveys water
- Water level sensor2: It observes water level of tank2 and transmit the observation value d1 to PLC/DCS2 at fixed time intervals
- Electric power source of water level sensor2: It supplies electric power which is required for the water level sensor to work correctly
- PLC/DCS2: PLC/DCS receives two observation values, i.e. water level of tank2 and status signal of electric power source of water level sensor2, and transmit a form of water level data d2 with a quality bit q2 at fixed time intervals. When the electric power source of water level sensor2 is abnormal or PLC/DCS2 itself has some abnormality, the water level observation value d2 is considered to be incorrect and the quality bit q2 is set to "not good."
- oneM2M MN: oneM2M MN receives water level observation values d1 and its corresponding quality bit q1 from PLC/DCS1 as a form of time series data, receives water level observation value d2 and its corresponding quality bit q2 from PLC/DCS2 as a form of time series data, calculates

average value d3 as specified by data catalogue, and transmits the average value d3 and its quality bit q3 to oneM2M platform. When quality bit q1 or q2 is “not good”, the calculated average d3 is considered to be incorrect and quality bit q3 is set to “not good.”

- oneM2M platform: oneM2M platform receives time series data and its corresponding quality bit from oneM2M MN and transmit them to Application.
- oneM2M Application: oneM2M Application receives time series data and its corresponding quality bit, and performs user-defined procedure(s) referring quality bit value.
- Real-time Ethernet: Real-time Ethernet connects PLC/DCS and oneM2M MN.
- Underlying network: connects oneM2M MN and oneM2M platform.

12.17.4 Pre-conditions

Observation value of sensor is coupled with its quality bit and correspondence relation is defined.

12.17.5 Triggers

PLC/DCS receives observation value at fixed time intervals and receives status signal of electric power supply of the water volume sensor.

12.17.6 Normal Flow

1. When the electric power source of water level sensor1 is normal and PLC/DCS1 has no abnormality, the observation value d1 is considered to present correct water level and to be usable and PLC/DCS1 adds quality bit q1 “good” to the observation value d1. Otherwise, when the electric power source of water level sensor 1 is abnormal or PLC/DCS1 has some abnormality, the observation value d1 is considered to be incorrect and PLC/DCS1 adds quality bit q1 “not good” to the observation value d1. Similarly, PLC/DCS2 adds quality bit q2 “good” or “not good” to the observation value d2.
2. oneM2M MN receives observation value d1 and its corresponding quality bit q1 from PLC/DCS1 as a form of time series data receives observation value d2 and its corresponding quality bit q2 from PLC/DCS2 as a form of time series data, calculates average value d3 as specified by data catalogue, and transmits the average value d3 and its quality bit q3 to oneM2M platform. When q1 or q2 is “not good”, the calculated average value d3 is considered to be incorrect and quality bit q3 is set to “not good.”
3. oneM2M platform receives time series data and its corresponding quality bit from oneM2M MN, and transmits them to oneM2M application.
4. Application receives time series data and its corresponding quality bit from oneM2M platform and performs user-defined procedure(s) referring quality

bit value. Usually, observation value with quality bit “not good” is not used to monitoring or controlling functions.

12.17.7 Alternative flow

None.

12.17.8 Post-conditions

None.

12.17.9 High Level Illustration

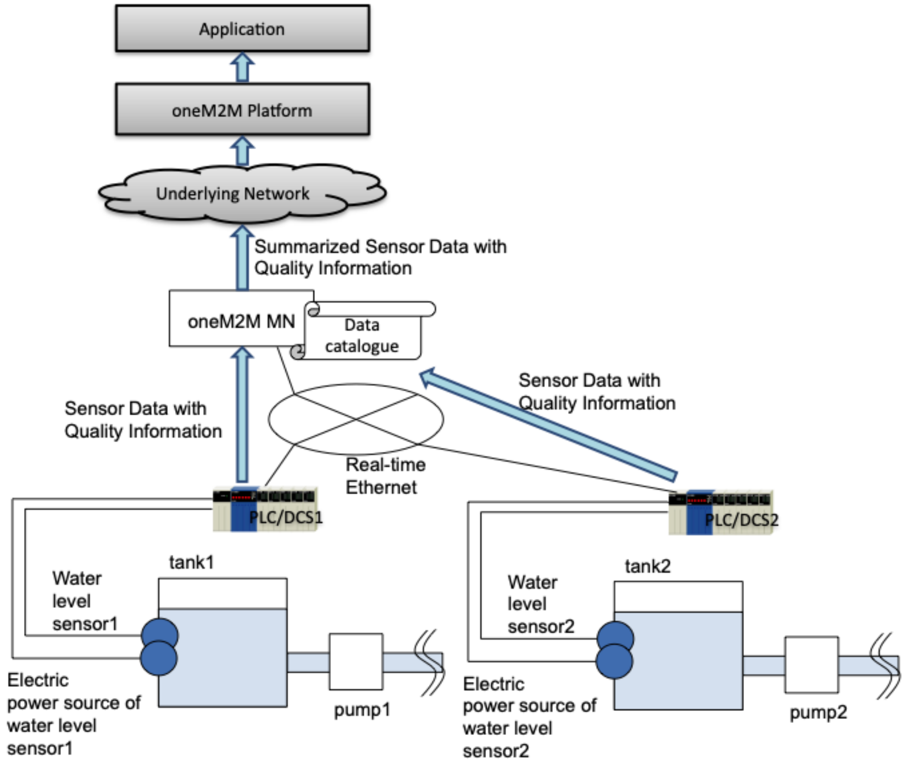

Application
oneM2M Platform
Underlying Network
Summarized Sensor Data with Quality Information
oneM2M MN
Data catalogue
Sensor Data with Quality Information
Sensor Data with Quality Information
Real-time Ethernet
PLC/DCS1
PLC/DCS2
tank1
tank2
Water level sensor1
Water level sensor2
Electric power source of water level sensor1
Electric power source of water level sensor2
pump1
pump2

Figure 80: Figure 12.17.9-1 Quality of sensor data

12.17.10 Potential requirements

1. The oneM2M system shall provide capability to manage data quality description of resource.

12.18 Agriculture monitoring drone system

12.18.1 Description

Drone was originally developed for military purpose for surveillance of enemy troops. However, the drone is now used in a wide variety area specifically in sport, logistic, media, industry, and agriculture area. Since drone can be equipped with GPS flight assistance, Sensor, Radar, and Camera, it can detect abnormal action when it fly over the farmland and report the data to the administration centre. In addition, the drone can carry pesticides and spray over the crop to protect it from fungal infections.

Drone collects the information regarding the condition of farmland and crop and send the monitoring data to the administration centre. At agriculture administration centre, the aggregated data can be analysed and the information used for smart faming solution e.g., knowing how much fertilizer needs to be used, detecting what harmful insects are living in the farmland.

Drone is operated with battery power and after receiving command message from administration centre, it follows the action described in the command message e.g., modifying monitoring region coverage, coming back to the battery charging station. If a series of command messages are not delivered to each drone because of communication loss or if the message is delivered well but it malfunctioned then the desired actions are not performed. In order to prevent this situation, service transaction mechanism was introduced in the M2M platform. This use case is based on service transaction and this additionally introduces policy-based transaction rescheduling mechanism.

12.18.2 Source

REQ-2015-0607R01 Use Case for Agricultural Drone

12.18.3 Actors

- Drone, which can monitor the condition of farmland and crop and report data to the administration centre through M2M platform. It also carry pesticides or fertilizer on the move to spray over the crop.
- M2M Platform, which can manage the resources about drones and receive message from drone and deliver control message to the drone connected via access network.
- Agriculture Monitoring administration Centre (AMC), which receive the data from drones for monitoring farmland and crops and send the command message to each drone for desired action.

12.18.4 Pre-conditions

None

12.18.5 Triggers

The battery level of one drone is low and needs to be recharged. In this situation, AMC sends the drone a command message which indicates the drone coming back. At the same time, AMC sends group of drones command messages which direct coverage modification about monitoring region.

12.18.6 Normal Flow

0. All Drone are registered with M2M Platform and AMC sends control messages to each drone for monitoring the farmland and crop.
1. If one drone's battery level become low, AMC gets this information and waits for sending the control message which indicates the drone with low level battery should come back to the battery charging station. If one drone come back to the charging station and then the number of drone monitoring the farmland decrease. Thus each drone needs to update its monitoring coverage. To this end, AMC waits for sending each drone control messages which indicate modifying its monitoring coverage.
2. Because a series of command message is important, AMC initiates transaction triggering mechanism and sends command message to drone 1 - 6.
3. In this situation, drone 1 - 5 responded with success information, drone 3 has a problem and responded with failure information.
4. Because transaction mechanism was initiated, AMC sends the roll-back message to drone 1 - 6 which enables each drones to cancel the received command message and return to the previous status.

12.18.7 Alternative Flow

The alternative flow is about the scenario represents policy-based rescheduling mechanism.

0. AMC initiates transaction triggering mechanism and sends command message to drone 1 - 6.
1. In this situation, drone 1 - 5 responded with success information, drone 3 has a problem and responded with failure information.
2. Based on the responding message from drone 1 - 6, M2M platform triggers transaction rescheduling mechanism referring to the transaction policy.
3. Transaction group is created for transaction rescheduling for example, drone 1 - 3 are grouped with A, drone 4 - 6 are grouped with B.
4. In this case, if drone 3 fails again as the same in previous situation, only drone 1 - 3 in Group A would be affected by the cancellation of the operation.

12.18.8 Post-conditions

None.

12.18.9 High Level Illustration

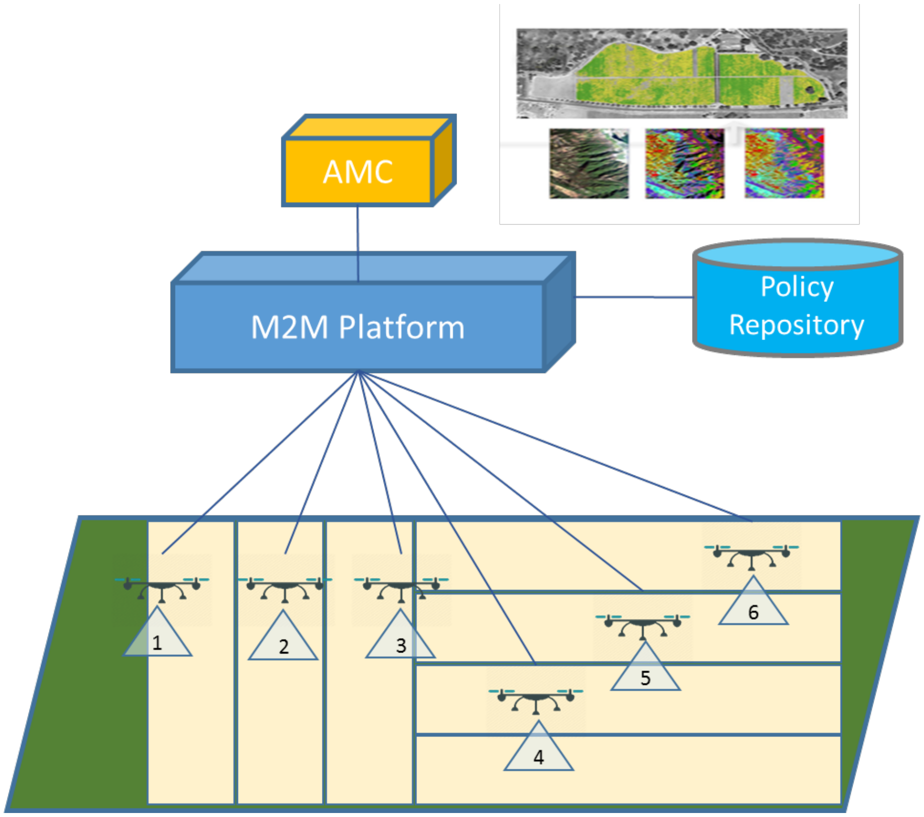


Figure 81: Figure 12.18.9-1 Agriculture monitoring drone system

12.18.10 Potential requirements

1. 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.

12.19 Terms And Conditions Markup Language for Privacy Policy Manager

12.19.2 Description

Given different legal jurisdictions and individual preferences, there is a need to at least semi-automate the process for configuring privacy preferences and agreement to Terms and Conditions (T&C's). Otherwise the user (data subject) would have to agree multiple T&C's and each smart device and service would have to have a GUI that the user would have to access and configure to set their privacy preferences by hand. A better way forward would be to allow the profile owner configure a single set of profile's (house, work, personal, parental, legal etc.) and as a new smart device or service is added:

- A. Where the terms and conditions fall within the parameters set in the user's profile, the device can be automatically authorised (with a notification to the user). If the T&C don't fall within the parameters set, only the differences (as a delta to the user's profile) are presented to the user for authorisation with the exception of the parental/Legal profile which the user will not be able to override, only the profile owner (e.g. parent/Local government respectively) can override.
- B. The user's privacy settings from their profile can be automatically configured where relevant, with confirmation notification to the user. Where it's not possible to fully configure the relevant security controls the user is alerted and can manually decide

  To make this possible we need to be able to convert Terms & Conditions and privacy settings in to a standard mark-up language that can be understood by smart devices and translated in to a human readable format. Another advantage of this mark-up language will allow standard translations of this mark-up language in to multiple human languages allowing new compliant devices to be rapidly brought to market in multiple countries. Customers can also shop for devices and services that meet their requirements, such a meeting their defined minimal level of data encryption, thus allow business to more easily market the high value features of their products to mass market customers.

  Consider someone buying a prebuilt new home in the year 2025, the buyer will be looking at a home with integrated smart sensors, smart home appliances, each selected by builder or their subcontractor. Each of these will potentially have a separate set of terms and conditions, such as the Oven, fridge, washing machine, security motion sensor, fire alarm etc. just in an integrated kitchen alone. Currently as part of the legal information that the builder has to provide to a buyer certain paperwork, mainly focuses on legal liabilities governed by law which the buyer's solicitor will check on buyer behalf for any issues.

  In 2025 the buyer will also have to go through potentially dozens of sets of T&C before purchasing the property, the buyer may also need to check this with their insurer (e.g. who can access alarm data) and Mortgage company as they could affect the value of the property (such as the issues with zero priced solar panels & roof leases in the UK, example of devices). In addition to the smart devices, which may be tied to specific service, selected by the builder such as electrical power and water, the builder may have selected other services such as Fire and security monitoring services that are pre-configured as part of the smart home.

[The builder may have selected these as they provide free trials they can use to demonstrate the features, may be required to by law (Energy), their own backers (such as banks funding the development wanting fire/security monitoring to protect their investment), the smart device makers may offer a discounted price in return for connecting the service or the builder may be provided with finical incentives to “install” a service by a specific company. There will be business interest by service providers in getting builders to pre-select and configure their services on the grounds that inertia selling will convert a percentage of home buyers in to customers.]

The home purchaser will have to read though all the terms and conditions*, decide which he agrees with, which he does not, then go through the process to disable each of the devices/services they don’t accept the T&C for, add their own selected services before configuring the devices and services how they want. In theory as each of the devices and services is gathering data about the new owner, they should suspend their operation until the user has formally provided informed consent to the T&C in accordance to local laws.

This will require that smart devices and services do the following:

- Announce their presence to the new owner.
- Be able to display their terms and conditions directly to the user.
- Have some way for the new owner to accept the terms and conditions.
- Configure their preferences
- Be able to receive a revocation of permissions command and delete user configuration to trigger the above steps.

Another option would be for all machine to machine devices to be able to communicate this information to a user’s selected control devices e.g. a Smart Phone.

12.19.2 Source

REQ-2015-0619R02 Terms And Conditions Markup Language for Privacy Policy Manager

12.19.3 Actors

Names are based on the current European Union (EU) data protection definitions.

- Data subject. The living individual about who the data is captured. May or may not be the data owner.
- Data owner. The individual who owns the data. E.g. the home owner. Can be the data processor or a separate entity. [But also need to account for Non EU companies who may believe they own the data].
- Data processor. The entity who processes the data on behalf of the data owner

12.19.4 Pre-conditions

None

12.19.5 Triggers

None

12.19.6 Normal Flow

1. The profile owner configures a single set of profile's (house, work, personal, parental, legal etc.)
2. A new smart device or service is added:
3. Where the terms and conditions fall within the parameters set in the data subject's profile, the device can be automatically authorised (with a notification to the data subject).
4. If the T&C don't fall within the parameters set, only the differences (as a delta to the data subjects profile are presented to the data subjects for authorisation.
5. The data subject will not be able to override the parental/legal profile. Only the profile owner (e.g. parent/local government respectively) can override.
6. The data subject's privacy settings from their profile can be automatically configured where relevant, with confirmation notification to the data subject..

12.19.7 Alternative flow

Where it's not possible to fully configure the relevant security controls the data subject is alerted and can manually decide

12.19.8 Post-conditions

The data subject has given or refused informed consent for data capture for each oneM2M service based only on the deltas between each new service and the terms and conditions already accepted.

12.19.9 High Level Illustration

The concept of a Privacy Policy Manager (PPM), as described in TR-0016 [i.20] is

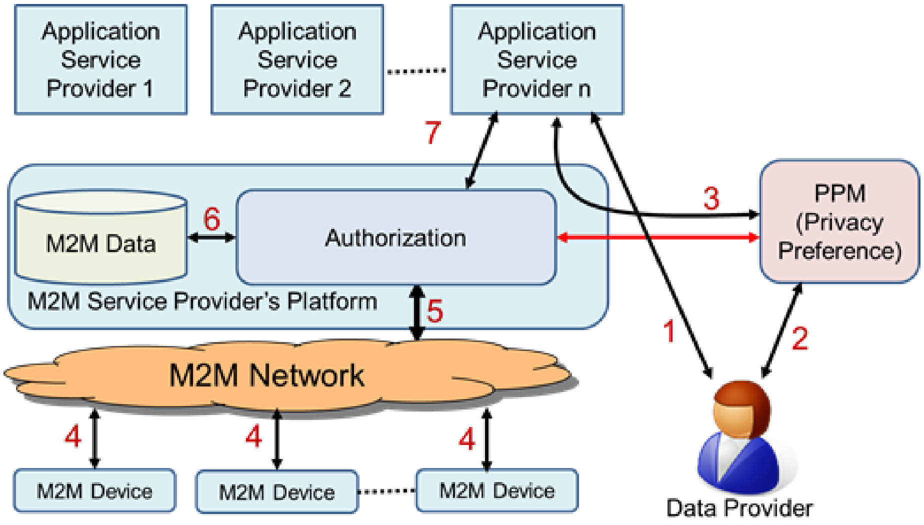
"The PPM had been adapted to large scale HEMS (Home Energy Management System) as trial, and they had started evaluation of PPM effectiveness.

The PPM is based on the following two main concepts:

- *Based on 'Privacy by Design', Inclusion in the architecture of a personal data distribution base.*

- *Based on 'Privacy First', the provision of an " end users function" by which end users can manage their own personal data distribution according to their privacy preferences."*

An overview of the proposal is shown below (Data Provider is the equivalent of Data Subject in UE data protection legislation).



Application Service Provider 1
Application Service Provider 2
Application Service Provider n
7
3
PPM (Privacy Preference)
6
M2M Data
Authorization
M2M Service Provider's Platform
5
1
2
M2M Network
4
4
4
M2M Device
M2M Device
M2M Device
Data Provider

Figure 82: Figure 12.19.9-1 Terms And Conditions Markup Language for Privacy Policy Manager

12.19.10 Potential requirements

1. The oneM2M system shall store and process privacy preferences in an interoperable manner.
2. The oneM2M system shall support privacy profiles at various levels to care for conditions of legal requirements, manufacturers, and data subjects.
3. The oneM2M system shall be able to prioritise privacy profiles where there is a conflict between profiles (legal profile takes priority over data subject profile, for example).

12.20 Intelligent agricultural product traceability

12.20.1 Description

Traceability is the ability to trace backward the history (e.g. operation, location) of an entity by means of recorded identifications. It is widely used in product life-cycle monitoring. Intelligence agriculture product traceability is a typical application.

Agricultural product traceability implements a mechanism to monitor and trace the supply chain, including all the participant parties, for example, the producer, processor, logistics providers, distributors, retailers and so on. Every party has a responsibility to manage traceability information by keeping disciplined record, so that the traceability application can obtain the life-cycle information accordingly.

The ***traceability information*** consists of static information (e.g. product name, date of production, process information of production) and dynamic information (e.g. logistics information, and distribution information). Most information is captured by the devices. For instance, during the production phase of agricultural products the traceability information is augmented with a planting monitoring log. The planting monitoring log is composed of temperature data and humidity data, which are collected by related sensors.

Another example is the traceability information gathered during processing phases, e.g. the chemical content and dosage monitored and recorded by sensors.

For traceability requirements, the traceability information should be associated with the product identifier which usually is a unique ID stored in two-dimension code or RFID tag.

Traceability linking provides a mapping that relates a product identifier to product related information such as

- Logs
- Information on ID service nodes, such as:
  - servers that provide access to traceability information, and
  - devices (sensors and gateways) that gather traceability information

The ***M2M service platform*** is an entity that is responsible to provide the traceability linking service.

The ***traceability application*** can request the M2M service platform to provide traceability linking service, and then obtain corresponding traceability information.

12.20.2 Source

REQ-2016-0043R05 Use Case Intelligence agricultural product traceability

12.20.3 Actors

- Traceability application

  Traceability application is the trace request initiator, which can capture traceability identifier (which is equal to, or can be transformed to product identifier) via typing or scanning. It initiates a trace request, and receives the traceability information. The traceability application is usually used by consumers or regulators.

- M2M service platform

  The M2M service platform is an entity that can maintain the traceability links for product identifier and product related information. The M2M service platform can respond to queries regarding traceability links related to a product identifier.

- ID service node

  The ID service nodes are

  – information servers that provide access to traceability information, and
  – devices (sensors and gateways) that gather traceability information

It can provide traceability linking services for product identifier and its corresponding information, forward the links to M2M service platform.

12.20.4 Pre-conditions

All ID service nodes register in the M2M service platform, and forward the existing traceability links for product identifier and traceability information.

12.20.5 Triggers

The traceability application captures a product identifier (traceability identifier), and initiates a trace request.

12.20.6 Normal Flow

1. The traceability application initiates a trace request.
2. The M2M service platform fetches all the traceability information related to the traceability identifier.
3. The M2M service platform provides the traceability information to the traceability application.
4. The traceability application requests the traceability information from ID service nodes.

12.20.7 Alternative flow

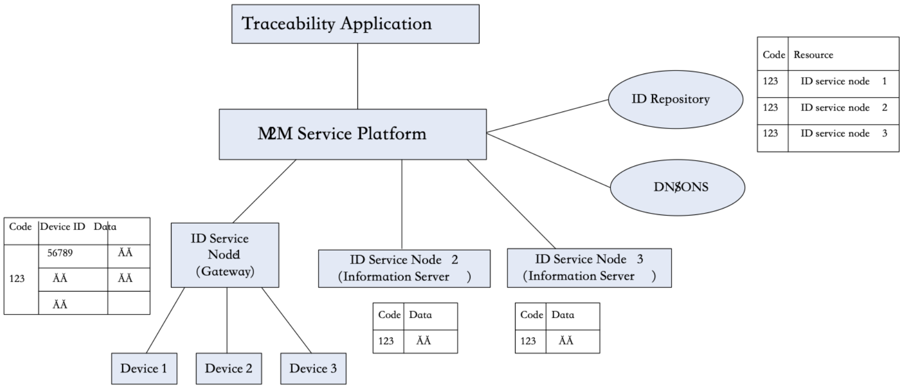
The traceability application can obtain the device identifier from M2M service platform, and access the device directly without ID service nodes.

In case the M2M service platform cannot provide accurate traceability information, it would forward the query to the ID service nodes and update the traceability link records.

12.20.8 Post-conditions

None

12.20.9 High Level Illustration


Traceability Application
M2M Service Platform
ID Repository
DNS/ONS
ID Service Node1 (Gateway)
ID Service Node 2 (Information Server)
ID Service Node 3 (Information Server)
Device 1
Device 2
Device 3

Code	Resource
123	ID service node 1
123	ID service node 2
123	ID service node 3

Code	Device ID	Data
123	56789	ÄÄ
	ÄÄ	ÄÄ
	ÄÄ	

Code	Data
123	ÄÄ

Code	Data
123	ÄÄ

Figure 83: Figure 12.20.9-1 Intelligent agricultural product traceability

12.20.10 Potential requirements

1. The oneM2M system shall be able to support the traceability linking service which provides a mapping that relates a product identifier to product related traceability information.

   Traceability information consists of:

   - Logs
   - Information on ID service nodes, such as:
     - i. servers that provide access to traceability information, and
     - ii. devices (sensors and gateways) that gather traceability information

2. The oneM2M system shall be able to enable applications to retrieve the traceability information related to product identifiers.

12.21 Support for configuration of and authentication to non-oneM2M node

12.21.1 Description

This use case is to provide support for authentication of oneM2M user applications to non-oneM2M vendor's specific node (server, or IoT application). The authentication is required to configure the non-oneM2M application through the user application. The objective is to ease IoT services developers to integrate with devices which their applications require to be authenticated to specific platforms. For example, it can be a camera with vendor specific cloud server which must authenticate the user or the application which configures the camera.

This is important to avoid that an attacker or a non autorised person control or configure the camera.

Let assume there are 3 communication channels between user application and vendor specific platform which is non-oneM2M node:

- communication channel for authentication,
- communication channel for node and stream configuration/control ,
- communication channel for data streaming. This is the classic stream used for data transport.

Those are introduced to simplify authentication and configuration of non-oneM2M platform provided by a vendor using an authentication method (standardized or proprietary). Communication channel for data streaming is out of oneM2M scope and is separated from configuration and authentication channels. The M2M System is used only for the authentication and configuration process.

This use case addresses needs of applications that require to register on non-oneM2M vendor specific applications or platforms. Please note that the camera and video streaming is given only as an example. Streamed data could be also photos, music, files, etc. Other data flows could be considered. The use case aims to highlight the need to configure and authenticate to non-oneM2M entities.

12.21.2 Source

REQ-2018-0001R05-TR-0001 use case for authentication to non-oneM2M devices.

12.21.3 Actors

Vendor specific node (application or server), AE (user application).

12.21.4 Pre-conditions

None

12.21.5 Triggers

- User Application wants to authenticate to non-oneM2M specific vendor node (authentication communication channel).
- User Application wants to change configuration of non-oneM2M specific vendor node or data streaming provided by this node (configuration/control communication channel).
- User Application wants non-oneM2M node to start streaming data (configuration/control communication channel).
- User Application wants non-oneM2M platform to stop streaming data (configuration/control communication channel).

12.21.6 Normal Flow

- Application entity wants to authenticate to non-oneM2M platform. To do so the user application (AE) sends the authentication request through the IoT Server (MN/IN-CSE) and Proxy-API using authentication communication channel. Proxy-API translates given request and forwards it to non-oneM2M platform. Then it responds using the same dataflow channel. This process is depicted in step 1 of Figure 12.21.9-1.
- Application entity wants to change configuration of non-oneM2M node or data stream. To do so AE sends the configuration change request through IoT Server (MN/IN-CSE) and Proxy-API using configuration communication channel. Proxy-API translates given request and forwards it to non-oneM2M node (device or platform). Then it responds using the same communication channel. This process is depicted in step 2 of Figure 12.21.9-1
- Application entity wants to control data streaming provided by non-oneM2M node (device or platform). To do so AE sends the control request through IoT Server (MN/IN-CSE) and Proxy-API using configuration/control communication channel. Proxy-API translates given request and forwards it to non-oneM2M platform. If it is needed it responds using the same communication channel. This process is also depicted in steps 2 of Figure 12.21.9-1 (same flow with configuration flow).

12.21.7 Alternative Flow

None

12.21.8 Post-conditions

None

12.21.9 High Level Illustration

Figure 12.21.9-1 depicts high level illustration of describing use case. Data streaming communication channel is out of one-M2M scope and is separated from authentication and non-oneM2M node configuration/control communication channels. According to Figure 12.21.9-1, it's possible for the Data streaming to be received by another user application(s).

12.21.10 Potential Requirements

- The M2M System must be able to distinguish between the raw dataflow and the configuration/control flow for the purpose of authentication.

- The M2M System must be able to provide an framework for end-to-end authentication of user application to the M2M vendor's specific node (non oneM2M).

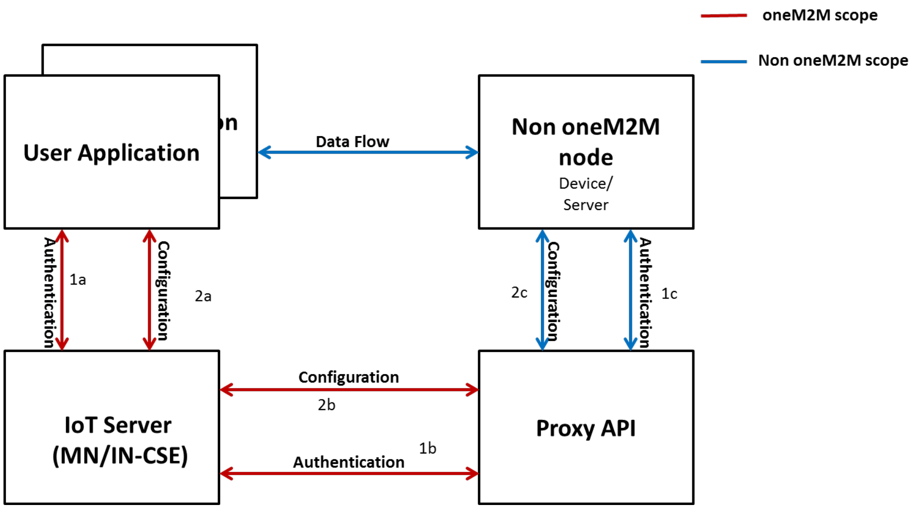


Figure 84: Figure 12.21.9-1 Call flow for configuration and authentication

12.22 Link Binding in Digital Twins and Edge/Fog Computing

12.22.1 Description

In a smart manufacturing use case in emerging Industry 4.0 and/or Industrial Internet, physical domain and cyber domain are connected via Internet technologies toward industrial Cyber-Physical Systems. Various sensors and actuators will be installed and/or attached to physical parts, machines, and devices in the physical domain so that their status and information will be effectively collected to the cyber domain or the Internet. On the other hand, reverse control commands may be issued from the cyber domain to a single physical part, machines, and/or devices. Smart manufacturing in general aims to render the manufacturing process more efficient, autonomous, and smart by leveraging Internet of Things (IoT) and the convergence of Information Technology (IT) and Operation Technology (OT) in product lifecycle, which could include four phases (i.e. conceive, design, realize, and service). For example, in the 'realize' phase, the product will be manufactured in a factory, sold to the customer, and delivered to the customer in sequential steps. The efficiency of those phases can be greatly improved based on IoT; for instance, IoT allows to collect more complete and timely information about a sold product and customer feedback during "service" phase, which in turn can feed to "realize" phase in a real-time fashion to eventually improve manufacturing efficiency.

To exploit the full range of benefits from smart manufacturing, the concept "digital twins" has been proposed. Basically, digital twins refer to digital or virtual companions of physical products; digital twins use collected data from sensors installed on physical products to represent their near real-time status, working condition, and/or other information. Through digital twins, a physical product can be monitored, managed, and maintained remotely and even more efficiently without sending any technician to check the product physically. **Digital twins actually necessitate link binding and resulted automatic content synchronization from physical products to their digital twins or vice versa,** for example:

- **Scenario 1:** In order to create digital twins in the cyber domain, the status of the physical product in each phase of its lifecycle needs to be monitored and connected. Then, a link binding between physical products (i.e. source resource) in the physical domain and their digital twins (i.e. destination source) in the cyber domain can be established to enable automatic content synchronization from sensors of a physical product to its digital twins.
- **Scenario 2:** some maintenance commands need to be automatically transferred from digital twins to the corresponding physical products; in this case, a link binding will be created between digital twins (i.e. source resource) and physical products (i.e. destination resource).

12.22.2 Source

REQ-2018-0030-Link_Binding_Management_in_Digital_Twins_and_Edge_Fog_Computing

12.22.3 Actors

- Source Resource Host (SRH): A logical entity which hosts source resources (e.g., an oneM2M CSE). A fog/edge node (e.g., a vehicle in physical domain) could be a SRH (or a DRH).
- Destination Resource Host (DRH): A logical entity which hosts destination resources (e.g., an oneM2M CSE). A cloud node (e.g., a server in cyber domain) could be a DRH (or a SRH).

- Link Binding Coordinator (LBC): A logical entity or a management application which manages link bindings between source resources and destination resources (e.g. to discover source resources and destination resources, to formulate appropriate link bindings, to create a link binding and set attributes of a binding entry, to update a link binding by changing the attributes of a binding entry, and to cancel a link binding, etc.). An oneM2M AE or CSE could be a LBC.
- Resource Creator (RC): A logical entity which creates source resources at a SRH or destination resources at a DRH. An oneM2M AE or CSE could be a RC.

12.22.4 Pre-conditions

- There are various products in physical domain and/or at the network edge, which act as a SRH for sending data to digital twins (or a DRH for receiving commands from digital twins).

- The physical product has an embedded service platform. There is an physical product application as a RC in physical product (or physical domain) to create resources about the physical product in the embedded service platform. The physical product application usually resides at the network edge.
- Each physical product has its digital twin in cyber domain and/or in the cloud, which act as a DRH for collecting data from physical products (or a SRH for sending commands to physical products).
- The digital twin of a physical prodct maintain resources for the physical product.

- There is a management application as LBC to manage link bindings between physical products and their corresponding digital twins in cyber domain. The management application can be residing in the cloud.

12.22.5 Triggers

- New physical products are introduced and their digital twins are created. The management application as LBC establish link bindings between new physical products and their digital twins.

12.22.6 Normal Flow

Figure 12.22.6-1 illustrates the normal flow for link binding management for the scenario where physical products play as SRH to report data to their digital twins as DRH. Note that the similar flow can be applied to the case when digital twins play as SRH to send commands to physical products as DRH.

1. Step 1: The physical product application as a RC creates source resources at the SRH. In the meantime, the RC provides binding support in this process along two aspects: 1) The RC can indicate certain binding hints for the resource to be created. The binding hints could be the binding role of the resource (i.e. source resource, or destination resource), the type of the resource to be bound to, binding attributes the resource can support, etc. Such binding hints could be provided to the RC via a user interface or previsioned to the RC. 2) The RC can also create link binding in this step. In other words, the RC creates new resources and new link bindings simultaneously. For example, when creating a source resource at the SRH, the RC can provide the destination resource and binding attributes to the SRH and accordingly create a link binding from the resource to be created to the destination resource at the SRH (i.e. for Push mode).
2. Step 2: The management application as a LBC discovers appropriate resources (i.e. source resources and destination resources) from the DRH and the SRH. The LBC will provide new filters related to link binding such as link binding role (i.e. source resource or destination resource), binding attributes which the resource to be discovered can support, etc.

Based on those new filters, more appropriate resources for link binding will be identified and returned from the DRH/SRH to the LBC. Before discovering any resource, the LBC basically does not know if a resource host maintains source resources, destination resources, or both. It just simply issues a resource discovery request to a resource host; the resource discovery request will indicate whether it intends to search source resources or destination resources.

3. Step 3: The LBC triggers to create a link binding at the DRH for Poll/Observe mode or at the SRH for Push mode. In either case, the LBC instructs both the DRH and the SRH to be aware of each other's context information and binding attributes of the created link binding. Alternatively, the SRH can initiate to send a request to the DRH to create the link binding for Poll/Observe mode and similarly the DRH can initiate to send a request to the SRH to create the link binding for Push mode.

4. Step 4: Based on the created link binding in Step 3, binding-aware content synchronization will be repeatedly conducted from the SRH to the DRH. In Poll/Observe mode, the DRH will send RETIREVE/GET messages to the SRH (and accordingly a response message to GET will be sent from the SRH to the DRH), while UPDATE/PUT messages will be sent from the SRH to the DRH for Push mode (and accordingly a response message to PUT will be sent from the DRH to the SRH). In either case, link binding indicator such as binding attributes can be contained in GET or PUT messages so that the SRH or the DRH knows that the corresponding context exchange is not an ordinary one-time content exchange, but repeatable content synchronization due to a link binding. As such, both the SRH and the DRH are aware of binding attributes during content synchronization and in turn can be better prepared (e.g. adjust its sleep schedule) for content synchronization in the future. Being aware of binding attributes, the SRH (or the DRH) can also authenticate whether each received GET message (or PUT message) satisfies the conditions as specified in binding attributes.
5. Step 5: An established link binding can be updated by the LBC, the DRH, or the SRH. Link binding update can be triggered under various conditions. For example, the LBC may update the link binding with a more frequent content synchronization. The source resource or the destination resource involved in the link binding can also be changed to a new resource.

6. Step 6: An established link binding can be suspended by the LBC, the DRH, or the SRH. Link binding suspension can be triggered under various conditions. For example, the DRH under Push mode may request to halt a link binding at the SRH when it is too overloaded to receive any future PUT messages from the SRH; similarly, the SRH under Pull mode may request to pause a link binding at the DRH when it aims to reduce energy consumption by stopping receiving future GET messages from the DRH.

7. Step 7: A halted link binding can be restored or resumed after certain time by the LBC, the DRH, or the SRH. Link binding restoration can be triggered under various conditions. For example, the DRH under Push mode may request to resume the halted link binding at the SRH when it becomes underloaded and able to receive PUT messages from the SRH; similarly, the SRH under Pull mode may request to resume the halted link binding at the DRH.
8. Step 8: An existing link binding may be removed by the LBC, the DRH, or the SRH for various scenarios. For example, the LBC may just simply cancel the link binding and disable the content synchronization; in this case, both the source resource and the destination resource are still kept. In another example, when the source resource becomes unavailable, the link binding is actually invalid and needs to be removed accordingly.

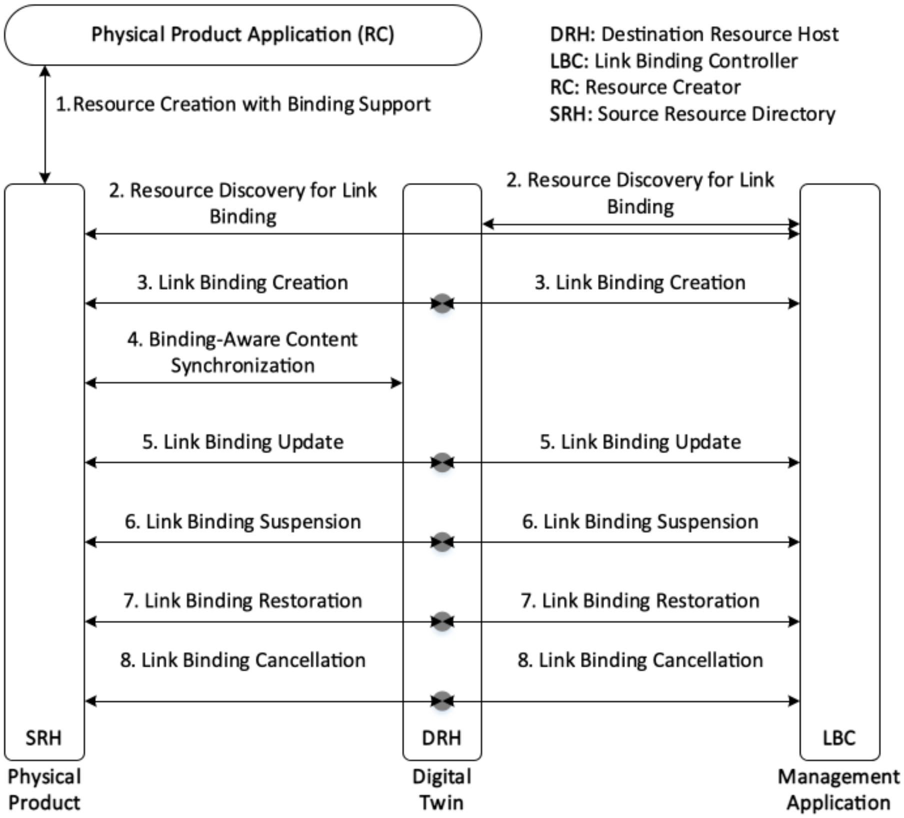

Physical Product Application (RC)
DRH: Destination Resource Host
LBC: Link Binding Controller
RC: Resource Creator
SRH: Source Resource Directory
1. Resource Creation with Binding Support
2. Resource Discovery for Link Binding
2. Resource Discovery for Link Binding
3. Link Binding Creation
3. Link Binding Creation
4. Binding-Aware Content Synchronization
5. Link Binding Update
5. Link Binding Update
6. Link Binding Suspension
6. Link Binding Suspension
7. Link Binding Restoration
7. Link Binding Restoration
8. Link Binding Cancellation
8. Link Binding Cancellation
SRH
DRH
LBC
Physical Product
Digital Twin
Management Application

Figure 85: Figure 12.22.6-1 Normal Flow - Link Binding Management

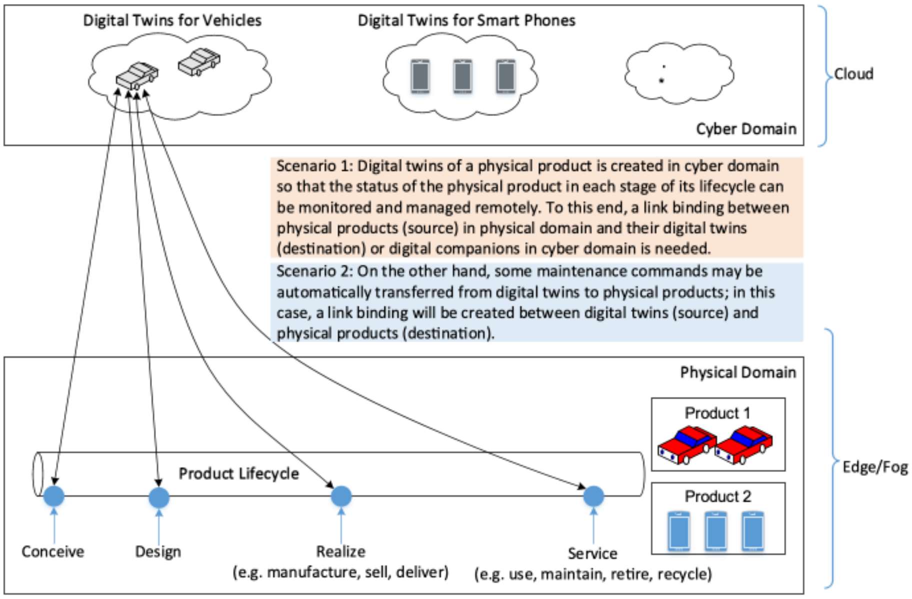
12.22.7 Alternative Flow

None

12.22.8 Post-conditions

- After appropriate link bindings are established between a physical product and its digital twin, they automatically exchange data and command accordindg to the established link bindings.

12.22.9 High Level Illustration


Digital Twins for Vehicles
Digital Twins for Smart Phones
Cloud
Cyber Domain
Physical Domain
Product 1
Product 2
Edge/Fog
Product Lifecycle
Conceive
Design
Realize
(e.g. manufacture, sell, deliver)
Service
(e.g. use, maintain, retire, recycle)

Scenario 1: Digital twins of a physical product is created in cyber domain so that the status of the physical product in each stage of its lifecycle can be monitored and managed remotely. To this end, a link binding between physical products (source) in physical domain and their digital twins (destination) or digital companions in cyber domain is needed.

Scenario 2: On the other hand, some maintenance commands may be automatically transferred from digital twins to physical products; in this case, a link binding will be created between digital twins (source) and physical products (destination).

Figure 86: Figure 12.22.9-1 High Level Illustration - Link Binding in Digital Twins

12.22.10 Potential requirements

1. The oneM2M System shall enable methods to identify resource link-binding roles, such as source resource and destination resource.
2. The oneM2M System shall enable the link binding between a source resource and a destination resource.
3. The oneM2M System shall enable to create link bindings between a source resource and a destination resource.
4. The oneM2M System shall enable to update link bindings between a source resource and a destination resource.
5. The oneM2M System shall enable to cancel link bindings between a source resource and a destination resource.

12.23 Automatic ontology mapping.

12.23.1 Description

In M2M applications, reusing of common ontologies (e.g. location, time ontologies, etc.) plays an important role in developing cost effective and high-quality ontologies. It could save the cost and time required for the ontology construction of specific domains.

For example, a user wants to build ontology to provide syntactic and semantic interoperability of the smart home System. He could reuse some existing ontologies (e.g. the oneM2M Base Ontology, sensor ontologies, environment ontologies) and build his own ontology by mapping them.

Ontology mapping is to find the mapping relationships between different ontologies to reuse ontologies. Ontology mapping can be implemented either by manual approaches or automatic approaches. However, discovering manually mappings is often too labour-intensive, error-prone, and impractical for large heterogeneous ontologies. Therefore, oneM2M system needs to automatically discover, create and save the mappings (equivalent or inherited relationships) between semantically related ontology entities by using industry-proven mapping algorithms, e.g. the edit distance, language-based similarity, structural-based similarity, or external- resources-based similarity etc.

12.23.2 Source

REQ-2018-0048R04 Use case for automatic ontology mapping

12.23.3 Actors

- End User: the user who wants to build his own ontology by mapping existing ontologies.
- The ontology is a vocabulary with a structure. It could capture a shared understanding of a domain of interests and provide a formal and machine interpretable model of the domain. It may be mapped to others with the help of ontology mapping function.
- Ontology Mapping Function is responsible for discovering, creating and saving mappings between the ontologies defined in the context of the oneM2M System and/or other external ontologies. It is a service layer functionality provided by the oneM2M System.
- The ontology mapping file is a RDF document including the mappings between ontologies. It can be saved and managed in the oneM2M System as a resource.

12.23.4 Pre-conditions

None

12.23.5 Triggers

An ontology is required to be mapped to other ontologies automatically.

12.23.6 Normal Flow

The normal message flow is described as follows:

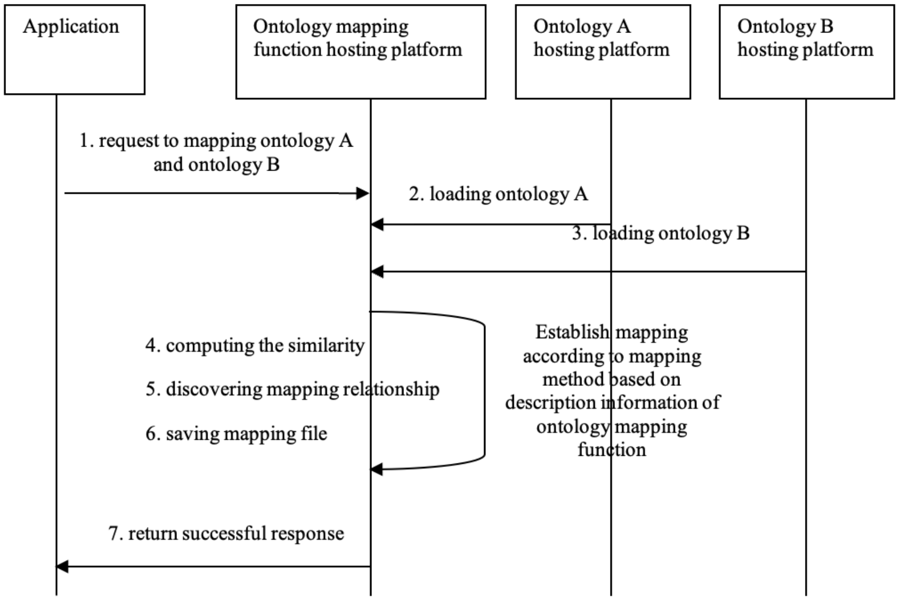

Application
Ontology mapping function hosting platform
Ontology A hosting platform
Ontology B hosting platform
1. request to mapping ontology A and ontology B
2. loading ontology A
3. loading ontology B
4. computing the similarity
5. discovering mapping relationship
6. saving mapping file
Establish mapping according to mapping method based on description information of ontology mapping function
7. return successful response

Figure 87: Figure 12.23.6-1 Message flow for automatic ontology mapping operation

1. An application (representing the End User) sends a request for mapping ontology A and ontology B to the ontology mapping function in the oneM2M platform.
2. An ontology A is loaded into the ontology mapping function.
3. Another ontology B is loaded into the ontology mapping function.
4. The similarities between entities (classes, properties, instances.) of ontologies are computed by the ontology mapping function.
5. Mapping discovery is performed based on similarity between entities and other helpful information like synonyms, hypernym-hyponym relations from external knowledge bases by the ontology mapping function.
6. The mapping result between Ontology A and Ontology B is saved as an ontology mapping resource by ontology mapping function.
7. The mapping result (e.g. resource id) is return to the application.

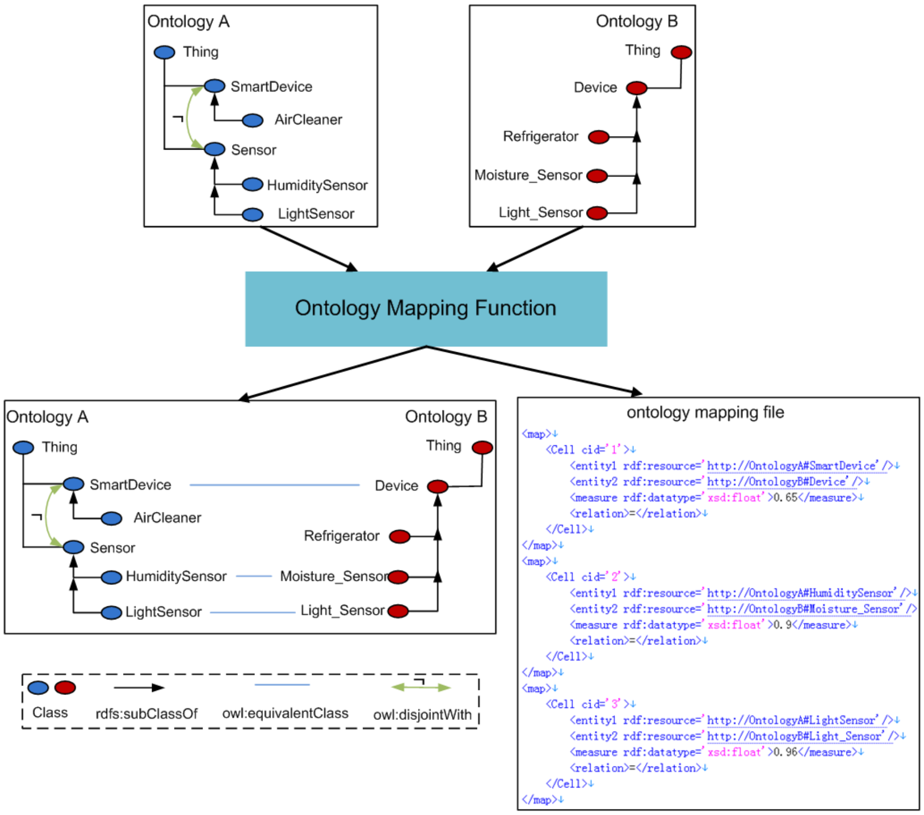
12.23.7 Alternative flow

None

12.23.8 Post-conditions

None

12.23.9 High Level Illustration



```
<map>↓
    <Cell cid='1'>↓
        <entity1 rdf:resource='http://OntologyA#SmartDevice'/>↓
        <entity2 rdf:resource='http://OntologyB#Device'/>↓
        <measure rdf:datatype='xsd:float'>0.65</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
<map>↓
    <Cell cid='2'>↓
        <entity1 rdf:resource='http://OntologyA#HumiditySensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Moisture_Sensor'/>
        <measure rdf:datatype='xsd:float'>0.9</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
<map>↓
    <Cell cid='3'>↓
        <entity1 rdf:resource='http://OntologyA#LightSensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Light_Sensor'/>↓
        <measure rdf:datatype='xsd:float'>0.96</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
```

Figure 88: Figure 12.23.9-1 Ontology Mapping High Level Illustration

12.23.10 Potential requirements

1. The oneM2M System shall be able to automatically discover and create semantic mappings between ontologies and save them as resources.

12.24 Ontology mapping conflict detection and repair.

12.24.1 Description

Ontology mapping is an effective way to reuse existing ontologies to provide semantic support for M2M applications. Whether ontology mapping is implemented by manual approaches or automatic approaches, there are often semantic conflicts among candidate mappings. These conflicts will make the mapped ontology becoming incoherent, so the oneM2M system shall be able to detect these conflicts among mappings and repair them.

12.24.2 Source

REQ-2018-0049R03 Use case for ontology mapping conflict detection and repair.

12.24.3 Actors

- End User: the user who wants to detect and repair the conflicts among mapping relationships between ontologies.
- The ontology is a vocabulary with a structure. It could capture a shared understanding of a domain of interest and provide a formal and machine interpretable model of the domain. It may be mapped to others with the help of ontology mapping function.
- Ontology Mapping Function is responsible for discovering, creating and saving mappings between the ontologies defined in the context of the oneM2M System and/or other external ontologies. It is a service layer functionality provided by the oneM2M System.
- The ontology mapping file is a RDF document including the mappings between ontologies. It can be saved and managed in the oneM2M System as a resource.
- Ontology Mapping Conflict Detection & Repair Function is responsible for detecting and repairing conflicts among the mappings between the ontologies defined in the context of the M2M System and/or other external ontologies. It is a service layer functionality provided by the oneM2M System.
- The repaired ontology mapping file is a RDF document including the mappings without conflicts between ontologies. It can be saved and managed in the oneM2M System as a resource.

12.24.4 Pre-conditions

The conflict among mappings is a kind of logical incoherence.

12.24.5 Triggers

There is logical inconsistency in the mapped ontology according to the existing mappings.

12.24.6 Normal Flow

The normal message flow is described as follows:

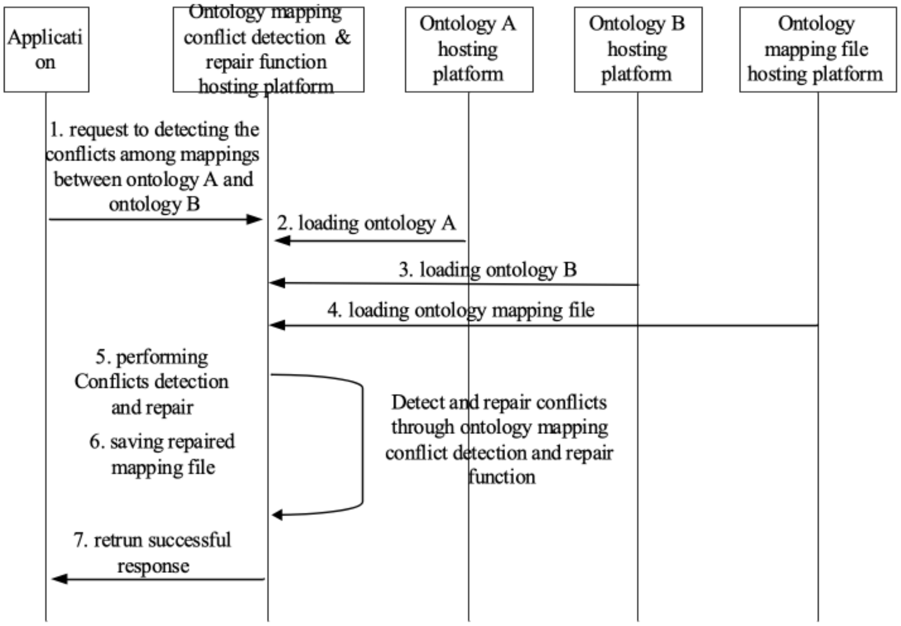

Applicati
on
Ontology mapping conflict detection & repair function hosting platform
Ontology A hosting platform
Ontology B hosting platform
Ontology mapping file hosting platform
1. request to detecting the conflicts among mappings between ontology A and ontology B
2. loading ontology A
3. loading ontology B
4. loading ontology mapping file
5. performing Conflicts detection and repair
6. saving repaired mapping file
Detect and repair conflicts through ontology mapping conflict detection and repair function
7. retrun successful response

Figure 89: Figure 12.24.6-1 Message flow for ontology mapping conflict detection and repair operation

1. An application (representing the End User) sends a request for detecting and repairing the conflicts among mappings between ontology A and ontology B to the ontology mapping conflict detection function in the oneM2M platform.
2. An ontology A is loaded into the ontology mapping conflict detection function.
3. Another ontology B is loaded into the ontology mapping conflict detection function.
4. The ontology mapping file including the mappings between ontology A and ontology B is loaded into the ontology conflict detection function.
5. Conflicts detection and repair is performed from the mappings by the ontology conflict detection and repair function.
6. The repaired mapping result is saved as an ontology mapping resource by ontology mapping conflict detection and repair function.
7. The repaired mapping result (e.g. resource id) is return to the application.

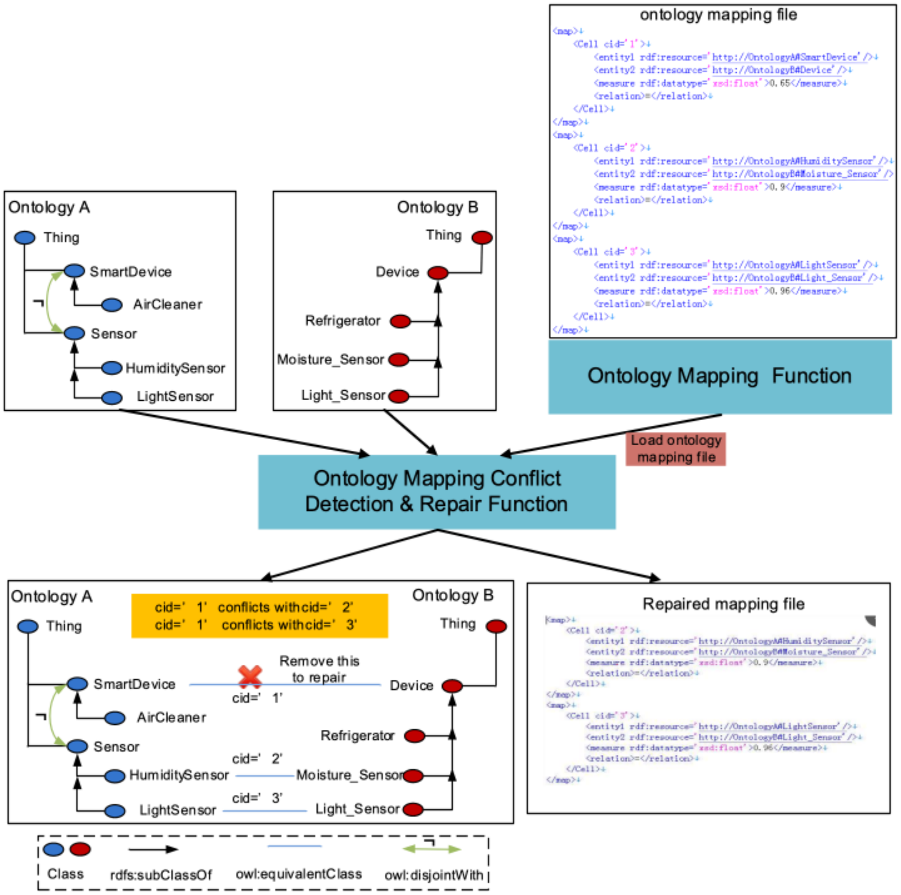
12.24.7 Alternative flow

None

12.24.8 Post-conditions

None

12.24.9 High Level Illustration



ontology mapping file

```
<map>↓
    <Cell cid='1'>↓
        <entity1 rdf:resource='http://OntologyA#SmartDevice'/>↓
        <entity2 rdf:resource='http://OntologyB#Device'/>↓
        <measure rdf:datatype='xsd:float'>0.65</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
<map>↓
    <Cell cid='2'>↓
        <entity1 rdf:resource='http://OntologyA#HumiditySensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Moisture_Sensor'/>
        <measure rdf:datatype='xsd:float'>0.9</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
<map>↓
    <Cell cid='3'>↓
        <entity1 rdf:resource='http://OntologyA#LightSensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Light_Sensor'/>↓
        <measure rdf:datatype='xsd:float'>0.96</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
```

Repaired mapping file

```
<map>↓
    <Cell cid='2'>↓
        <entity1 rdf:resource='http://OntologyA#HumiditySensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Moisture_Sensor'/>↓
        <measure rdf:datatype='xsd:float'>0.9</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
<map>↓
    <Cell cid='3'>↓
        <entity1 rdf:resource='http://OntologyA#LightSensor'/>↓
        <entity2 rdf:resource='http://OntologyB#Light_Sensor'/>↓
        <measure rdf:datatype='xsd:float'>0.96</measure>↓
        <relation>=</relation>↓
    </Cell>↓
</map>↓
```

Figure 90: Figure 12.24.9-1 Ontology mapping conflict detection and repair - High-level Illustration

12.24.10 Potential requirements

1. The oneM2M system shall be able to detect ontology's mapping conflicts and repair them.

12.25 Semantic query/discovery based on automatic ontology mapping

12.25.1 Description

Semantic descriptions in the oneM2M system can be annotated in heterogeneous ontologies given the data and knowledge can be generated from different domains and stakeholders. In many cases, heterogeneous ontologies may have common/similar concepts that are mappable (linked) between each other. Such mapping relationship is useful to get a more comprehensive result of semantic query/discovery. For example, the oneM2M system can return the semantic instances of both "Ontology-A: light" and "Ontology-B: lamp" for someone querying for a generic "light" device.

Automatic ontology mapping (described in clause 12.23) is to find the mapping relationships between different ontologies to reuse ontologies.

After completing the automated ontology mapping, the semantic query/discovery process can leverage the mapping knowledge to generate a more complete and accurate results.

12.25.2 Source

REQ-2018-0055R01 Use case for semantic query and discovery based on ontology mapping

12.25.3 Actors

- Application: the user who wants to do semantic query/discovery across heterogeneous ontologies.
- oneM2M Platform: an oneM2M CSE that supports semantic query/discovery based on ontology mapping.

12.25.4 Pre-conditions

- The oneM2M System stores semantic description of resources annotated in different ontologies (e.g. A & B).
- The ontology mapping results are saved and managed in the oneM2M System as a resource.

12.25.5 Triggers

The application issues a semantic query/discovery request to the oneM2M platform indicating the use of automatic ontology mapping.

Normal Flow

The normal message flow is described as follows:

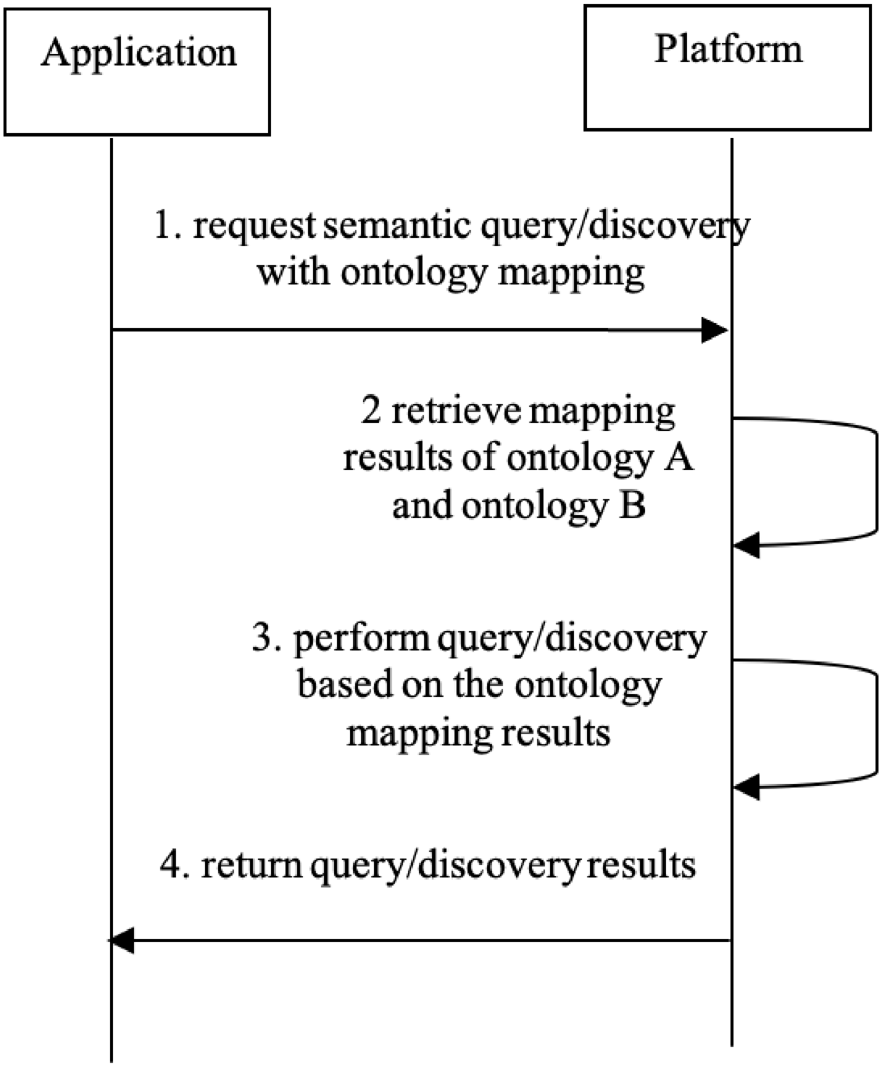

Application
Platform
1. request semantic query/discovery with ontology mapping
2 retrieve mapping results of ontology A and ontology B
3. perform query/discovery based on the ontology mapping results
4. return query/discovery results

Figure 91: Figure 12.25.6-1 Message flow for semantic query/discovery supported with automatic ontology mapping

1. An application sends a semantic query/discovery request to the oneM2M platform to query/discovery the semantic description of certain resources. The semantic query/discovery request contains semantic filter criteria described in ontology A, but also indicates that equivalent (or related) semantic description annotated in ontology B should be returned.
2. After receiving the query/discovery request, the oneM2M platform first retrieves mapping results of ontology A and ontology B.
3. The oneM2M platform then performs the semantic query/discovery combing the knowledge of the mapping results between ontology A and ontology B. This may be done by converting the semantic filter criteria or the target semantic descriptions according to the ontology mapping results.
4. The oneM2M platform returns the query/discovery results, which contains the matching semantic descriptions annotated in both ontology A and B, to the application

12.25.7 Alternative Flow

None

12.25.8 Post-conditions

None

12.25.9 High Level Illustration

None

12.25.10 Potential requirements

1. The oneM2M system shall be able to support semantic query and discovery across heterogeneous ontologies including the support of automatic ontology mapping.

12.26 Semantic control based on automatic ontology mapping

12.26.1 Description

Semantic descriptions in the oneM2M system can be annotated in heterogeneous ontologies given the data and knowledge can be generated from different domains and stakeholders. In many cases, heterogeneous ontologies may have common/similar concepts that are mappable (linked) between each other. Such mapping relationship is useful to get a more effective and precise command of semantic control.

In this use case, semantic control refers to sending an oneM2M primitive which contains semantic triples that represent some control command(s) targeting at a device. Such control commands may be pertaining to a certain ontology.

For example, the control command for device A is “turn on/off” according to Ontology-A, while the same command for device B could be “switch on/off” according to Ontology-B.

A oneM2M application may understand only Ontology-A (not Ontology-B) so that it can normally interact with only device A (not device B) by sending control commands (“turn on/off”) as the semantic payload in the oneM2M primitives (such as CREATE a <contentInstance> resource with the content of RDF triples that contains the semantic description of “turn on/off”).

With the capability of automatic ontology mapping (described in clause 12.23), oneM2M system is able to find the mapping relationships between ontology A and B, so that it has the possibility to convert the semantic control command into different ontologies for different target devices on behalf of the application.

12.26.2 Source

None

12.26.3 Actors

- Application: the entity performs semantic control with limited knowledge of device ontologies.
- oneM2M Platform: an oneM2M CSE that supports semantic control based on ontology mapping.

12.26.4 Pre-conditions

- The oneM2M System stores semantic description of resources annotated in different ontologies (e.g. Ontology-A & Ontology-B).
- The ontology mapping results are saved and managed in the oneM2M System as a resource.

12.26.5 Triggers

- The application issues a semantic control request to the oneM2M platform indicating the use of ontology mapping.

12.26.6 Normal Flow

The normal message flow is described as follows:

1. An application sends a semantic control request to the oneM2M platform for controlling different devices (device A and device B) that are described based on different ontologies (Ontology-A and Ontology-B respectively). The semantic control request contains a control command based on ontology B and it also indicates the use of ontology mapping result between Ontology-A and Ontology-B

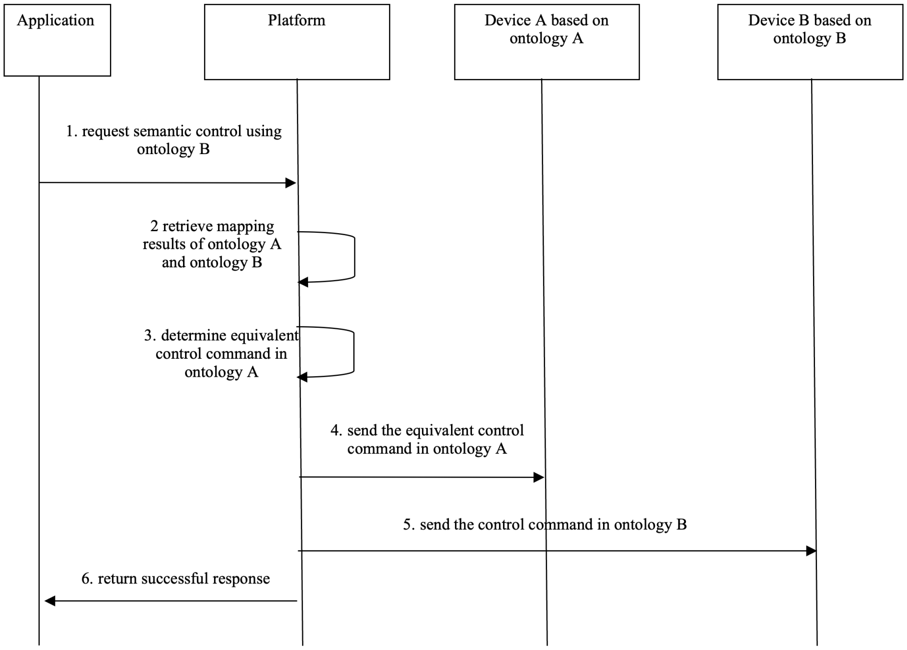

Application
Platform
Device A based on ontology A
Device B based on ontology B
1. request semantic control using ontology B
2 retrieve mapping results of ontology A and ontology B
3. determine equivalent control command in ontology A
4. send the equivalent control command in ontology A
5. send the control command in ontology B
6. return successful response

Figure 92: Figure 12.26.6-1 Message flow for semantic control based on automatic ontology mapping operation

2. After receiving the semantic control request, the platform (e.g. IN-CSE) first retrieves the mapping results between Ontology-A and Ontology-B.
3. The oneM2M platform then can determine an equivalent control command described in Ontology-A for device A according to the ontology mapping results;
4. The platform sends the equivalent control command in Ontology-A to device A;
5. The platform sends the original control command in Ontology-B to device B;
6. The platform returns a successful response to the application.

12.26.7 Alternative Flow

None

12.26.8 Post-conditions

None

12.26.9 High Level Illustration

None

12.26.10 Potential requirements

1. The oneM2M system shall support semantic control of devices described in heterogeneous ontologies including the support of automatic ontology mapping.

12.27 Cooperative Fog Services with Drones

12.27.1 Description

Drones with fog capabilities can be operated in many environments and applications, such as supply chain delivery, environment surveillance and video broadcasting, providing near real-time adjustments and collaboration in response to anomalies, operational changes or threats. With various capabilities such as computing, sensing, video recording, data storage, and communicating, drones can act as fog nodes, which interoperate and cooperate as a dynamic community to efficiently distribute services across compute, storage, networking, security, and other functions.

In many scenarios, a request of fog service may require a cluster of drones to operate cooperatively to provide the required capabilities and complete the task, since each drone itself is limited by the capabilities or coverage. In this case, the fog service request will first be split into smaller “pieces” with each piece containing a portion of capability requirements, such that they can be handled by the fog nodes jointly. For example, in an environment surveillance scenario, each drone can only monitor a limited area, so surveillance over a large area may require the combination and synergy from multiple drones' monitoring where each drone is responsible for a sub-area under its coverage. Similarly, a computation intensive video analysis task may exhaust the battery of a drone rapidly, or the limited computation speed of a drone cannot meet the real-time processing requirements, in which case the task can be split and distributed to multiple drones to be completed efficiently. Moreover, a drone may need another's communication capability to help relay messages to a destination out of its reach.

The cooperation is also necessary when considering the dynamic availability of drones due to mobility and limited power supply. A drone low in power might be turned off until it is recharged, during which time the associated fog capabilities are lost and may need to be accommodated by other drones. A drone flying away from some area may look for a replacement to continue the ongoing service in this area. Therefore, in addition to tracking drones in-service, the coordination algorithms require tracking of drones in other states, e.g. available (but not in-service), partially in-service, etc. This results in a coordination scheme which not only associates drones into a cluster but also adapts to the dynamic capability distribution within the group.

12.27.2 Source

REQ-2018-0072R02 Use Case for Cooperative Fog Service

12.27.3 Actors

- Fog Node: A fog node is a node with certain types of fog capabilities or resources such as computing, storage, control, networking, that can be shared with and leveraged by users and other fog nodes. A fog node may have one or multiple types of capabilities, may also have other software or services that are running on the node. A fog node can be located at the edge of deployment or higher layers. The fog nodes, especially the ones close to the edge, are considered to have limited capabilities compared to the cloud, and the capabilities may not be available all the time.
- Fog Leader: Fog leader is a fog node that will coordinate and combine other fog nodes together to serve a fog service request which demands large fog capabilities and cannot be completed at a single fog node. A fog leader will form both potential group(s) for fog capability discovery, and service group(s) for serving fog service requests. The fog leader could be located at any layer of the fog hierarchy, as long as it is capable of forming potential groups, creating service groups, and adjusting service groups.
- User/Requestor: A user/requestor is the entity that may send a fog service request to the fog leader. The request may ask for completing a task, reserving capabilities for a period of time or consistently providing fog service.

12.27.4 Pre-conditions

- Fog nodes are deployed, each willing to share (part of) its fog capabilities.
- Fog nodes may have discovered nearby (geographically or logically) fog nodes.
- At least one fog node is willing and capable to act as the fog leader to coordinate several fog nodes in completing a request.

12.27.5 Triggers

- A (potential) fog service request requires multiple fog nodes' capabilities to fulfil.
- The capability of a fog node changes.
- A new fog node enters the coverage of a fog leader, or a fog node leaves the coverage of a fog leader.

12.27.6 Normal Flow

Figure 12.27.6-1 illustrates the high-level flows of cooperative fog service use case, which consists of the following steps:

- Step 1: The fog leader may discover capabilities of fog nodes that can potentially cooperate on a future fog service request. The capability of a fog node may include computing (with CPU resource), storage (with memory resource), communication (with bandwidth resource), sensing, controlling, actuating (with firmware or software resource), etc. The fog leader may track the status of the potential fog nodes as well as their capabilities, which may later be used as the reference or hints when selecting nodes to complete a fog service request.
- Step 2: The user sends a fog service request to the fog leader. The request may ask for a certain amount of resources (e.g. 1GB data storage) to be reserved for a period of time, or to complete a task with or without a completion time constraint (e.g. perform data analysis on the video data generated from equipped cameras (within 5 minutes)), or to provide consistent service (e.g. monitor the traffic density of the downtown area and calculate optimal path).
- Step 3: Based on the received request, the fog leader selects a group of fog nodes and reserves capabilities from the nodes for the request.
- Step 3.1: After receiving a request, the fog leader will first interpret the request to get information of what and how much capabilities are required, and select fog nodes to satisfy the requirements. Based on that, the request will be split into sub-requests for each selected fog node with each containing a relatively small portion of capability requirements such that they can be handled by the fog nodes cooperatively. For example, the request may ask the drones to monitor the environment in a large area, while each drone can only cover a small area. In this case, the request will be divided into sub-requests with each one corresponding to a sub-area

covered by one drone, and the leader will then merge the results collected from the drones to complete the request. Moreover, the request may ask for a storage size or computation speed that exceeds the capacity of a drone, in this case the request can be sliced into “smaller” sub-requests and jointly completed by multiple drones. The request can also be split in the time domain according to the predicted availability of fog nodes in case some fog nodes are only available for a limited period of time. For example, a 24-hour surveillance request can be split into day-time and night-time sub-requests and assigned to different sets of drones, where the day-time working drones will be turned off for recharging during night-time and their place taken by the night-time working drones.

- Step 3.2: After splitting, the sub-requests will be distributed to the selected group of fog nodes along with the capability requirements for each fog node.
- Step 3.3: The fog nodes reserve capabilities according to the received sub-requests.
- Step 3.4: After reserving the required capabilities, the fog nodes send responses to the fog leader indicating whether the reservation is successful.
- Step 4: The fog leader sends a response to the user indicating whether the request can be completed.
- Step 5: Under the coordination of the fog leader, the group of selected fog nodes will provide fog service with the reserved capabilities, or the user will start to use the fog services provided by the fog nodes. Dynamics or changes during this step may trigger service update in the next step.
- Step 6: The capabilities of the in-service fog nodes may be changing and result in group dynamics. The update of fog service request, receiving multiple requests competing for the same fog node’s capabilities, or a time sequential request may also trigger the group dynamics since the leader will need to make adjustments to the group to adapt to the changes. As such, the fog leader needs to perform dynamic group management or service update accordingly.
- Step 7: After the fog request is completed or the subscription/lease of fog capabilities terminates, the reserved fog capabilities will be released.

12.27.7 Alternative Flow

None

12.27.8 Post-conditions

None

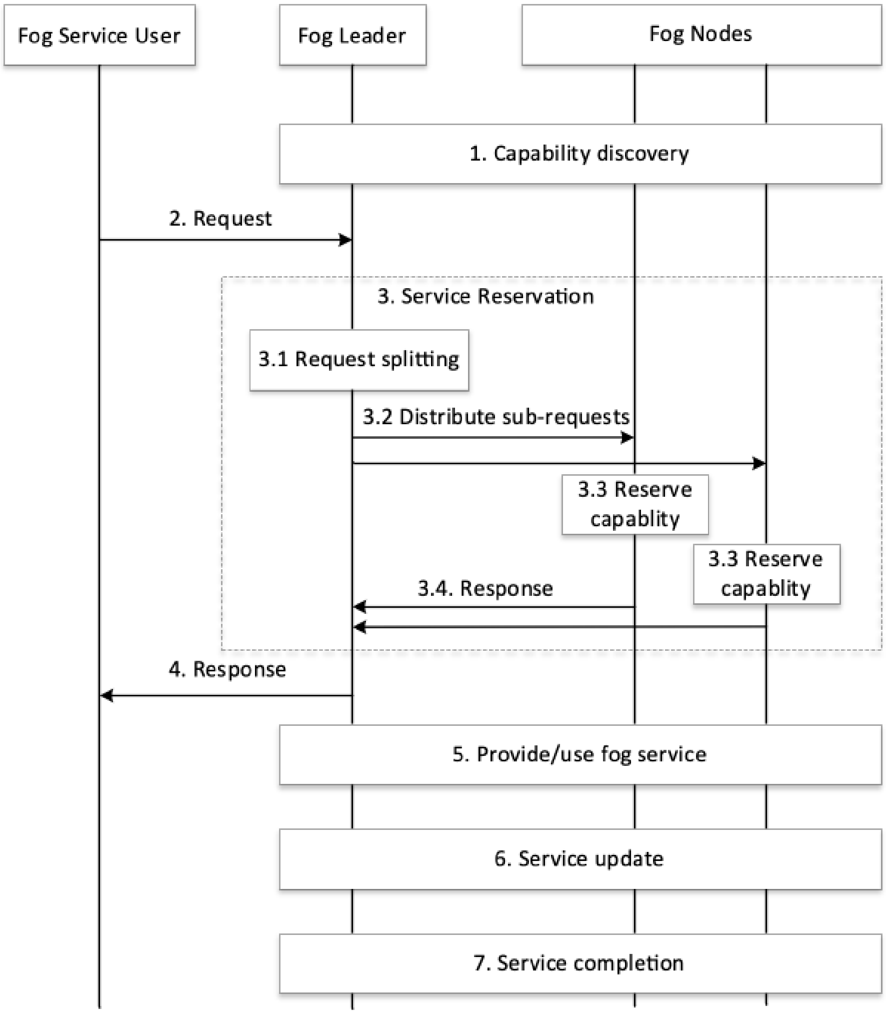


Figure 93: Figure 12.27.6-1 Normal Flow - Cooperative fog service

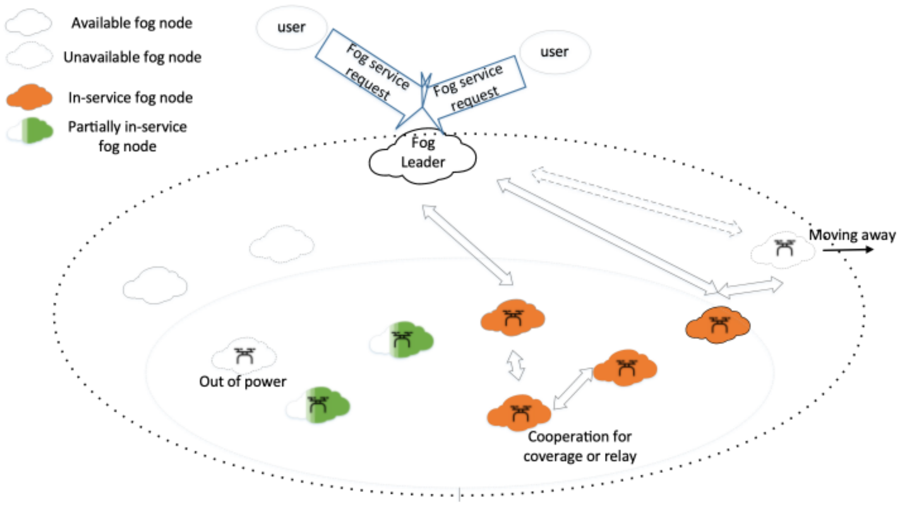


Figure 94: Figure 12.27.9-1 High Level Illustration - Cooperative Fog Service

12.27.9 High Level Illustration

12.27.10 Potential requirements

1. The oneM2M System shall enable a fog node to identify fog nodes that can potentially cooperate to complete a request and to track their capabilities (e.g. battery level, available memory) in an efficient manner.
2. The oneM2M System shall enable a fog node to select a group of fog nodes to cooperate on a fog service request, and split the request into multiple sub-requests according to the type, amount, and availability of the selected fog nodes' capabilities, such that the capability requirement in each sub-request will not exceed the capacity of the corresponding fog node.
3. The oneM2M System shall enable a fog node to coordinate a group/cluster of fog nodes to provide services to a user.
4. The oneM2M System shall enable a group of fog nodes cooperating on a service to re-allocate tasks among the group nodes as needed to adapt to the dynamic capability distribution within the group.
5. The oneM2M System shall enable identification and management of hierarchical fog clusters.

12.28 Use Cases for Smart Lifts

12.28.1 Description

These use cases have been elaborated to facilitate the potential support in oneM2M for Smart Lifts collecting and developing type and range of data which might be exchanged between lifts and their relevant management applications. It also includes the information about the monitoring of the activities and the performance of such lifts, including the possible interactions with the rest of the IoT devices and applications.

The information provided include:

- the combination of the data exchanged and their classification,
- the possible users of the data currently collected, organized as actors and user roles categories.

12.28.2 Actors

There are several type of user roles that are organized within three main categories:

- The users of the lift (the passengers) that could have different needs.
- The people and companies that work on the lift market.
- The owner of the building or administrator of group of building where the lift(s) is(are) installed.

For the purposes of the present use cases, users and roles have been classified as follows:

Building owner:

The owner of the building or a group of building.

Maintenance companies:

The companies that are in charge of the maintenance of the lifts, with the target to manage every problem that could arise on the lift.

Maintenance technicians:

The technicians of the maintenance companies, i.e. the people that work often on site, to fix problems and perform maintenance-related activities in general.

Passengers without priority:

The standard passenger of the lift.

Passengers with priority:

All the other kind of passenger that could have priority to use the lift (disabled people, elderly people, etc.).

Supplier technicians (especially of control cabinet):

The control cabinet is the brain of the lift, all the information is managed by the control cabinet; these are the technicians of the company that manufactured the control cabinet.

Control room operator:

People located in a (usually remote) control room, whose task is to supervise and control the operations of lifts or group of lifts.

12.28.3 Potential requirements

No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.28.4 Management of Group of Lifts

12.28.4.1 Description This case is about the control room operator that is in charge of monitoring and manage the lifts installed in the railway stations; the railways company want the possibility of monitoring the status of each lift and the possibility of controlling the lifts from a remote control room.

To achieve this purpose the control cabinet of the lift has to expose the status of several systems, making available the related signals and giving the possibility to send the commands to an individual lift or a to group of lifts (e.g. to make a ride to a specific floor).

This case could be extended to all the cases where the building's owners want to manage and monitor lifts in a single building or in several buildings (like railway stations, hospitals, office buildings, etc. . .); the objective is to manage and control the situation from a single and centralized control room.

12.28.4.2 Source RDM-2020-0011R03-Smart_Lifts_Use_Cases

> Note: informative source refer to ETSI TR 103 546 Requirement & Feasibility study for Smart Lifts in IoT, Section 6.1 [i.22].

12.28.4.3 Actors

☐ Building owner.
☐ Maintenance companies.
☐ Maintenance technicians.
☐ Passengers without priority.
☐ Passengers with priority (disabled people, elderly people, etc.).
☐ Supplier technicians (especially of control cabinet)
☒ Control room operator.

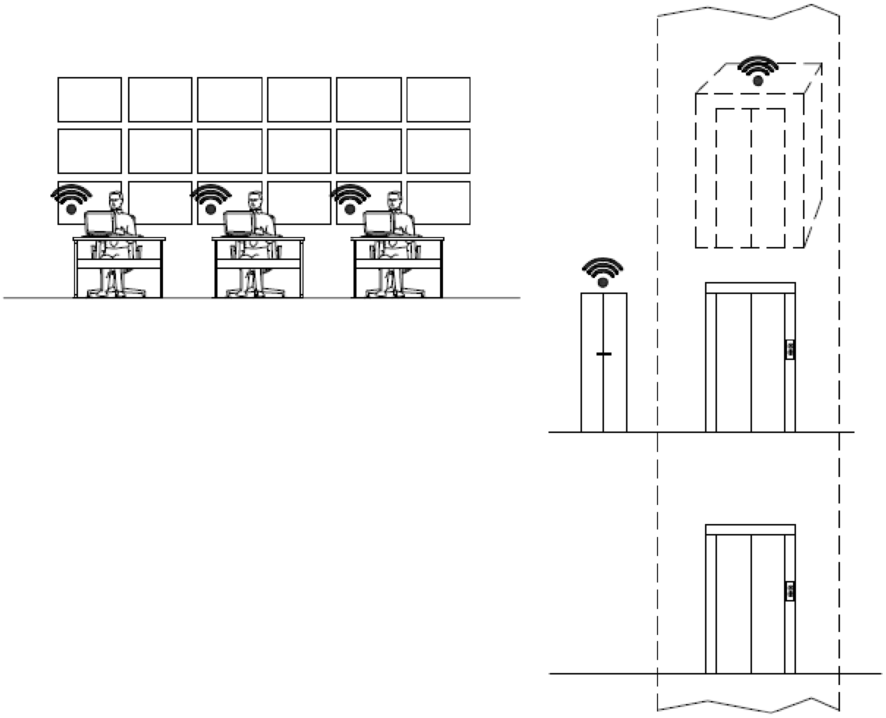


Figure 95: Figure 12.28.4.1-1 Management of Group of Lifts: Overview

> Note: the list above shows the actors identified in clause 12.28.2, those that are relevant for the current use case are marked with the symbol X.

12.28.4.4 Pre-conditions The regulations for the railway stations are mandating that every day - before the opening of the railway station - the personnel who is in charge of the station has to perform a test ride; in this case this test ride can be performed from the control room by the operator.

To achieve this purpose the control cabinet of the lift has to expose the status of several systems making available the related signals and to give the possibility to send the commands to the lift or to a group of lifts (to make a ride to a specific floor, for example).

12.28.4.5 Triggers The operator - by means of the control panel where he can see the status of the lifts - can evaluate if the test ride can be performed and - if all the parameters are OK - can conduct the test.

These test rides could be scheduled in function of the opening times of the railway stations, so the operator would not need to attend to all the tests in the control room.

12.28.4.6 Normal Flow In the control room the operator would receive these categories of signals:

- Monitoring signals: all the monitoring signals except the statistic signals.
- Alarms signals: all the alarm signals.
- Command signal: call to a specific floor, send car to a specific floor, out of service, test ride.

12.28.4.7 Alternative flow Another situation that the operator can manage from the control room, could be when a fault occurs and/or an alarm is activated.

In that case, by means of the CCTV display available in the control room the operator can have a view of what is happening in the lift and, based on that, take the needed actions, e.g.:

- alert the people in the railway station.
- notify the company that is in charge of the maintenance of the lift.
- alert the police or the firefighter.

12.28.4.8 Post-conditions If the result of the test is positive, the lift can be left in service.

Result of test ride is notified to the railway station manager (e.g. by sending an email or via other suitable means).

12.28.4.9 High Level Illustration None

12.28.4.10 Potential requirements No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.28.5 Predictive maintenance and Fault Resolution

12.28.5.1 Description This case is about how the maintenance companies and technicians can use the available information to set a predictive maintenance program for the lift, and how they can use the remote connection with the lift to fix the faults or the problems.

Predictive maintenance is the "new" trend in lift industry even if it has been applied in several industrial sector for ages; the scope of predictive maintenance is to anticipate the event of a fault, evaluating the fault rate of the single components based on the number of runs of the lift. So, the maintenance companies can substitute the components before the fault arise and they can reduce the out of service for the lift.

Furthermore, there are some faults very hard to discover and that require long time to be fixed, so the capability for the maintenance technician to have the direct and real-time support by the control cabinet's technician could drastically reduce the out of service necessary to fix the fault.

A typical problem is that a fault has been detected but when the maintenance technician is on site the lift runs properly; this is a typical case when the users smash the manual landing doors with the consequence is that the locking devices work sometimes well and sometimes badly.

In this case for the maintenance technician it is very hard to discover the fault; the best solution is that the technician of the control cabinet supplier connects to the lift from the remote position and analyses the faults; by the history of the faults recorded and the capability of analysing the single input and output of the main board, he can very quickly identify which landing door causes the fault and - usually – understand why the fault appears.

12.28.5.2 Source RDM-2020-0011R03-Smart_Lifts_Use_Cases

> Note: informative sources refer to ETSI TR 103 546 Requirement & Feasibility study for Smart Lifts in IoT, Section 6.1[i.22].

1228.5.3 Actors

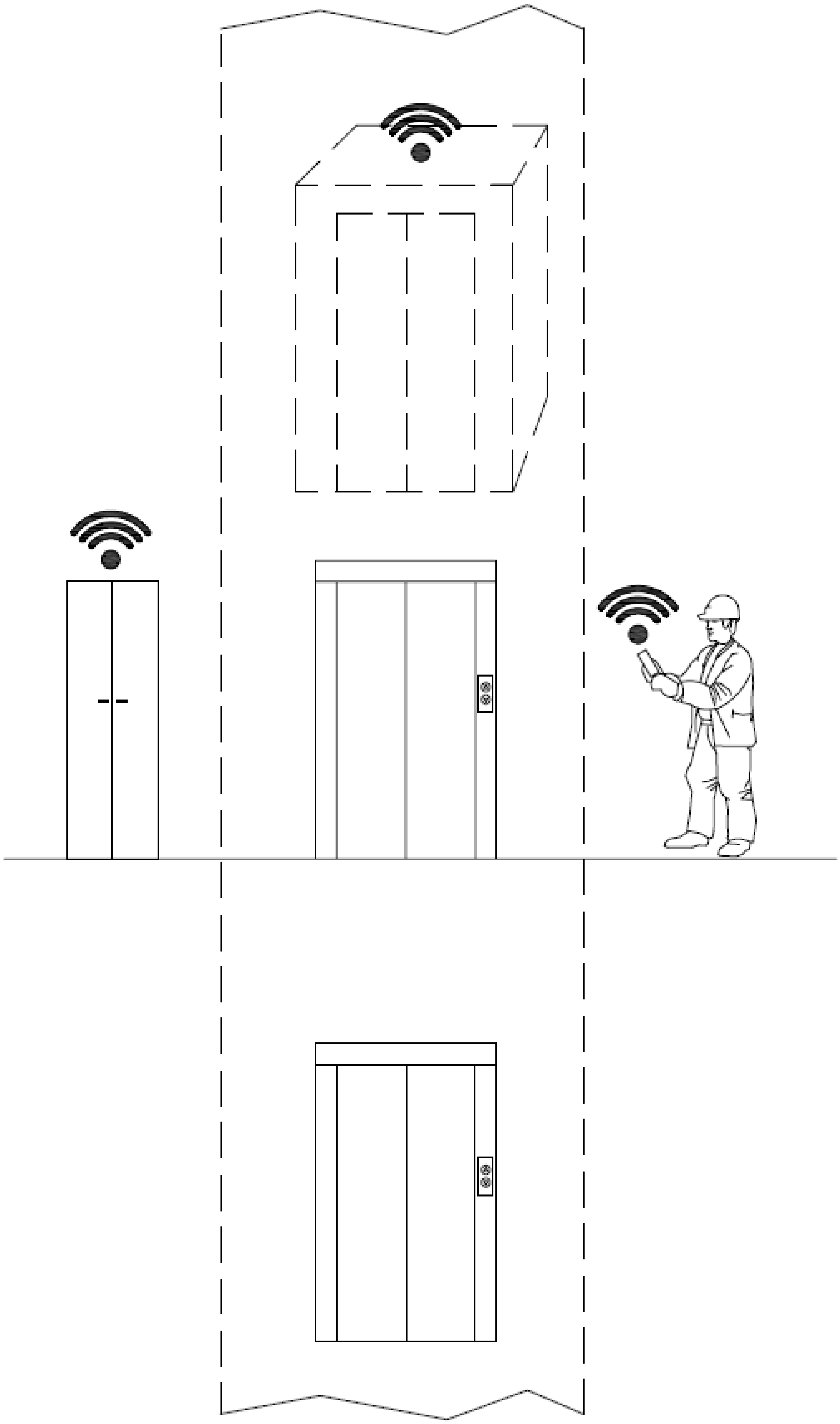


Figure 96: Figure 12.28.5.1-1 Preventive Maintenance and Fault Resolution: Overview

☐ Building owner.
☒ Maintenance companies.
☒ Maintenance technicians.
☐ Passengers without priority.
☐ Passengers whit priority (disabled people, elderly people, etc.).
☒ Supplier technicians (especially of control cabinet).

- [ ]Control room operator

  Note: the list above shows the actors identified in clause 6.3.3, those that are relevant for the current use case are marked with the symbol X.

12.28.5.4 Pre-conditions The lift is connected to a central platform, and the relevant information is transmitted.

On the platform, a set of automatic rules monitor the data received and determine if a failure is likely to happen soon, or if some part is likely to show sub-optimal performance due to predictable causes, such as wear.

Based on the kind of data and domain knowledge available, the rules complexity can range from simple ones, based on counting operating cycles or service time, to extremely sophisticated AI applications.

12.28.5.5 Triggers With predictive maintenance the system sends a message to the maintenance company that the lifetime of a component (e.g. wheel of the doors, pushbutton, etc.) has expired.

12.28.5.6 Normal Flow For the predictive maintenance:

- Monitoring signals: statistic signals.

For the fault's resolution:

- Monitoring signals: all the monitoring signals except the statistic signals.
- Command signal: call to a specific floor, send car to a specific floor, out of service, board reset.

12.28.5.7 Alternative flow None

12.28.5.8 Post-conditions Having received the notification of impending fault (e.g. by an e-mail report or by a message sent automatically by the lift), the maintenance company can send a technician to substitute the component with a new one. This can happen even in absence of a user call from the lift, thus reducing the time to repair and possibly avoiding the risk of service interruption altogether.

12.28.5.9 High Level Illustration None

12.28.5.10 Potential requirements No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.28.6 Servicing Priority People

12.28.6.1 Description There are some cases in which the system should manage passengers with priority (like disabled people) to give them the access to the lift - or better a group of lifts - in the faster and appropriate way.

In other cases, blind people could have a smart system when they can have access to a building more or less like all the other people, except the tactile path on the floor and/or tactile plan to understand where are the stairs, the lifts, the toilettes, etc.

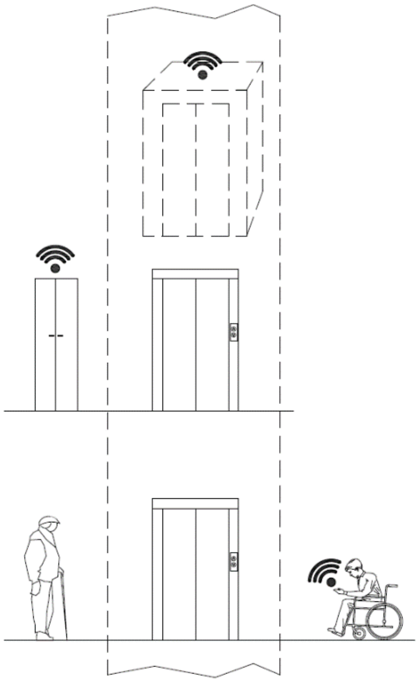


Figure 97: Figure 12.28.6.1-1 Servicing Priority People: Overview

12.28.6.2 Source RDM-2020-0011R03-Smart_Lifts_Use_Cases

> Note: informative sources refer to ETSI TR 103 546 Requirement & Feasibility study for Smart Lifts in IoT, Section 6.1[i.22].

12.28.6.3 Actors

☒ Building owner.
☐ Maintenance companies.
☐ Maintenance technicians.
☒ Passengers without priority.
☒ Passengers whit priority (disabled people, elderly people, etc.).
☐ Supplier technicians (especially of control cabinet).
☐ Control room operator.

> Note: the list above shows the actors identified in clause 6.3.3, those that are relevant for the current use case are marked with the symbol X.

12.28.6.4 Pre-conditions To achieve this the building has to manage and exchange the information through the devices and put the information available to the app. Both for the disabled people and blind people, the capability to do by them self every task is very important and with a simple application for mobile phone they can improve their quality of life.

12.28.6.5 Triggers In a building with a group of lifts (for example office building, hospital, railway station, etc.), due to the traffic during the peak time, the cars of the lifts are full; if a system can recognize the people with disability (especially people on a wheelchair), the system can give priority to them and "reserve" a specific lift.

Another case is about blind people: if the system can recognize them at the entrance of the building and if the building is a Smart building, by an app on the mobile phone or similar device, the blind people can use the information available on the app to find the appropriate path inside the building, reach the lift and go to the office (or the train, etc.).

12.28.6.6 Normal Flow All the signals,

- Monitoring signals: all the monitoring signals except the statistic signals.
- Alarms signals: all the alarm signals.
- Command signal: call to a specific floor, send car to a specific floor.

12.28.6.7 Alternative flow None

12.28.6.8 Post-conditions None

12.28.6.9 High Level Illustration None

12.28.6.10 Potential requirements No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.28.7 Management of maintenance and inspection visits of the lift or group of lifts

12.28.7.1 Description This case is about how to check the visits scheduled by the maintenance company, as well as those of verification of the notified body.

The owner or manager of the lift checks that the scheduled maintenance visits defined in the contract with the maintenance company are carried out with the agreed deadline and also checks that the notified body performs the pertinent checks.

In this case the control panel must recognize and record the access to the system in case of maintenance and / or verification and send a signal (e-mail report or a message).

The owner or manager of the lift records the event and can make the data available to the owners of the building.

12.28.7.2 Source RDM-2020-0011R03-Smart_Lifts_Use_Cases

> Note: informative sources refer to ETSI TR 103 546 Requirement & Feasibility study for Smart Lifts in IoT, Section 6.1[i.22].

12.28.7.3 Actors

☒ Building owner.
☒ Maintenance companies.
☒ Maintenance technicians.
☐ Passengers without priority.
☐ Passengers whit priority (disabled people, elderly people, etc).
☐ Supplier technicians (especially of control cabinet).
☐ Control room operator.

> Note: the list above shows the actors identified in clause 6.3.3, those that are relevant for the current use case are marked with the symbol X.

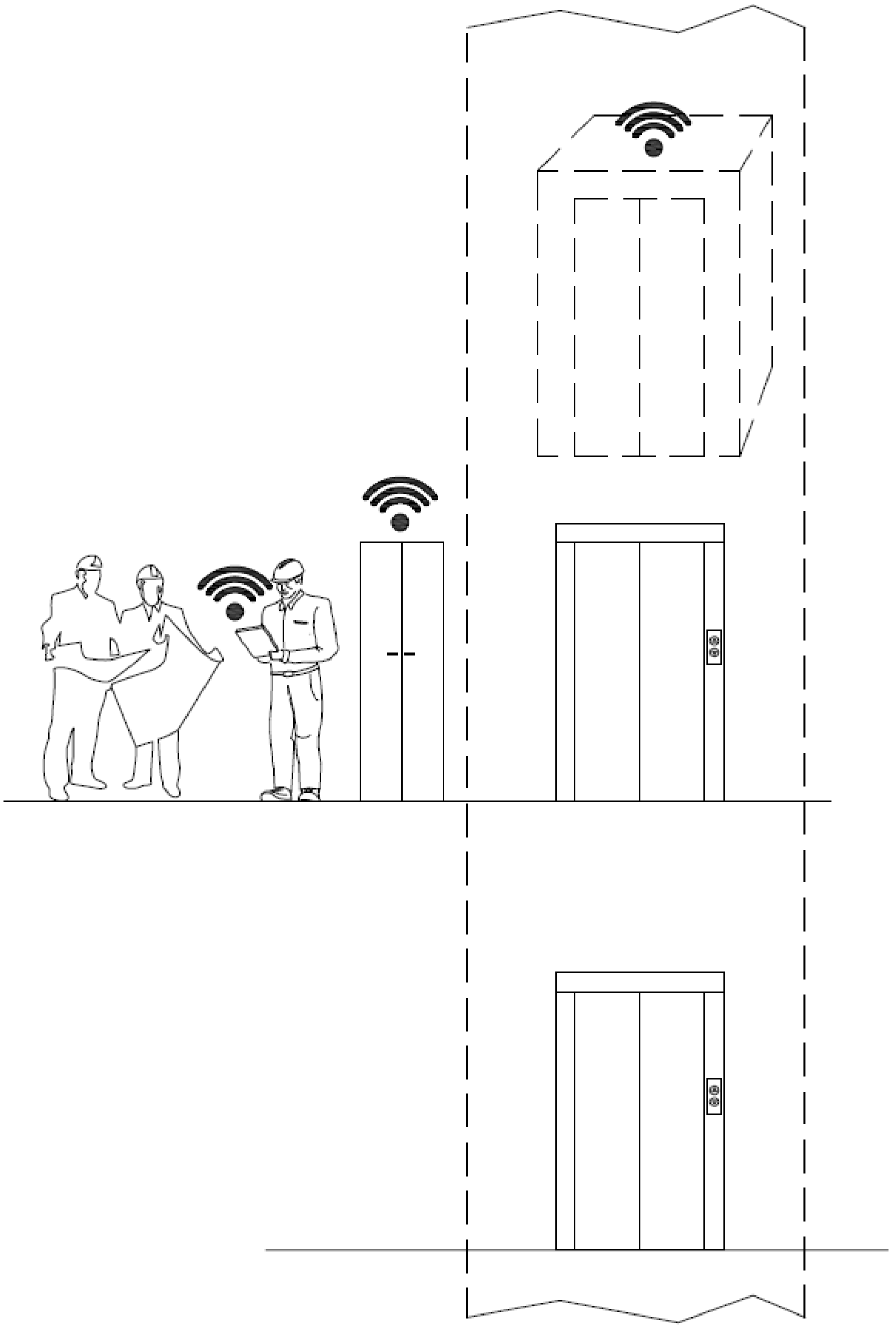


Figure 98: Figure 12.28.7.1-1 Management of maintenance and inspection visits of the lift or group of lifts: Overview

12.28.7.4 Pre-conditions Building managers (condominium administrators or real estate management companies) report property owners on the expenses incurred in general building management. In the specific case of the lift, a maintenance contract is stipulated with the company in charge that provides for a number of maintenance visits (defined according to the type of plant) to keep the plant in efficient service. Furthermore, periodically, a notified body must verify the lift safety devices.

12.28.7.5 Triggers The maintenance technician, who arrives on the plant, by means of the control panel, activates the maintenance operation mode and automatically sends a signal (e.g. e-mail or message) to the operator who can record the intervention and check whether it is congruous with the planned dates of the contract.

12.28.7.6 Normal Flow The plant manager receives:

- maintenance start signal.
- end of maintenance signal.
- inspection start signal.
- end of inspection signal.

12.28.7.7 Alternative flow None

12.28.7.8 Post-conditions Records are kept demonstrating that maintenance activities have been performed according to the planned schedule.

Supervision authorities are notified that maintenance complies with regulation mandates and best practices.

12.28.7.9 High Level Illustration None

12.28.7.10 Potential requirements No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.28.8 Call/Reserve Lift Car via Smartphone App

12.28.8.1 Description This case concerns the passenger's interaction with the elevator via an application downloaded to the smartphone. The application allows you to call the predetermined elevator lift car and take it to the desired floor using an application and/or voice control. There is also the possibility of receiving notifications about scheduled maintenance or down time.

In this case, the application itself is made to provide an acknowledgment of the elevator or elevators to be used (an application can register and recognize multiple installations) via a QR Code. At this point, the passenger near the elevator can proceed to the choice of the lift, its identification and the call of the lift car on the desired floor. The application will exchange the request with the lift controller framework that will verify the ability to handle the call by bringing the cabin to the desired floor.

12.28.8.2 Source RDM-2020-0011R03-Smart_Lifts_Use_Cases

> Note: informative sources refer to ETSI TR 103 546 Requirement & Feasibility study for Smart Lifts in IoT, Section 6.1[i.22].

12.28.8.3 Actors

☐ Building owner.
☐ Maintenance companies.
☐ Maintenance technicians.
☒ Passengers without priority.
☒ Passengers whit priority (disabled people, elderly people, etc.)
☐ Supplier technicians (especially of control cabinet).
☐ Control room operator.

> Note: the list above shows the actors identified in clause 6.3.3, those that are relevant for the current use case are marked with the symbol X.

12.28.8.4 Pre-conditions The plant manufacturer or maintainer makes a QR code of the elevator visible (in and/or near the elevator).

A suitable app is installed on the passenger's smartphone.

The user of the system, with the smartphone or similar device, recognize through the QR code the application downloaded to the device. Once the application installed, the passenger will be able to identify the system and send the call request to the floor both near the elevator and at a distance. The control panel recognizes the request, verifies the status of the system and accepts the call, sending the lift car to the desired floor.

12.28.8.5 Triggers The passenger is able to identify the system (via the QR codes) and sends the call request to the floor both near the elevator and at a distance.

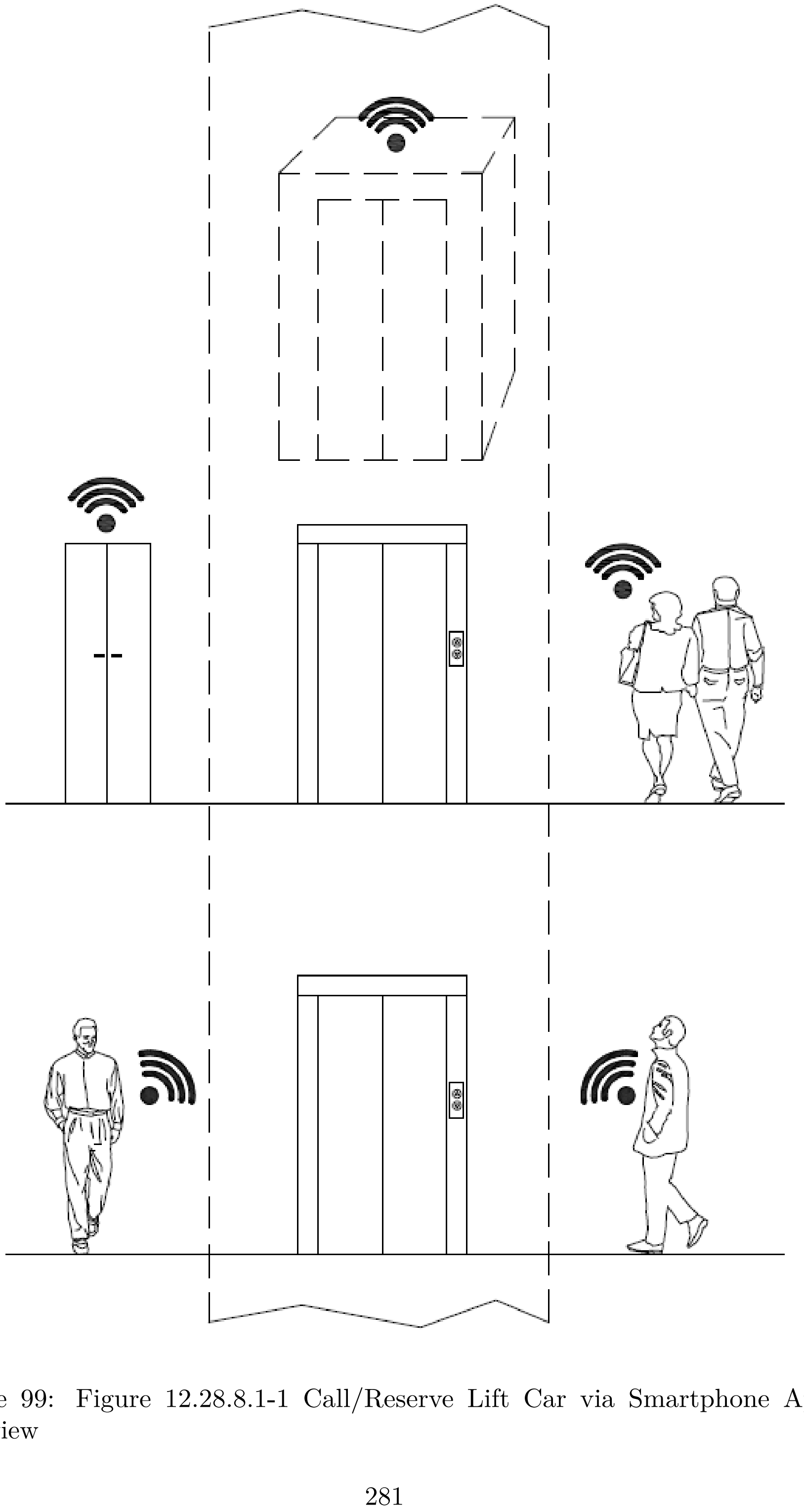


Figure 99: Figure 12.28.8.1-1 Call/Reserve Lift Car via Smartphone App: Overview

12.28.8.6 Normal Flow The control panel recognizes the request, verifies the status of the system and accepts the call, sending the lift car to the desired floor.

Passenger receives from lift car:

- lift car position (floor number).
- lift car status (if doors open/closed).
- lift car direction (ascending/descending).
- lift car status (moving/out of service).

12.28.8.7 Alternative flow None

12.28.8.8 Post-conditions None

12.28.8.9 High Level Illustration None

12.28.8.10 Potential requirements No specific new features are currently identified as result of the analysis of Smart Lift use cases. The oneM2M system Rel 3 seems to support properly these use cases. It remains necessary to include the data structure to be exchanged by Smart Lifts in the oneM2M semantic work. As it is also deemed to be included in the ETSI SAREF package to assure proper semantic interoperability with other systems it is also necessary to verify the SAREF alignment.

1. oneM2M shall support Smart Lift data model and its possible evolution, e.g. as identified in [i.21].

12.29 Advanced Semantic Discovery - a network of nodes across IoT Domains

12.29.1 Description

The oneM2M system has implemented basic native discovery capabilities. The use cases specified in clauses 12.29, 12.30, 12.31 and 12.32 lead to potential requirements, which extend the existing requirements of the use case clause 12.9.10 of the present document with a focus on the discovery and query capabilities, introducing a direct relation with the semantic aspects and enabling more sophisticated semantic queries as e.g. a capability in the CSE, that takes routing decisions for forwarding a received Advanced Semantic Discovery Query.

This use case could be considered as either the "use-case zero", or a "parametric use-case" for Advanced Semantic Discovery (ASD) and it can be instantiated in many domain specific cases.

This use case illustrates the needs for an Advanced Semantic Discovery (ASD) within distributed network of CSEs belonging a single Service Provider and across different IoT Service Providers. This distributed scenario is partially faced in the present document in clause 12.9 (Semantics query for device discovery across M2M Service Providers).

It shows the importance of formalizing:

- *an Advanced Semantic Discovery Query Language* (ASDQL) able to write Advanced Semantic Discovery Query (ASDQ);
- *a Semantic Discovery Routing Protocol* (SDRP) to route an *Advanced Semantic Discovery Query* (ASDQ) between different CSEs;
- *a Semantic Discovery Agreement* (SDA), to state some communication agreements between CSEs;
- *a Semantic Query Resolution functionality* (SQR) allowing to locally resolve an Advanced Semantic Discovery Query (ASDQ) into some elementary standard oneM2M Semantic Discovery Queries (SDQ).

The concepts included in the present use case is intensively used in the following clauses of the present document, namely:

- 12.30 Advanced_Semantic_Discovery - Semantic_Recommendation in a network of nodes across IoT Domains
- 12.31 Advanced_Semantic_Discovery -Facility_Management_of_a_Supermarket_Chain, and
- 12.32 Advanced_Semantic_Discovery -Healthcare_Network_and_Clinical_Knowledge_Administration.

12.29.2 Source

RDM-2020-0035R03-Semantic_discovery_with_multiple_M2M_SP

> Note: informative source refer to ETSI TR 103 714 SmartM2M; Study for oneM2M Discovery and Query use cases and requirement [i.23].

12.29.3 Actors

- 5 *Application Entities* (AE) X of type T1, Y of type T2, Z of type T3, V of type T4, and W of type T5.
- 2 *Middle Node Common Service Entities* (MN-CSE) P, and Q.
- A MN-CSE has a local database containing information on their registered AE. The local database includes location information (where each device is presently located), the device type, etc. Let P and Q have some Semantic Discovery Agreement (SDA) with A. Semantic Discovery Agreement (SDA) can be relaxed inside a single Service Provider, see Note 2 of Definition 2.
- 4 *Infrastructure Node Common Service Entities* (IN-CSE) A, B, C, and D.
- An IN-CSE has a local database containing information on their registered MN-CSEs and AEs. The local database includes location information (where each device is currently located), the device type, etc. Let A, B, C, and D have some Semantic Discovery Agreement (SDA) among each other's.

12.29.4 Pre-conditions

Consider the following topology:

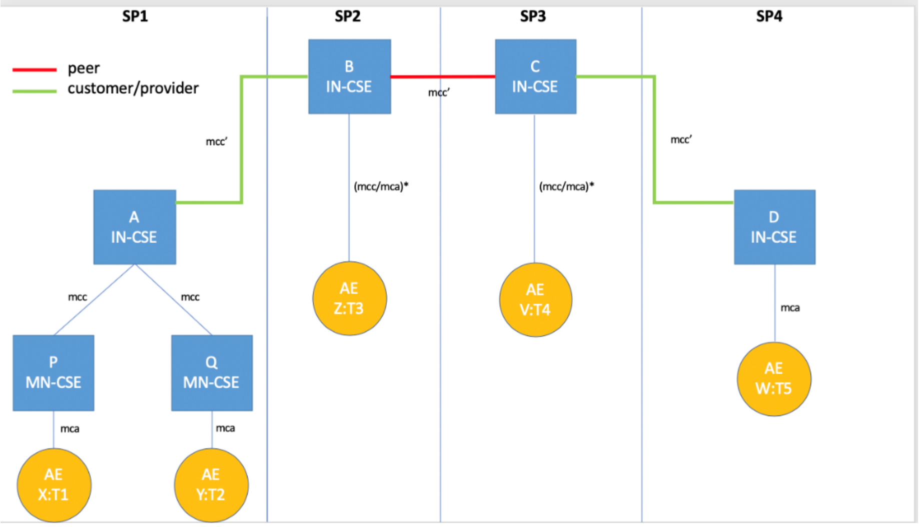


Figure 100: Figure 12.29.4-1 - Pre-condition topology

12.29.5 Triggers

This section presents, informally, three examples of the Advanced Semantic Discovery Query Language (ASDQL). Let AND, OR, NOT be *non-terminals* and FC be some *filter-criteria*, and ?T be a *meta-variable* of type T to be resolved.

Example 1. X:T1 send to MN-CSE P

ASDQ1 = ?T2|FC2 AND ?T3|FC3 AND ?T4|FC4 AND ?T5|FC5

The query can be intuitively read as follows: X is looking for

- some AE of type T2 registered in any CSE satisfying the filter criteria FC2, AND
- some AE of type T3 registered in any CSE satisfying the filter criteria FC3, AND
- some AE of type T4 registered in any CSE satisfying the filter criteria FC4, AND
- some AE of type T5 registered in any CSE satisfying the filter criteria FC5.

Example 2. X:T1 send to MN-CSE P

ASDQ = ?T2|FC2 OR ?T3|FC3 OR ?T4|FC4 OR ?T5|FC5

The query can be intuitively read as follows: X is looking for

- some AE of type T2 registered in any CSE satisfying the filter criteria FC2, OR
- some AE of type T3 registered in any CSE satisfying the filter criteria FC3, OR
- some AE of type T4 registered in any CSE satisfying the filter criteria FC4, OR
- some AE of type T5 registered in any CSE satisfying the filter criteria FC5.

Example 3 . X:T1 send to MN-CSE P

ASDQ = (?T2|FC2 OR ?T3|FC3) AND (?T4|FC4 OR ?T5|FC5)

Example 4 . X:T1 send to MN-CSE P

ASDQ = (?T2|FC2 AND ?T3|FC3) OR (?T4|FC4 AND ?T5|FC5)

Example 5 . X:T1 send to MN-CSE P

ASDQ = (?T2|FC2 AND ?T3|FC3) OR (?T4|FC4 AND (NOT ?T5|FC5))

It is also possible to consider other non-terminals, such as (list not exhaustive):

- ANY = search in all CSE databases;
- CURRENT = search in the CSE local database;
- CUSTOMER[N] = search in the databases of N CUSTOMER CSE;
- PROVIDER[N] = search in the databases of N PROVIDER CSE;
- PEER[N] = search start on the databases of N PEER CSE;
- BETWEEN_TIME[SEC] = search should return in SEC;
- BETWEEN_SPACE[METER] = search should give results in METER;
- OF_BRAND[NAME] = search should give results of brand NAME.

12.29.6 Normal Flow

We present a "trace" of the Semantic Discovery Routing (SDR) generated by Example 1, the other examples can be easily traced following the same logic. This trace is inspired to a semantic discovery routing as described in [i.24] and [i.26] and proceeds as follows:

- X sends an Advanced Semantic Discovery Query (ASDQ1) to P;
- P verifies the integrity of ASDQ1 and forward the Advanced Semantic Discovery Query ASDQ1 to A that starts the Semantic Discovery Routing Protocol (SDPR) into the network of CSE;
- ASDQ1 is resolved using the Semantic Query Resolution System (SQRS) locally in A into four subqueries, namely ASDQ2, ASDQ3, ASDQ4, and ASDQ5, where:
  - ASDQ2 = ?T2|FC2
  - ASDQ3 = ?T3|FC3
  - ASDQ4 = ?T4|FC4

- ASDQ5 = ?T5|FC5

1. A starts lookup in its local database, trying to solve {ASDQ2,3,4,5} but fail
2. A down-forwards ASDQ1 to Q via an mcc pointer
3. Q solve the subquery ASDQ2 ?T2|FC2 in its local database returning Y to A
4. A send back Y to P and X
5. A up-forwards ASDQ3 and ASDQ4 and ASDQ5 to B
6. B solve the ASDQ3 ?T3|FC3 in its local database returning Z to A (and back to P and X)
7. B side-forwards ASDQ4 & ASDQ5 to C
8. C solve the ASDQ4 ?T4|FC2 in its local database returning V to B (and back to A, P and X)
9. C down-forwards ASDQ5 to D
10. D solve the ASDQ5 ?T5|FC5 in its local database returning W to C (and back to B, A, P and X)

Note 3. When A up-forwards to B, it follows that A respect the CUSTOMER-PROVIDER SDA with B (e.g. A respect the Semantic Discovery Agreement (SDA) directives of B). When B side-forwards to C, it follows that B and C respect the PEER-PEER Semantic Discovery Agreement (SDA) directives. When C down-forwards to D, it follows that D respect the PROVIDER-CUSTOMER Semantic Discovery Agreement (SDA) with C (e.g. D respect the Semantic Discovery Agreement (SDA) directives of C).

The moral is : B and C should be “acknowledged” for their”routing job”.

12.29.7 Alternative flow

In the following alternative topology, the CUSTOMER-PROVIDER Semantic Discovery Agreement (SDA) are reversed:

A possible “trace” of the Semantic Discovery Routing Protocol (SDRP), again inspired to [i.24] and [i.25] proceeds as in clause 12.20.6, excepting for the following caveat.

Caveat. When A down-forwards to B, it expects that B should respect the provider-customer Semantic Discovery Agreement (SDA) with A (e.g. B *should acknowledge* A. **This is not intuitive** since *B does a favour to A and acknowledge A*). When B side-forwards to C, it expects that B and C have a common Semantic Discovery Agreement (SDA) and, as such, they not acknowledge it each other. When C up-forwards to D, it expects that C and D have a common Semantic Discovery Agreement (SDA) (e.g. C *should acknowledge* D). **This is not intuitive** since *C does a favour to D and acknowledges D*).

The moral is : B and C do a job for their providers and, moreover, they have to *acknowledge* for their “routing job”.

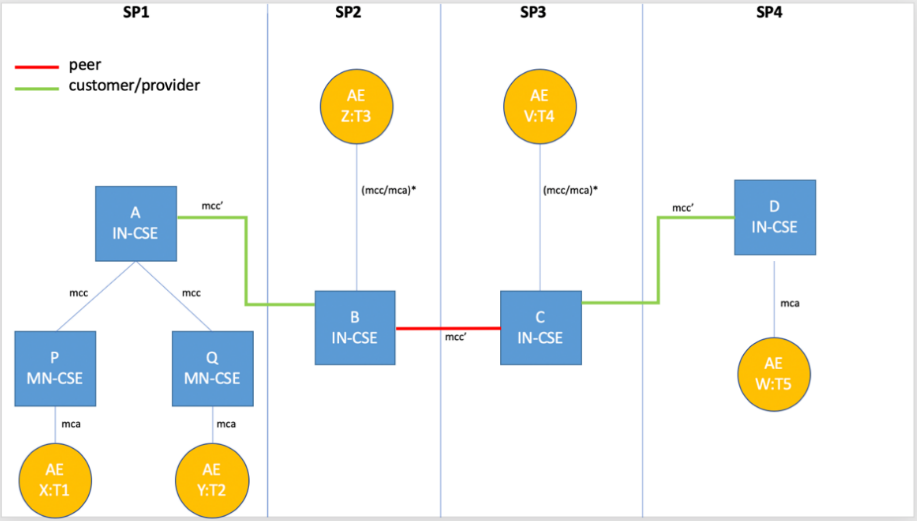


Figure 101: Figure 12.29.7-1 - Pre-condition topology for alternative flow

Alternative traces happen in practice. Because of the distributed nature of the Semantic Discovery Routing Protocol (SDRP), it is beneficial to try incentivizing routing respecting the Semantic Discovery Agreement (SDA), and, as such, avoid routing not respecting the Semantic Discovery Agreement (SDA). Those situations are not new in Internet and are referred as VALLEY ROUTING by [i.24]. "Good routing" should guarantee that routing is always "valley preserving" (or "no valley"). Valley routing property is also preserved in the Network Aware Resource Discovery Protocol [i.25].

12.29.8 Post-conditions

X can start to interact with Y, Z, V, and W.

12.29.9 High Level Illustrations

12.29.10 Potential requirements

The oneM2M system shall provide mechanisms for Advanced Semantic Discovery (ASD) across a distributed network of IoT nodes within a single oneM2M Service Provider and across different IoT Service Providers.

A CSE receiving an Advanced Semantic Discovery Query (ASDQ) shall extract the Semantic Discovery Query (SDQ), embedded in the packet payload, and shall resolve the query with respect to the locally available information and shall forward to other suitable CSEs the Advanced Semantic Discovery Query (ASDQ) to complete the discovery.

More specifically, the oneM2M system shall provide:

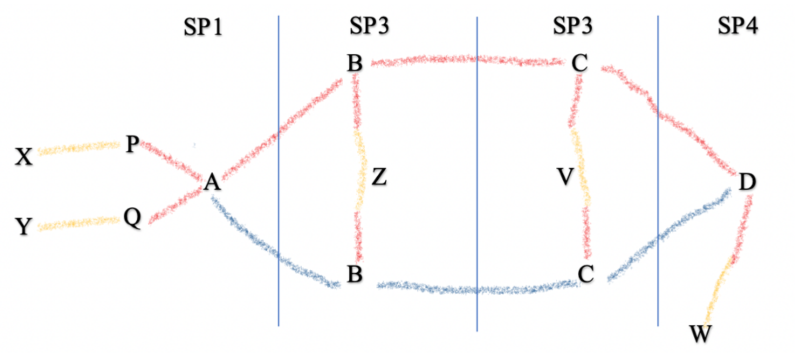


Figure 102: Figure 12.29.9-1 - Illustration for multiple service providers semantic discovery use case

2. An Advanced Semantic Discovery Query Language (ASDQL) that the ability to write Advanced Semantic Discovery Query (ASDQ);

A Semantic Discovery Agreement (SDA) to state some communication agreements between CSE;

A Semantic Query Resolution (SQR) that allows to locally translate an Advanced Semantic Discovery Query (ASDQ) into some elementary oneM2M Semantic Discovery Queries (SDQ);

A Semantic Discovery Routing (SDR) to route an Advanced Semantic Discovery Query (ASDQ) between different CSEs.

12.30 Advanced Semantic Discovery - Semantic Recommendation in a network of nodes across IoT Domains

12.30.1 Description

This use case is built upon a cross-domain scenario in which a Hospital has a large number of IoT devices, which are in charge of performing different tasks. The IoT devices can be classified into the following categories: energy devices (load consumption, flexibility monitoring, energy switch, etc), building devices (lights, door sensors, occupancy sensors, etc) , personal devices (smart bands, smartphones, etc), and devices related to health (hearth rate sensor, glucose monitor, etc). These IoT devices are connected across in the hospital network but they do not necessarily belong to the same oneM2M Service Providers.

In this scenario, several actors need to discover and use IoT devices that are allocated outside their oneM2M Service Providers. For instance, if the energy devices detect an incoming negative peak of energy, entailing that a large number of devices should be switched off to avoid the whole hospital to run out of energy (losing critical systems for the patients). Then, the energy devices (or an application in charge) should be able to discover all the sensors in the building that are related to energy (like light bulbs or air condition) and switch them off. Also, the same actor (the energy devices or an application in charge) should detect the critical eHealth IoT devices for the patients and ensure that they are switched on. In the case that one of the eHealth IoT devices would run off, then the energy devices, or an application in charge, should perform a discovery task over the personal devices in order to find relevant people, i.e. doctors, nearby the critical eHealth IoT devices that are running out of energy in order to assist the patients.

This use case assumes that there is an interoperability platform (oneM2M) that allows monitoring and controlling the different IoT devices regardless their vendor. Also, the platform should ensure a secure and private environment so no unauthorized third party could access the network. This platform should ensure a sufficiently rich discovery in order to meet the previous example Please note that the definitions and acronyms provided in clause 12.20.1 of the current document apply to this use case:

- It is fully distributed in order for the *Advanced Semantic Discovery* (ASD) to reach from one oneM2M Service Provider to others that may contain relevant infrastructures.
- The *Advanced Semantic Discovery Query* (ASDQ) is expressed using an *Advanced Semantic Discovery Query Language* (ASDQL) so specific semantic terms from domains like energy or eHealth can be used.
- *The Advanced Semantic Discovery* (ASD) needs to happen in quasi real-time and therefore the communication mechanism across infrastructures that belong to different Service Provider should not be blind; instead it should be guided by a *Semantic Recommendation* (SR).

This use case can be generalized to other domains in which IoT devices are spitted in different IoT Service Providers and discovery needs be performed across them avoiding flooding the infrastructures, i.e. relying on a guided Semantic Recommendation System (SRS) to which infrastructures perform the Advanced Semantic Discovery (ASD), and to which discard, leveraging the network load.

12.30.2 Source

RDM-2020-0032R03-Semantic_Recommendation_in_CSEs_for_Discovery

> Note: informative source refer to ETSI TR 103 714 SmartM2M; Study for oneM2M Discovery and Query use cases and requirement [i.23].

12.30.3 Actors

M2M Applications, M2M Service Providers

IN-CSE and MN-CSE

IoT devices from the different domains

Medical staff, building staff, or technicians

12.30.4 Pre-conditions

A network infrastructure distributed across different IoT Service Providers. Intuitively, network infrastructure of the oneM2M Service Providers is a set of M2M devices and Application Entities (AE) that have been installed and registered to their corresponding MN-CSE (Middle Node - Common Services Entity). The MN-CSEs have in turn been registered to the corresponding IN-CSE (Infrastructure Node - Common Service Entity).

All the different CSEs have *Semantic Discovery Agreements* (SDA) with each other, resulting in a tree-like network topology. In such a topology, the CSEs should rely as a Semantic Recommendation (SR) in order to assist the advanced semantic discovery resolution task performed by the CSEs involved in. As smarter is the Semantic Recommendation (SR), as efficient will be the discovery in terms of time, CSEs visited, and number of queries forwarded, among others. The discovery should allow expressing some network directives to address efficient routing across CSEs.

Both the registering and the discovery should be expressed according to the oneM2M described in TS-0012. Nevertheless, due to tailored-domain terms required in our use case, the registering and the discovery should be also expressed with specific domain ontologies like the different extensions of SAREF.

> Note. Semantic Discovery Agreement (SDA) is defined in clause 12.29.1 of the current document.

12.30.5 Triggers

The IoT energy devices, or a technician, send first an Advanced Semantic Discovery Query (ASDQ) to find all the non-critical IoT devices allocated in the building. Then, a second Advanced Semantic Discovery Query (ASDQ) is issued to find all the critical IoT devices from the eHealth domain, and if required, a third Advanced Semantic Discovery Query (ASDQ) is issued to find relevant medical staff that could be near critical devices. The different Advanced Semantic Discovery Query (ASDQ) will rely on specific semantics, the first will contain information about devices and if they consume energy, the second about eHealth devices that are critical and cannot be switched off, and the third about the people, their roles in hospital, and their location.

12.30.6 Normal Flow

1. An IoT energy device, or a technician, sends an ordinary oneM2M Semantic Discovery Query (SDQ) to its CSE, written in SPARQL. The SPARQL query will contain terms about sensors that consume energy, that are not from the eHealth domain, and that are located in the building.

2. The CSE verifies the integrity of the Semantic Discovery Query (SDQ), and it tries to answer. If the CSE is not able to reply, it builds an Advanced Semantic Discovery Query (ASDQ) wrapping the Semantic Discovery Query (SDQ).
3. Then the CSE forwards the Advanced Semantic Discovery Query (ASDQ) to other CSEs that may be located in the same oneM2M Service Provider, or in a different oneM2M Service Providers, or even sent to a non oneM2M IoT Service Provider.
4. Relying on the *Semantic Recommendation* (SR), the CSE selects and queries the relevant CSEs.
5. The CSE of the Building will receive the Advanced Semantic Discovery Query (ASDQ) and will try to solve the embedded Semantic Discovery Query (SDQ). The building contains suitable IoT devices so that the CSE will be able to produce and forward back a positive answer.
6. Finally, the IoT energy device, or a technician, will receive the answer and the semantic discovery terminates successfully.

12.30.7 Alternative Flow

None

12.30.8 Post-Conditions

The query is answered if a resource that fulfils the discovery criteria is present in the network and "reasonably" reachable. For example, the discovery task needs be completed in an given threshold time even when crossing different IoT Service Providers is required.

12.30.9 High Level illustration

12.30.10 Potential requirements

The following potential requirements are additional to the ones already identified in clause 12.29.10:

1. The oneM2M system shall integrate already standardized ontology extensions to the current oneM2M ontology to cope with new specific domains (ex: SAREF core and its extensions SAREF4BLDG, SAREF4ENVI, SAREF4ENERGY, SAREF4CITY, SAREF4AGRI, SAREF4WATER).
2. Based on semantic information, the oneM2M system shall take routing decisions for forwarding a received Advanced Semantic Discovery Query (ASDQ). The semantic information will allow the oneM2M system to maximize and to accelerate the semantic discovery process.

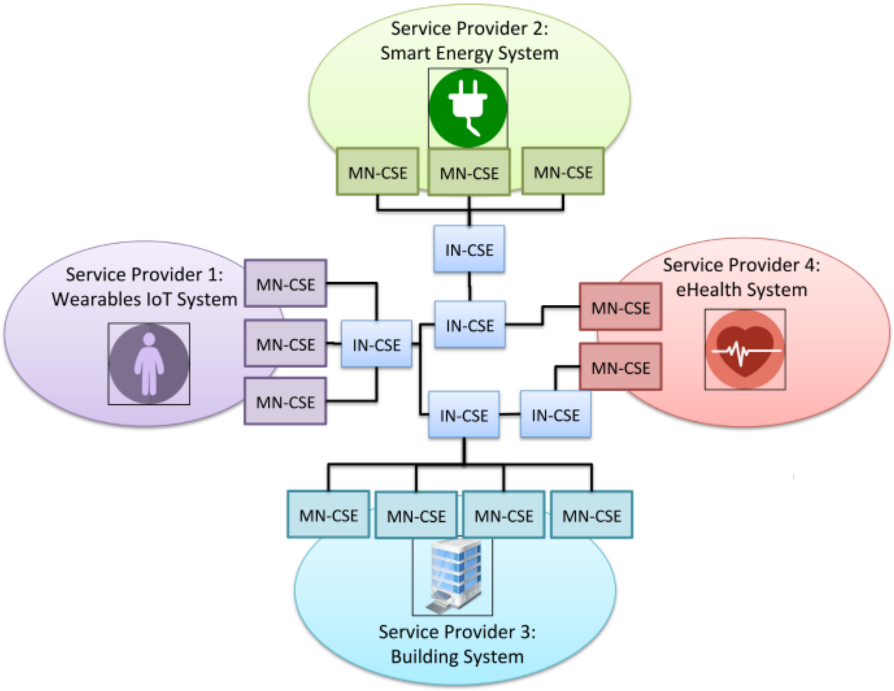


Figure 103: Figure 12.30.9-1 - Illustration for Semantic Recomandation use case

12.31 Advanced Semantic Discovery - Facility management of a supermarket chain

12.31.1 Description

Building and facility managers need a helicopter view of the facilities management processes, regardless of existing building installations in order to make better-informed decisions and to enforce cross building policies. Building managers are faced with heterogeneous and vendor-specific installations. Centralized management of buildings oftentimes forces the owners to go through costly replacements to adopt mono-vendor solutions. Installation of new equipment requires costly system integration because devices are often designed to communicate with specific applications only.

This use case assumes a facility manager working for a supermarket chain and responsible of dozens of buildings. It is supposed that there is an interoperability platform (oneM2M) that offers a standard interface to monitor and control all the buildings regardless of vendor. The facility manager could apply energy efficiency strategies to all buildings on large scale. He could for example, compare buildings to detect leaks, adjust the heat and the lighting according to forecast or predictive models, and compliant with applicable regulations.

The exposure of the huge amounts of data through modern APIs allows proliferation of new building services such as situational awareness, energy efficiency, intrusion detection, preventive maintenance and smart data.

Through further APIs, wider integration of the buildings with the outside world is achieved to give rise to fully integrated cities. The buildings start to interwork with energy grids (smart and micro grids), smart parking, Electrical Vehicle charging, waste management, etc., the ultimate goal for buildings to be considered really smart.

Assuring interoperability between all the data producing, data storing, and data processing components, semantic discovery and query mechanisms across and between sensors, devices, APIs and even IoT platforms are essential.

This use case is similar to the use case “Semantics query for device discovery across M2M Service Providers” in clause 12.9 of the present documents. However, it extends the requirements with a focus on the discovery and query capabilities, introducing a direct relation with the semantic aspects and enabling more sophisticated semantic queries.

12.31.2 Source

RDM-2020-0031R04-Facility management of a supermarket chain

> Note: informative sources refer to the following documents:
>
> ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach

[i.31].

ETSI TR 103 714 SmartM2M; Study for oneM2M Discovery and Query use cases and requirements [i.23].

12.31.3 Actors

- M2M devices as e.g. energy meters, temperature sensors, fire detectors, leak detectors, lightning controls, heat and air condition controls, surveillance cameras , cash boxes, inventory controls
- Facility manager
- M2M Service providers
- M2M Applications e.g. data analytics, fault detection, energy efficiency, hypervision

12.31.4 Pre-conditions

M2M devices in the super markets have been installed and registered to their corresponding MN-CSE (Middle Node - Common Services Entity). The MN-CSEs have been registered to the corresponding IN-CSE (Infrastructure Node - Common Services Entity).

The M2M Application Provider 1 has contractual relationships with the M2M Service Providers 2, 3 and 4.
The M2M Service Providers 1 and 2 have databases that contain information on the devices located in the supermarkets of the supermarket chain.

The facility manager wants to make use of the devices within his supermarkets and of the API “Facility management” in order to apply energy efficiency strategies to all buildings on large scale and to compare buildings to detect leaks, adjust the heat and the lighting according to forecast or predictive models, and compliant with applicable regulations. Assessing the warehouses stocks enables to refill it in time and a centralized fault detection ensures to take countermeasures.

The M2M Service Provider 3 wants to access data from energy consuming/measuring devices and/or respective databases of the M2M Service Providers 1 and 2 in order to optimize his energy providing balance.

The M2M Service Provider 4 wants to access data from parking lot sensors, from charging stations for electrical vehicles, data about the product range and warehouse stocks of the M2M Service Providers 1 and 2 in order to provide relevant services to the city inhabitants.

12.31.5 Triggers

The facility manager, the API “Facility management”, the M2M Service Provider 3 or 4 (further on called “REQUESTER”) sends a semantic discovery service request to the M2M Service Provider 1 or 2 (further on called “REQUEST RE-

CEIVER"). The request contains information about the device to be discovered, e.g., a device type, a localization and other filters criteria.

12.31.6 Normal Flow

Following, one example of a typical scenario is described:

1. Via a device (e.g. user terminal), which is connected to the API "Facility management", the facility manager initiates a semantic discovery request within the domain of the M2M Service Provider 1 to the smart meters of a specific area of a special supermarket, which enquires information about its energy consumption.
2. The API "Facility management" verifies the integrity of the semantic discovery request and sends a semantic discovery request to the MN-CSE of the supermarket.
3. The database of the MN-CSE is searched for the specific requested type of devices whether they are connected to it or not.
4. If the requested type of devices is connected to the MN-CSE, it returns the requested information of the devices to the M2M Application.
5. If the requested devices are not connected to the MN-CSE, a negative acknowledge is sent back to the M2M Application.
6. The API "Facility management" processes, if necessary, the received information and forwards it to the requesting device of the facility manager.

12.31.7 Alternative Flow

Following, one example of an alternative scenario is described:

1. An M2M Application of the Service provider 4 (Smart Cities domain) launches a query to the domain of M2M Service Providers 1 and 2 to find and identify the sensors of their parking lots, which enquires information about free parking spaces.
2. The IN-CSE of the Service Provider 1 verifies the integrity of the semantic discovery request and distributes it to the MN-CSEs of the supermarkets.
3. The databases of the MN-CSEs are searched for the specific requested type of devices whether they are connected to it or not.
4. If the requested type of devices is connected to a MN-CSE, it returns the requested information of the devices to the IN-CSE, which forwards it to the requesting Service Provider 4.
5. +f the requested devices are not connected to the MN-CSE, a negative acknowledge is sent back to the IN-CSE, which forwards it to the requesting Service Provider 4.
6. The requesting M2M Application of Service Provider 4 processes the data and provides them in an appropriate way to the users of the M2M Application (e.g. city inhabitants).

12.31.8 Post-conditions

The facility manager, the API “Facility management”, the M2M Service Provider 3 or 4 can start to employ the devices based on the semantic discovery service request sent to the M2M Service Provider 1 or 2.

12.31.9 High Level Illustration

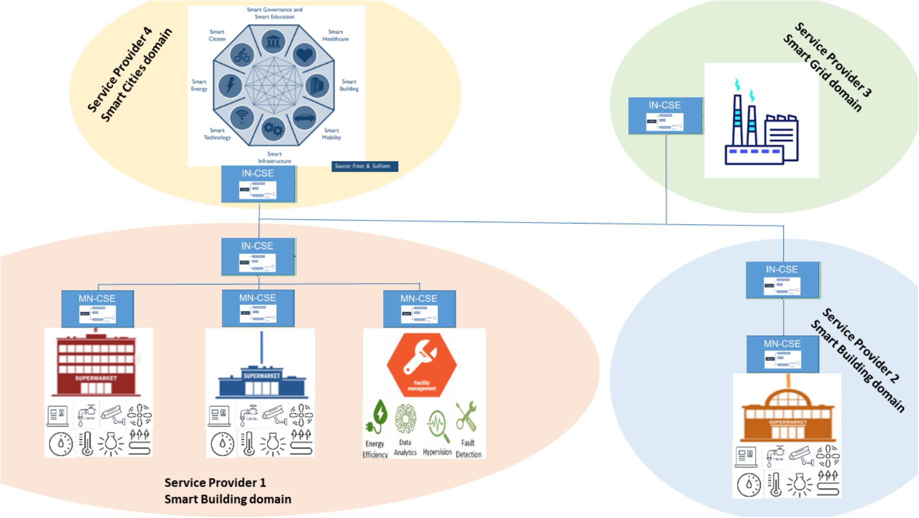


Figure 104: Figure 12.30.9-1 - Facility management of a supermarket chain

12.31.10 Potential requirements

The following potential requirements are additional to the ones already identified in clauses 12.29.10 and 12.30.10.

1. Advanced Semantic Discovery shall support queries written with specific domain ontologies, e.g. SAREF.
2. Advanced Semantic Discovery shall support semantic reasoning between the baseline oneM2M ontology and the identified domain specific ontologies, e.g. SAREF. As example, if a query is looking for a oneM2M device observing Celsius temperature, then the Advanced Semantic Discovery would potentially return a SAREF temperature sensor.
3. Advanced Semantic Discovery shall provide capabilities to identify multiple set of targets, and a multiplicity of searches (e.g. by setting parameters or filters).
4. The oneM2M Access Control Policy shall include discovery permissions to support Advanced Semantic Discovery. When an Advanced Semantic Discovery is performed by the oneM2M System, it shall operate according to the indications associated with the desired information.

It is also expected that:

- The solution would be based an evolution of the current oneM2M architecture and functionality and would reuse existing standard ontology mechanisms e.g. considering the SAREF standard developed in ETSI TC SmartM2M (which is also aligned with the W3C ontology approach). This intends to assure also a smooth interworking with relevant non-oneM2M solutions.
- The solution would be complete and will be a part of the oneM2M core functions, to avoid the need of ad hoc applications designed to expand the oneM2M functionality with the risk of being implemented with different flavours.

12.32 Advanced Semantic Discovery - Healthcare network and clinical knowledge administration

12.32.1 Description

This use case looks at the semantic discovery requirements through a networking environment between people with disease (patients), the elderly, who want to live an independent life while remaining in their homes, special invalid people with a high risk of falling in their homes, doctors/care taking people, people practicing fitness exercises to improve their health, and institutions/organizations, who manage a clinical knowledge & information data basis or analyses of patient data.

On one side the number of the elderly is increasing permanently, on the other side, the doctors' anterooms are overcrowded. Therefore, telecare and telehealth systems get more and more important. M2M applications for eHealth support the remote management of patient illnesses by e.g. tracking blood sugar levels, controlling insulin dosage, measuring blood pressure and heartbeat, record infrequent abnormal heart rhythms, etc.

M2M applications for eHealth can enable the elderly to live an independent life and remain in their homes in cases when normally assistance would be needed. Remote monitoring of patient vital signs (e.g. pulse, temperature, weight, blood pressure) minimizes the number of required doctor office visits. Further caretaking measures ensure that patients are taking their medications according to the required schedule and to track the activity level of seniors (e.g. time spent in bed each day, amount of daily movement in their homes) as a way of inferring their overall health and detecting changes that may require a doctor's or some other person's attention.

Various studies have concluded that falls in the home are the most common cause of injury among the elderly population, and one of the leading causes of morbidity and mortality among this population. A so called 'long lie' is a fall, in which the person remains on the ground for 5 min or more before being able to get up without assistance, or help arriving, which could detrimentally affect both the psychological as well as physical wellbeing of the individual. Automated fall detection systems are using worn fall detectors, which trigger an alarm, when both the orientation and acceleration forces of the person reach a pre-set threshold. In case of an emergency detection, an alarm will be sent immediately to the emergency service centre, possibly together with pictures or videos, which a camera being installed in the home has taken.

M2M applications for eHealth can be used to record health and fitness indicators such as heart and breathing rates, energy consumption, fat burning rate, etc. during exercise sessions, and to log the frequency and duration of workouts, the intensity of exercises, running distances, etc. When this information is uploaded to a back-end server, it can be used by the user's physician as part of their health profile, and by the user's personal trainer to provide feedback to the user on the progress of their exercise program. It allows adapting exercise programs or physiotherapy more precisely and more quickly to the needs of the patient/user.

This use case assumes that there is an interoperability platform (oneM2M) that offers a standard interface to monitor and control all the eHealth devices regardless of vendor. It is supposed that professional knowledge generation bodies (e.g. colleges/universities) get authorization to access the patient data. They can assist clinicians for the appropriate diagnosis and method of treatment by providing clinical (textual) guidelines and recommendations in order to reduce the risk of medical errors and to assist in decision-making processes.

Assuring interoperability between all the various data producing, data storing, and data processing components, semantic discovery and query mechanisms across and between sensors, devices, APIs and even IoT platforms are essential.

12.32.2 Source

RDM-2020-0030R04-Healthcare_network_and_clinical_knowledge_administration

> Note: informative sources refer to following documents:
>
> ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach [i.31].
>
> ETSI TR 103 714 SmartM2M; Study for oneM2M Discovery and Query use cases and requirements[i.23].
>
> AIOTI Report: IoT Relation and Impact on 5G, Release 2.0 [i.32].

12.32.3 Actors

- M2M eHealth devices, e.g. wearable sensors, falling detectors, blood pressure meter
- Emergency supervisor
- Doctors and caring people
- Knowledge generation bodies

- M2M Service providers
- M2M Applications e.g. data analytics

12.32.4 Pre-conditions

M2M devices in the patients / the elderly homes and fitness locations have been installed and registered to their corresponding M2M Service Provider. In this use case, the devices are represented by ADN registered to MN-CSEs.

The M2M Application Providers 1, 2 and 3 have relationships one with each other.
The M2M Service Providers 1 and 2 host information on the devices located in the patients / the elderly homes and fitness locations.

The doctors and caring people want to make use of the devices in the patients / the elderly homes and fitness locations in order to check the health or behavioural data of the patients as a way of inferring their overall health and detecting changes that may require a doctor's or some other person's attention.
The emergency supervisor is operating the Intelligent Emergency Response System and manages alarms.

The M2M Service Provider 3 wants to access data from of the M2M Service Providers 1 and 2 in order to manage its knowledge data basis and to update analysis results, recommendations and guidelines.

12.32.5 Triggers

The doctor or caring person, the API "Clinicians patient data analysis" or the M2M Service Provider 3 (further on called "REQUESTER") sends an Advanced Semantic Discovery Query to the M2M Service Provider 1 or 2 (further on called "REQUEST RECEIVER"). The query contains information about the device to be discovered, e.g., a device type, a localization and other filters criteria, such as performance and priority.

12.32.6 Normal Flow

Following, one example of a typical scenario is described:

1. Via a device (e.g., user terminal), which is connected to the API "Hospital", the doctor or caring person initiates a Advanced Semantic Discovery Query within the domain of the M2M Service Provider 1 to an eHealth device type of a specific group of patients, which enquires information about the pulse, temperature, weight, or blood pressure.
2. The API "Hospital" verifies the integrity of the Advanced Semantic Discovery Query and sends a semantic discovery request to the MN-CSE of the specific group of patients.
3. The MN-CSE searches for the specific requested type of devices whether they are connected or not.

4. If the requested type of devices are connected to the MN-CSE, then it returns the requested information of the devices to the M2M Application.
5. If the requested devices are not connected to the MN-CSE, then a negative acknowledge is sent back to the M2M Application.
6. The API "Hospital" processes, if necessary, the received information and forwards it to the requesting device of the doctor or caring person.

12.32.7 Alternative Flow

Following, one example of an alternative scenario is described:

1. An M2M Application of the Service Provider 3 (Clinical knowledge & information) initiates a Advanced Semantic Discovery Query within the domain of M2M Service Providers 2 to find and identify the sensors of their treadmills, which enquires information about activities of users.
2. The IN-CSE of the Service Provider 2 verifies the integrity of the Advanced Semantic Discovery Query and distributes it to the MN-CSEs of the fitness locations.
3. The MN-CSEs searches for the specific requested type of devices whether they are connected or not.
4. If the requested type of devices are connected to the MN-CSE, then it returns the requested information of the devices to the IN-CSE, which forwards it to the requesting Service Provider 3.
5. If the requested devices are not connected to the MN-CSE, then a negative acknowledge is sent back to the IN-CSE, which forwards it to the requesting Service Provider 3.
6. The requesting M2M Application of Service Provider 3 processes the data and provides them in an appropriate way to the users of the M2M Application (e.g. "Clinicians patient data analysis centre").

12.32.8 Post-conditions

The REQUESTER (doctors or caring people, the API "Clinicians patient data analysis" or the M2M Service Provider 3) can start to employ the devices based on the Advanced Semantic Discovery Query sent to the M2M Service Provider 1 or 2.

12.32.9 High Level Illustration

12.32.10 Potential requirements

The following potential requirements are additional to the ones already identified in clause 12.29, 12.30 and 12.31:

1. Advanced Semantic Discovery shall prioritize queries, e.g. to ensure a quick response to urgent situations.
2. Advanced Semantic Discovery shall minimize complexity to avoid impacting negatively the oneM2M system performance.

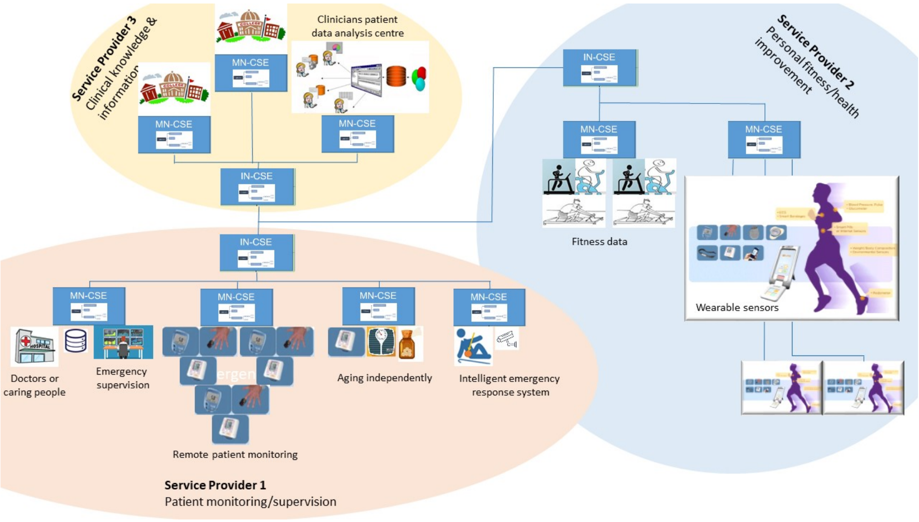


Figure 105: Figure 12.32.9-1 Healthcare network and clinical knowledge administration

12.32 Wildfire alert service with edge gateway

12.33.1 Description

Wildfire alert service is designed to detect the fire in advance. The service is provided over the selected area which can be the village, heritage site etc. Once the area is selected, drones distribute sensors over the area. To gather the CO2 and temperature measurement data from the sensors, edge gateways are deployed in the area. When the gateway receive the data from the sensor, the gateway processes the raw data via machine learning module. The machine learning module provides funcions of extracting the raw data/transforming into the standardized model, removing malfunction data in order to locate the fire. Then the processed data is sent to a M2M platform. The M2M platform is connected to the national disaster management system to share the emergency information with relavent stakeholders (e.g local government).

12.33.2 Source

RDM-2019-0134R01-Wildfire_alert_service_with_edge_gateway

12.33.3 Actors

- disposable IoT sensor: measures CO2 and temperature periodically to make sure the sensor is working properly.
- edge gateway: serves as a bridge between sensors and the M2M platform. Furthermore, this gateway processes raw data from the sensors and reports

it to the platform.
- M2M platform: provides IoT common services functions (e.g. data sharing, subscription/notification).
- local government: sends public warning message as well as cooperates with forestry administration and fire department.

12.33.4 Pre-conditions

- Sensors report measurement data to the gateway periodically. The data will be stored in the M2M platform.
- Each disposable sensor has data container on the M2M platform to save the sensor measurement data.
- Sensors are spread over the area and registered to the gateway. The gateway choose the pre-defined data model to save the data such as device information, measured data. The data is sent to the M2M platform with the chosen data model.

12.33.5 Triggers

- CO2 level and temperature get higher than certain threshold(s).

12.33.6 Normal Flow

1. When the wildfire outbreaks, the sensors near the fire can detect the radical changes of temperature and CO2.
2. The edge gateway verifies that there ourbreaks the wildfire by the machine learning module.
3. The gateway reports information of the fire, such as location of the fire, status of wildfire to the M2M platform.
4. The M2M platform sends the message contains warning information to the local government.

12.33.7 Alternative Flow

None

12.33.8 Post-conditions

None

12.33.9 High Level Illustration

12.33.10 Potential requirements

1. The oneM2M System shall be able to store historical geo-location of an entity.

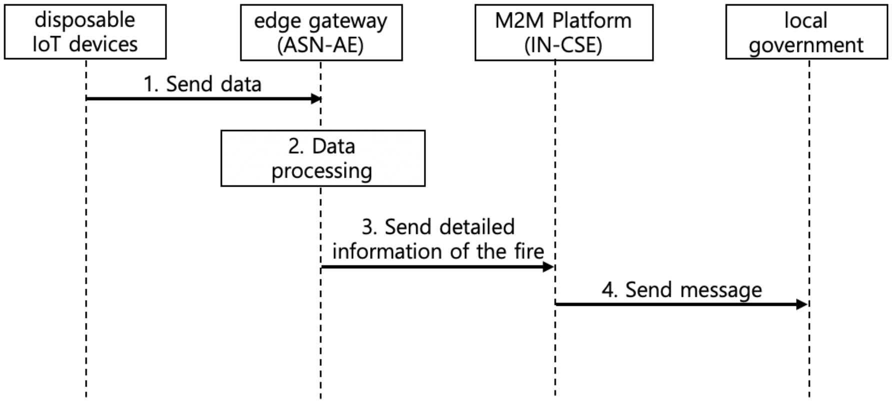


Figure 106: Figure 12.33.6-1 Normal flow - Wildfire alert service with edge gateway

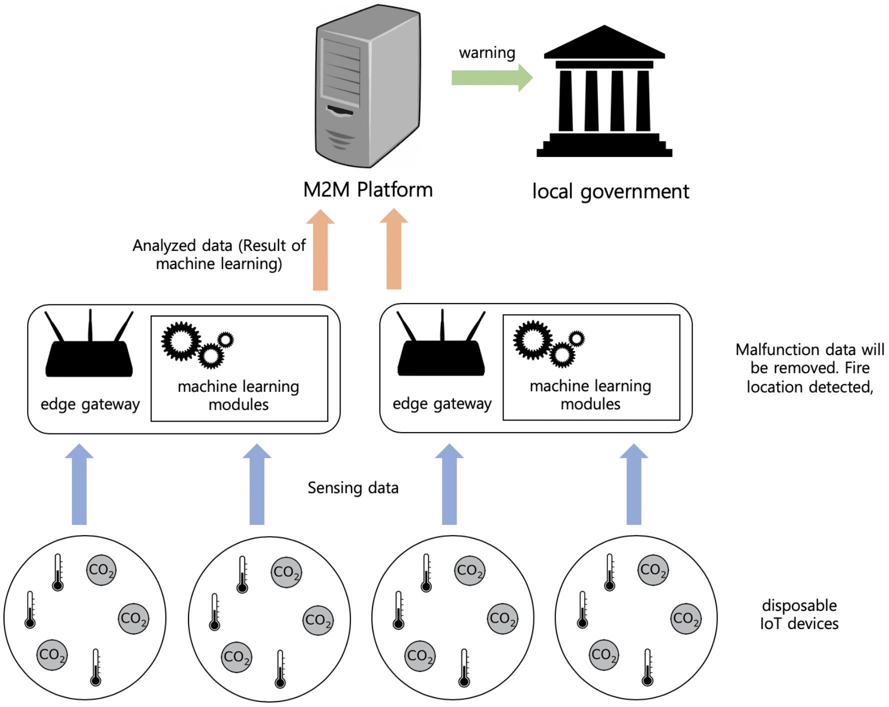


Figure 107: Figure 12.33.9-1 High Level Illustration - Wildfire alert service with edge gateway

12.34 Semantic mapping between IoT ontology and object identifiers

12.34.1 Description

With the development of communications and artificial intelligence technologies, the value of Internet of Things (IoT) is no longer limited to ubiquitous communication networks but providing intelligent services to human beings. These intelligent services appear in many representative scenarios without the aid of human intervention, such as smart home, self-service store, etc. To achieve these scenarios, objects with heterogeneous identifiers (e.g. EPC, Handle, OID, ucode, mCode, Ecode, etc.) need to cooperate with each other without the human intervention. However, all the existing identifiers appear as a sequence of characters and generally lack semantic information. IoT objects cannot identify what the interactive or cooperative object is through the identifier alone. Therefore, oneM2M system needs to enable semantic mapping between IoT ontology and identifiers to facilitate the IoT intelligence. Besides, the operations including create, retrieve, update, and delete (CRUD) of instances frequently occur in some smart scenarios. For example, in a self-service store, when a customer enters a store, a new instance belonging to the class "Person" should be added to the IoT ontology automatically. If a commodity has been bought by a customer, this "commodity" instance should be deleted from the ontology. It is impractical to achieve these instance operations manually. It requires a semantic mapping between the ontology and the identifiers of objects, which will help the IoT system to manage the instances in an unattended manner.

Take a coffee with an EAN-13 identifier (8938515483013) for example. The oneM2M platform can add semantic information (1.4.4.2) to the legacy identifier, which indicates a path from the root node to a class node in the IoT ontology. From the semantic information (1.4.4.2), this object can be mapped to the class "Coffee" other objects can know this identified object is a **Coffee** instance.

12.34.2 Source

RDM-2019-0093-use_case_for_semantic_mapping_between_IoT_ontology_and_object_identifiers

12.34.3 Actors

- Application: the device or object which wants to be mapped to the IoT ontology through its identifier.
- The ontology is a vocabulary with a structure. It could capture a shared understanding of a domain of interests and provide a formal and machine interpretable model of the domain.
- The M2M service platform provided by the M2M service provider
  - a. The M2M service platform has a semantic mapping function to discover the associated class that an object belongs to. It's a service layer functionality provided by the oneM2M System.

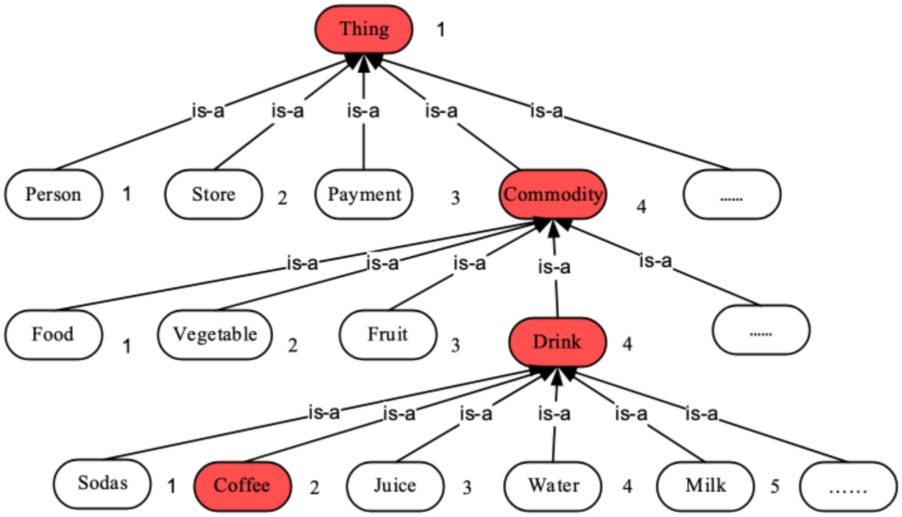


Figure 108: Figure 12.34.1-1 A part of the IoT ontology

12.34.4 Pre-conditions

The IoT ontology is required to be deployed on the M2M service platform.

The semantic information of identifiers is required to be related with the IoT ontology.

12.34.5 Triggers

An object is required to be mapped to the IoT ontology as an instance or identify what the interactive object is through its identifier.

12.34.6 Normal Flow

The normal message flow is described as follows:

1. An application sends a request for mapping an object to the ontology or identifying an object to the M2M service platform, which contains the identifier of the object with semantic information added.
2. After receiving the request, the oneM2M platform extracts semantic information from the identifier.
3. The oneM2M platform then finds the class associated with the object based on the extracted semantic information of the identifier.
4. The oneM2M platform returns the name of the class to the application.

12.34.7 Alternative flow

None

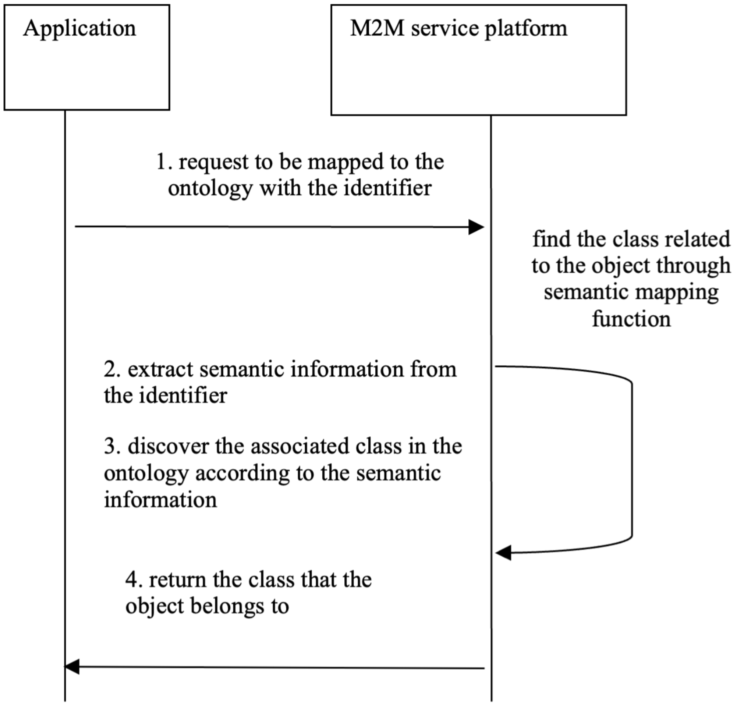
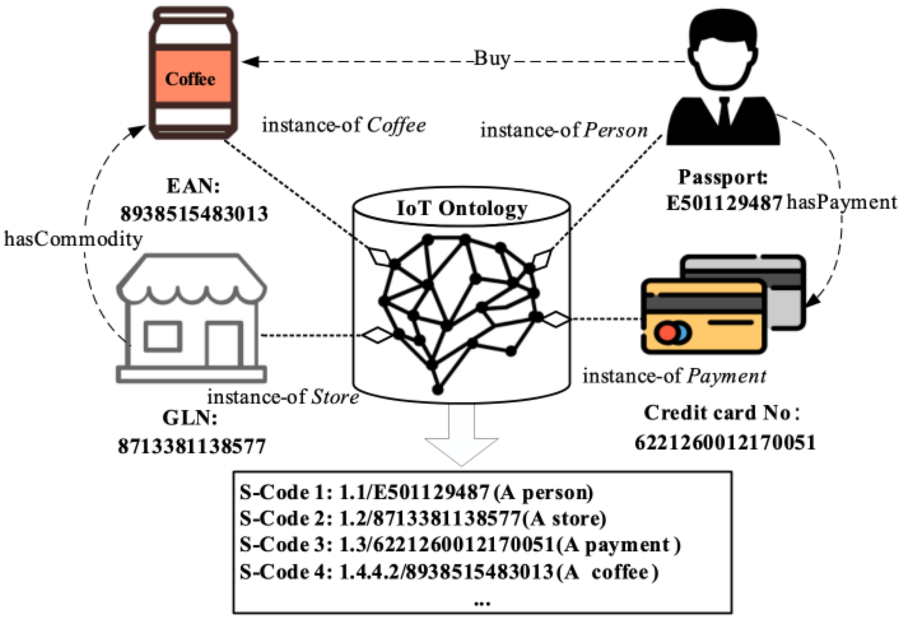

Application
M2M service platform
1. request to be mapped to the ontology with the identifier
find the class related to the object through semantic mapping function
2. extract semantic information from the identifier
3. discover the associated class in the ontology according to the semantic information
4. return the class that the object belongs to

Figure 109: Figure 12.34.6-1 Message flow for sematic mapping between the ontology and an identifier

12.34.8 Post-conditions

None

12.34.9 High Level Illustration



S-Code 1: 1.1/E501129487 (A person)
S-Code 2: 1.2/8713381138577(A store)
S-Code 3: 1.3/6221260012170051(A payment)
S-Code 4: 1.4.4.2/8938515483013(A coffee)
...

Figure 110: Figure 12.34.9-1 High Level Illustration

12.34.10 Potential requirements

The oneM2M System shall be able to provide machine understandable semantic information for object identifiers to map the identified objects to corresponding classes in the IoT ontology and enable objects to identify what the interactive object is independently.

12.35 Access Control using several tokens

12.35.1 Description

In order prevent some hacker attacks when an access is allowed from not protected networks, M2M nodes is enhaced to to expose only non-sensitive resources and to protect sensitive resources (e.g. Firwmare update, sensitive data retrieval). This is based on a request parameter indicating the role of the originator in the access or management of the requested resource. This will allow requests from an originator to be treated differently based on the role specified.

In order to allow this access control dynamically, the usecase requires that management of the access is provided by a DAS (Dynamic Authorisation Server) via tokens.

12.35.2 Source

RDM-2019-0080R02-Access_Control_Using_several_tokens

12.35.3 Actors

- **Managed Device** (for example Air Conditionners)
- **Maintainer (M)** who manages the device resources remotely (e.g. maintenance of Air Conditioners is subcontracted to a **maintainer (M)** who manages the device resources remotely : humidity level, temperature, on/off, power consumption, firmware version,. . . .)
- **Owner (O)** is also able to manage the device remotely (humidity level, temperature,. . .)
- **Dynamic Authorisation Server Owner (DAS_O)** managing authroisations for Owner resources
- **Dynamic Authorisation Server Maintainer (DAS_M)** managaing authorisations for Maintainer resources
- **Management Hub** which can be a gateway to which devices are connected

12.35.4 Pre-conditions

- Devices (like Air Conditionners) are installed as part of Smart Office and connected via Mangement Hub.
- Each actor is associated to a *role*
- **Management Hub** manages the resources exposure based on actors *role* . And validates all tokens used for device management.
- DAS_O (Dynamic Authorisation Server - Owner) provides token(s) based on the permissions/settings controlled by the Owner
- DAS_M (Dynamic Authorisation Server - Maintainer) provides token(s) based on the permissions/settings controlled by the Maintainer

12.35.5 Triggers

The administrator from Maintainer (M) wants to modify the firmware (sensitive device resource).

12.35.6 Normal Flow

Figure 12.35.6-1 illustrates the high-level flows of a use case showing how Maintainer process to update a Firmware of the devices which consists of the following steps:

- Maintainer requests firmware update (via remote access tool)

  - 1.1 Devices Management Hub detects that this request requires authorization from DAS_M (Dynamic Authorisation Server - Maintainer)
- Devices Management Hub rejects the request cause token is required
- Maintaner requests token from DAS_M
  - 3.1 DAS_M detects that this kind of operation requires the second token request from DAS_O (DAS_M needs to know whether a DAS_O token is needed or not. DAS_O can communicate this information through a security policy, documentation or a specific API)
  - 3.2 DAS_M requests a second token from DAS_O
  - 3.3 DAS_O provides a second token to DAS_M
  - 3.4 DAS_M sends both tokens as a list to Maintainer
- Maintaner sends a request for Firmware Update including both tokens
- Devices Menagement Hub performs the following:
  - 4.1 verifies token provided by DAS_M, extracts Owner token
  - 4.2 verifies token provided by DAS_O
  - 4.3 performs Firware Update on Devices
  - 4.4 confirms Firmware Udate request has been proceeded

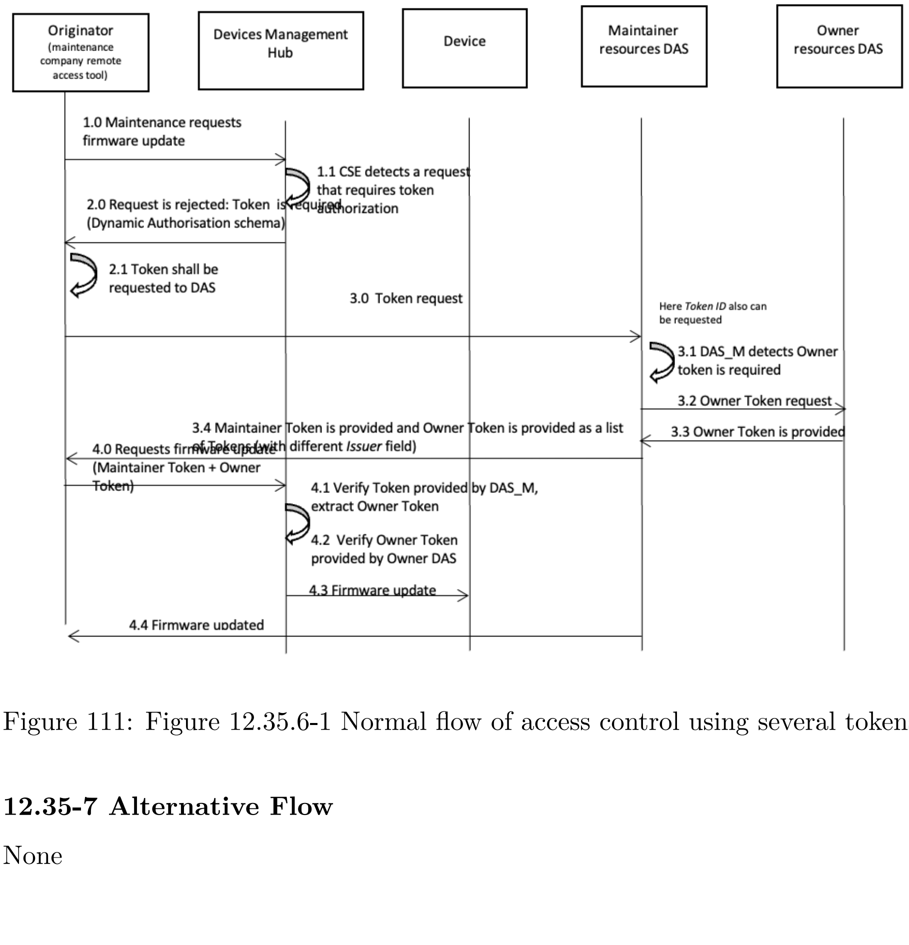

Originator
(maintenance company remote access tool)
Devices Management Hub
Device
Maintainer resources DAS
Owner resources DAS
1.0 Maintenance requests firmware update
1.1 CSE detects a request that requires token authorization
2.0 Request is rejected: Token is required (Dynamic Authorisation schema)
2.1 Token shall be requested to DAS
3.0 Token request
Here Token ID also can be requested
3.1 DAS_M detects Owner token is required
3.2 Owner Token request
3.3 Owner Token is provided
3.4 Maintainer Token is provided and Owner Token is provided as a list of Tokens (with different Issuer field)
4.0 Requests firmware update (Maintainer Token + Owner Token)
4.1 Verify Token provided by DAS_M, extract Owner Token
4.2 Verify Owner Token provided by Owner DAS
4.3 Firmware update
4.4 Firmware updated

Figure 111: Figure 12.35.6-1 Normal flow of access control using several tokens

12.35-7 Alternative Flow

None

12.35.8 Post-conditions

None

12.35.9 High Level Illustration

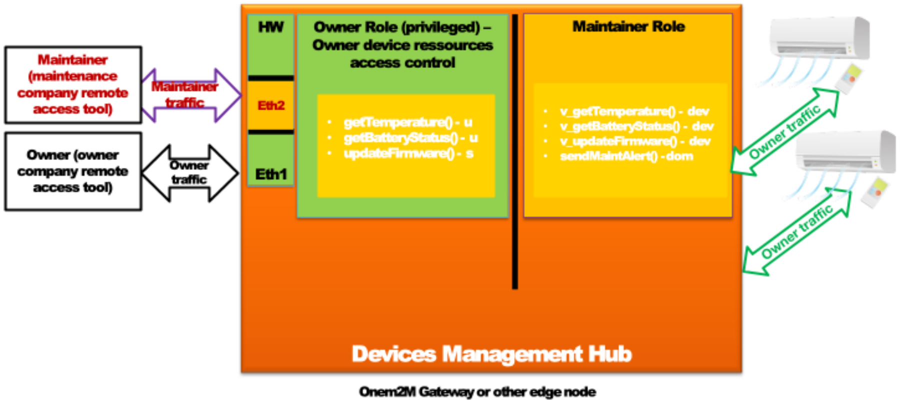

Maintainer (maintenance company remote access tool)
Maintainer traffic
Owner (owner company remote access tool)
Owner traffic
HW
Eth2
Eth1
Owner Role (privileged) – Owner device ressources access control
• getTemperature() - u
• getBatteryStatus() - u
• updateFirmware() - s
Maintainer Role
• v_getTemperature() - dev
• v_getBatteryStatus() - dev
• v_updateFirmware() - dev
• sendMaintAlert() -dom
Owner traffic
Owner traffic
Devices Management Hub
Onem2M Gateway or other edge node

Figure 112: Figure 12.35.9-1: High level illustration

12.35.10 Potential requirements

The M2M System shall support access control methods using validation of more than one token from different servers for a single operation.

12.36 Use case for automatic recognition of identification schemes for heterogeneous IoT identifiers

12.36.1 Description

In Internet of Things (IoT), a unique identifier is required for each object to serve as a digital identity. An identifier is represented using a sequence of numbers, characters, or a combination of them, and the detailed description information about the identified object can be indexed and discovered. For example, people can get the price, place of origin and manufacturer information of a commodity by scanning the product barcode, and the serial number on the barcode is the Global Standard 1 (GS1) identifier of this commodity. However, due to political, commercial and other reasons, there are thousands even tens of thousands of types of IoT identifiers co-existing in the IoT ecosystem (e.g. EPC, Handle, OID, etc.). These schemes have different encoding lengths, value ranges and structures, and each scheme has its own customized resolution rules. It requires different resolution systems to resolve these heterogeneous identifiers respectively. So, if we want to obtain the profile information about an object, the identification scheme of this object's identifier should be known in advance.

Currently, the co-existence of multiple objects tagged by different types of identifiers is becoming the norm. It is unrealistic to require all IoT objects to use the same kind of identifier scheme in IoT applications. Therefore, oneM2M System is required to recognize the identification schemes of IoT identifiers to support the unified resolution of heterogeneous IoT identifiers.

Take commodity source tracing for example. The lifecycle of a commodity is composed of a series of processes including material purchase, manufacturing, storage, transportation, sales, etc. In each process, different manufacturers will choose their conventional identification schemes to identify the commodity. If an application wants to acquire the detailed information about this commodity throughout the chain (of processes), the identification schemes of the identifiers in these processes should be known at first. To satisfy the requirements, the oneM2M System shall be able to recognize the identification schemes of these heterogeneous IoT identifiers from different processes.

12.36.2 Source

RDM-2021-0027R02-use_case_for_automatic_recognition_of_identification_schemes_for_heterogeneous_IoT

12.36.3 Actors

- Application: a device or a user who wants to recognize the identification scheme of an IoT identifier and configure the identified device in an oneM2M deployment.
- The M2M service platform provided by the M2M service provider.
  - a. The M2M service platform has a heterogeneous identification function to automatically recognize the identification scheme of an IoT identifier. It’s a service layer functionality provided by the oneM2M System.

12.36.4 Pre-conditions

The identifier recognition model is required to be deployed on the M2M service platform.

Provision the device in oneM2M, which includes:

- a. Associate with the user profile;
- b. Provide security credentials.

12.36.5 Triggers

The identification scheme of an object’s identifier is required to be automatically recognized.

12.36.6 Normal Flow

The normal message flow is described as follows:

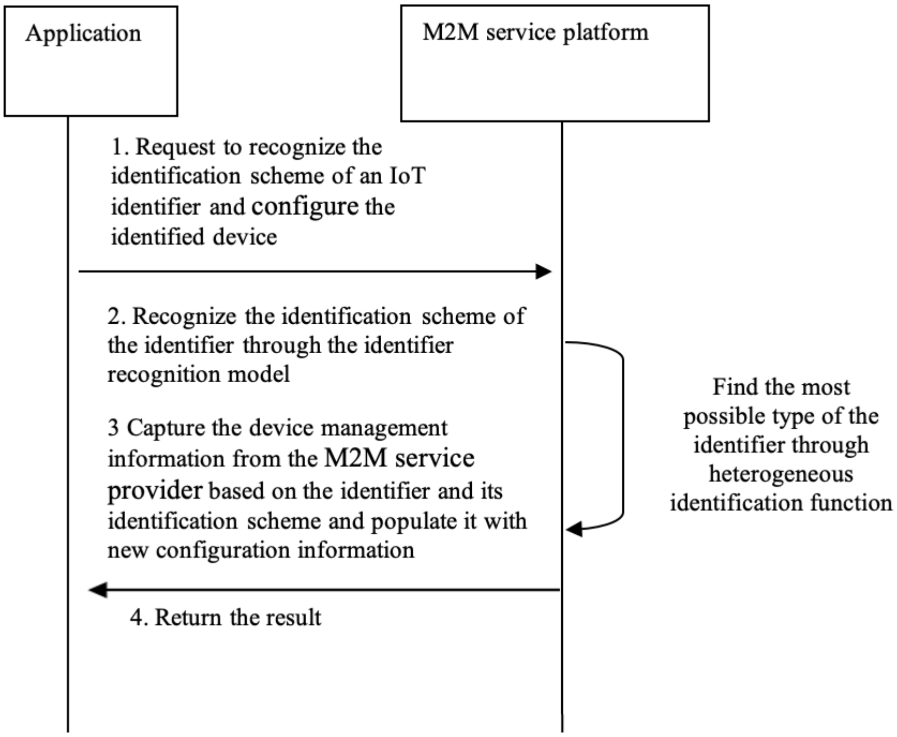

Application
M2M service platform
1. Request to recognize the identification scheme of an IoT identifier and configure the identified device
2. Recognize the identification scheme of the identifier through the identifier recognition model
3 Capture the device management information from the M2M service provider based on the identifier and its identification scheme and populate it with new configuration information
Find the most possible type of the identifier through heterogeneous identification function
4. Return the result

Figure 113: Figure 12.36.6-1-1: Message flow for automatic recognition of identification schemes for heterogeneous IoT identifiers

1. An application sends a request to the M2M service platform to recognize the identification scheme of an IoT identifier and then configure the device in an oneM2M deployment. The identifier recognition model is deployed on the M2M service platform which manifests as a rule base or a machine learning classification model.
2. After receiving the request, the oneM2M platform recognizes the identification scheme of the identifier based on the heterogeneous identification function.
3. Based on the identifier and its identification scheme, the oneM2M platform captures the device management information from the M2M service provider and populates it with new configuration information.
    - a. This identifier becomes a M2M External Identifier (M2M-Ext-ID);
    - b. Populate node resource and device management resources like firmware object, software object, etc.
4. The oneM2M platform returns the result to the application. This can be success or configuration complete message.

12.36.7 Alternative flow

Step 3 above could include an automatic trigger to begin a firmware update with the M2M service provider.

Or the M2M service provider could create resources on behalf of the device/application..

12.36.8 Post-conditions

None

12.36.9 High Level Illustration

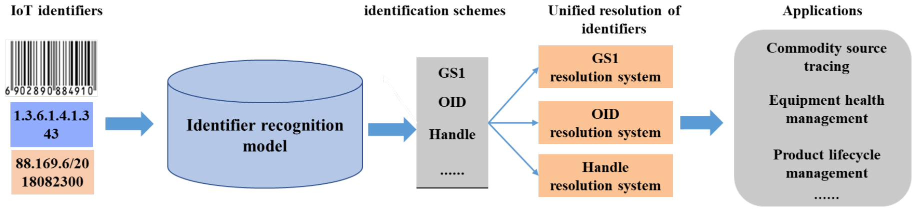


Figure 114: Figure 12.25.9-1: High Level Illustration

12.36.10 Potential requirements

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.

13 History

Publication history		
V5.0.0	<2021-12-02>	Release 5 baseline

Draft history (to be removed on publication)		
V 5.0.0	<2021-12-02>	Fist Rel baseline including following contributions: RDM-2020-0100R01 RDM-2021-0027R02
V5.1.0	<2022-09-26>	This baseline including following contributions: RDM-2021-0087R01_disguise_data_for_security_and_privacy RDM-2022-0009_Use_case_on_vanishing_IoT_sensor RDM-2022-0005-Use_case_on_IoT_device_calibration
V5.2.0	<2025-03-03>	This baseline including following contributions: RDM-2024-0008R04-change_request_TR-0001_with_advanced_semantic_discovery_use_cases
V5.2.1	<2025-04-13>	This baseline includes only the conversion to markdown format
V5.2.2	<2025-06-06>	This baseline including following contributions: RDM-2025-0062-Fixed_editor_notes_after_conversion RDM-2025-0063-Fixed_informative_references_section