ETSI TR 118 501 V1.0.0 (2015-05)

TECHNICAL REPORT

oneM2M Use Case collection

Reference
DTR/oneM2M-000001

Keywords
IoT, M2M, use case

ETSI

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

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

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

Important notice

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document includes a collection of use cases from a variety of M2M industry segments (listed in table 1.1). 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.14].

Table 1.1

Industry Segment	oneM2M Use Cases							
Agriculture								
Energy	Wide area Energy related measurement/ control system for advanced transmission and distribution automation	Analytics for oneM2M	Smart Meter Reading	Environmental Monitoring for Hydro-Power Generation using Satellite M2M	Oil and Gas Pipeline Cellular /Satellite Gateway			
Enterprise	Smart building							
Finance								
Healthcare	M2M Healthcare Gateway	Wellness services	Secure remote patient care and monitoring					
Industrial								
Public Services	Street Light Automation	Devices, Virtual devices and Things	Car/Bicycle Sharing Services	Smart parking	Information Delivery service in the devastated area			
Residential	Home Energy Management	Home Energy Management System	Plug-In Electrical Charging Vehicles and power feed in home scenario	Real-time Audio/Video Communication	Event Triggered Task Execution	Semantic Home Control	Semantic Device Plug and Play	
Retail								
Transportation	Vehicle Diagnostic & Maintenance Report	Remote Maintenance services	Neighbourhood Alerting on Traffic Accident	Fleet management service using Digital Tachograph				
Other	Extending the M2M Access Network using Satellites	M2M data traffic management by underlying network operator	Optimizing connectivity management parameters with mobile networks	Optimizing mobility management parameters with mobile networks	Sleepy nodes	Collection of M2M system data	Leveraging Broadcasting/ Multicasting Capability of Underlying Networks	Service Provisioning for Equipment with Built-in Device

2 References

2.1 Normative references

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

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

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

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

Not applicable.

2.2 Informative references

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

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

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

[i.1] oneM2M Drafting Rules.

NOTE: Available at http://ftp.onem2m.org/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] HGI-GD017-R3: "Use Cases and Architecture for a Home Energy Management Service".

[i.6] ISO/IEC 15118: "Road vehicles -- Vehicle to grid communication interface".

[i.7] Mandate 486: "Mandate for programming and standardisation addressed to the European Standardisation Bodies in the field of Urban Rail".

[i.8] 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.9] ETSI TR 102 638: "Intelligent Transport Systems (ITS);Vehicular Communications;Basic Set of Applications; Definitions".

[i.10] ETSI TS 122 368: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for Machine-Type Communications (MTC); Stage 1 (3GPP TS 22.368)".

[i.11] ETSI TS 123 682: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements to facilitate communications with packet data networks and applications (3GPP TS 23.682)".

[i.12] 3GPP TR 23.887: "Study on Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[i.13] Communications Guidelines defined in Continua Health Alliance, The Continua Version 2012 Design Guidelines.

[i.14] oneM2M-TS-0002: "Requirements Technical Specification".

[i.15] ETSI TS 103 383: "Smart Cards; Embedded UICC; Requirements Specification".

[i.16] IEC 61850: "Communication networks and systems in substations".

3 Abbreviations

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

3GPP	3rd Generation Partnership Project
A/C	Air Conditioner
AHD	Application Hosting Device
AL	Authorization Level
ALU	Alcatel Lucent
AMI	Advanced Metering Infrastructure
AP	Applications Provider
API	Application Programming Interface
ARIB	Association of Radio Industries and Business
ARPU	Average Revenue Per User
BMS	Building Management System
BTS	Bus Ticket System
CCSA	China Communications Standards Association
CCTV	Closed Circuit Television
CEN	Comité Européen de Normalisation
CIS	Customer Information System
CL	Criticality Level
CMS	Cryptographic Message Syntax
CP	Care Provider
CPU	Central Processing Unit
DAP	Data Aggregation Point
DB	DataBase
DER	Distributed Energy Resources
DIN	Deutsches Institut für Normung
DP	Device Provider
DR	Demand Response
DRX	Discontinuous reception
DSO	Distribution System Operator
DSRC	Dedicated Short Range Communications
DTG	Digital TachoGraph
DVR	Digital Video Recorder
EGW	Energy GateWay
EHR	Electronics Health Record
EP	Equipment Provider
EPBA	Equipment Provider Back-end Application
ETRI	Electronics and Telecommunications Research Institute
ETWS	Earthquake and Tsunami Warning System
EU	Equipment User
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
FFS	For Further Study
FMS	Fleet Management Service
GPS	Global Positioning System

GW	Gateway
HAMS	Home Automation Management System
HEM	Home Energy Management
HEMS	Home Energy Management System
HIPAA	Health Insurance Portability and Accountability Act
HMI	Human Machine Interface
HSM	Hardware Security Module
HV	High Voltage
HV/MV	High Voltage/Medium Voltage
ICCID	Integrated Circuit Card Identifier
IEC	International Electrotechnical Commission
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ITS	Intelligent Transportation System
ITS-S	Intelligent Transportation System Station
KCA	Korean Communications Agency
KDDI	Kokusai Denshin Denwa International
LAN	Local Area Network
LATAM	Latin American
LDR	Low Data Rate
LG	Lucky Goldstar
M2M	Machine to Machine
MB	Mega bytes
MDM	Medical Device Manufacturer
MDMMS	Medical Device Monitoring & Management Service
MDMS	Meter Data Management System
MDN	Mobile Directory Number
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
NEC	Nippon Electric Company
NFC	Near Field Communications
NTT	Nippon Telegram and Telegraph
PAN	Personal Area Network
PC	Personal Computer
PEV	Plug-in Electric Vehicle
PEV-SP	Plug-In Electric Vehicle - Service Provider
PEV-SW	Plug-In Electric Vehicle - Software
PKCS	Public Key Cryptology Standards
PLC	Power Line Communications
PMU	Phase Measurement Unit
QoS	Quality of Service
RL	Redaction Level
RPM	Revolutions Per Minute
RSU	Road Side Unit
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDDTE	Small Data and Device Triggering Enhancements
SDS	Samsung Data Systems
SG	Smart Grid
SGCG	Smart Grid Coordination Group
SGIP	Smart Grid Interoperability Panel
SIM	Subscriber Identity Module
SK	South Korea
SLA	Service Level Agreement
SM	Smart Meter
SMS	Short Message Service
SN	Sleepy Node
SP	Service Provider

SW	SoftWare
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSO	Transmission System Operator
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
WAM	Wide Area Measurement
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WG	Wireless Gateway
WIFI	Wireless Fidelity ISO/IEC local area network standard (IEEE 802.11 family)
WLAN	Wireless Local Area Network

4 Conventions

The keywords "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

- Fujitsu, from ETSI TR 102 935 [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 centers.

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:

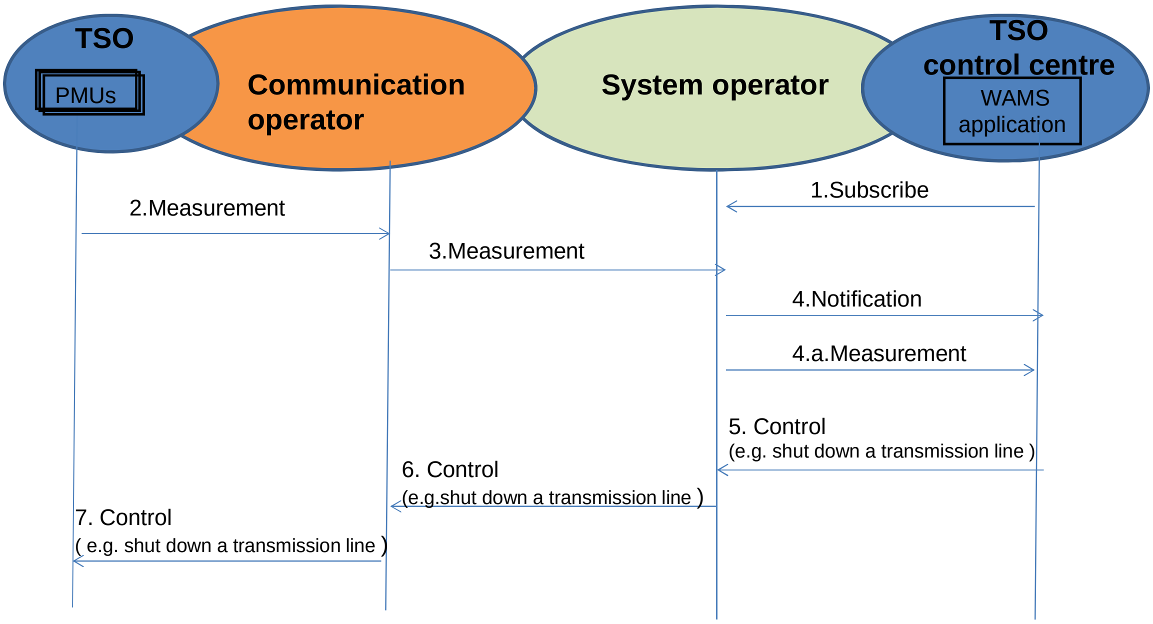

Figure 5.1: An example flow for the TSO scenario

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.
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:

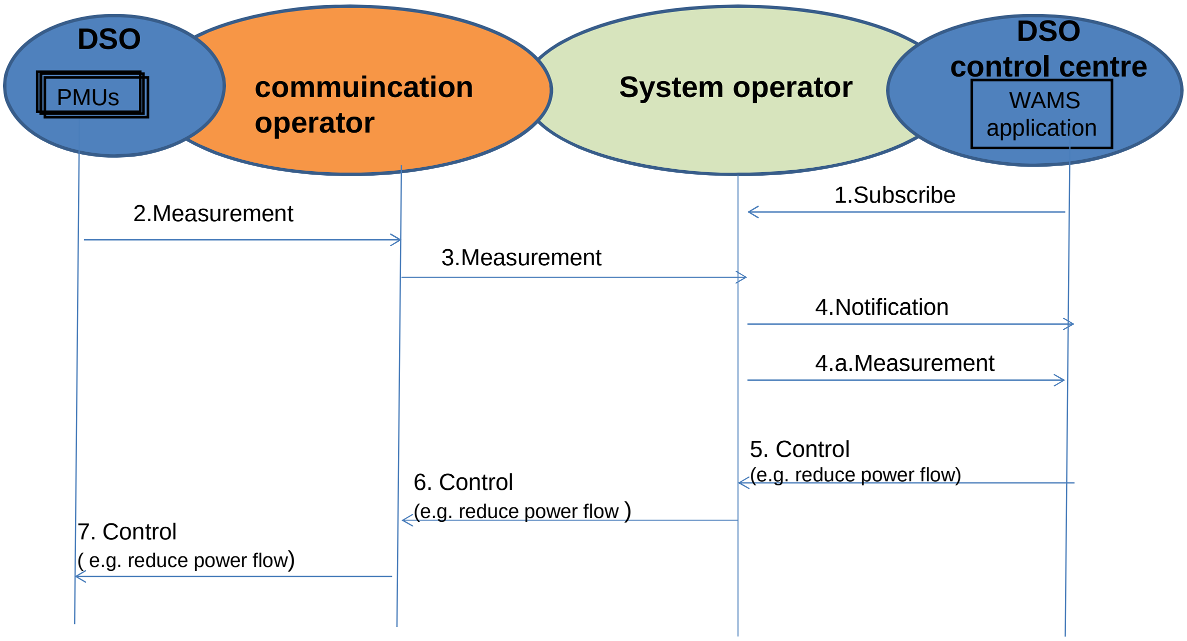

Figure 5.2: An example flow for DSO scenario

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.

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

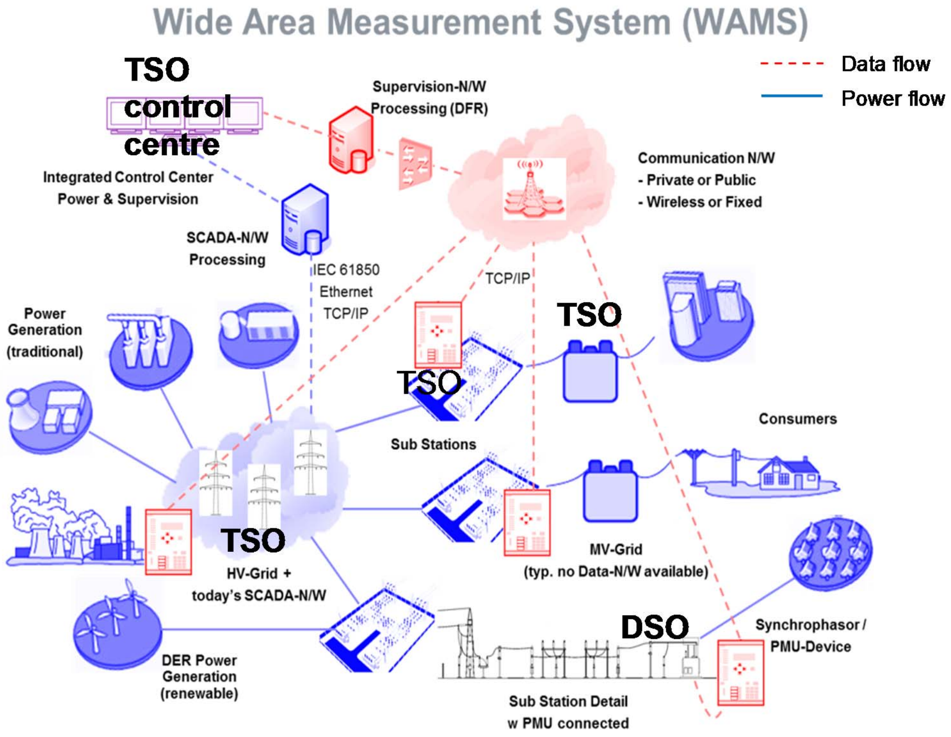
Wide Area Measurement System (WAMS)
Data flow
Power flow
TSO control centre
Integrated Control Center Power & Supervision
Supervision-N/W Processing (DFR)
Communication N/W
- Private or Public
- Wireless or Fixed
SCADA-N/W Processing
IEC 61850 Ethernet TCP/IP
TCP/IP
Power Generation (traditional)
TSO
TSO
Sub Stations
Consumers
TSO
HV-Grid + today's SCADA-N/W
MV-Grid (typ. no Data-N/W available)
DSO
Synchrophasor / PMU-Device
DER Power Generation (renewable)
Sub Station Detail w PMU connected

Figure 5.3: High Level Illustration of Wide Area Measurement System

5.1.10 Potential Requirements

Extracted from ETSI service requirements, ETSI TS 102 689 [i.3], 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 periodic reporting with the time period being defined by the M2M application;

     ▪ 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;

     ▪ 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 remotely 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:

     - Provide functionality to store and retrieve data.

     - Establish storage policies for stored data (e.g. define maximum byte size of the stored data).

     - 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.

        - Where permitted by the security policy, M2M System shall be able to remotely provide the following features, at the Application level:

          o Secure updates of application security software and firmware of the M2M Device/Gateway.

          o 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 Use Case 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).

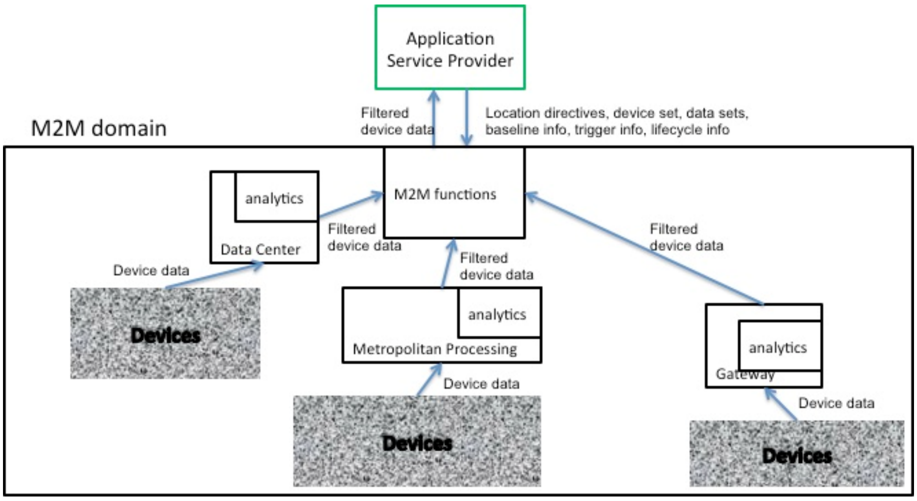

Figure 5.4: Analytics Use Case for M2M

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

- Cisco Systems.

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.

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 clause 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 clause 5.2.7.

5.2.6 Normal Flow

7) The devices provide M2M data to the oneM2M system.

8) The oneM2M system stores a set of M2M data (the storage set) from the devices.

9) The oneM2M system uses analytics to compare M2M data (the trigger set) from devices with the baseline.

10) 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.

11) 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

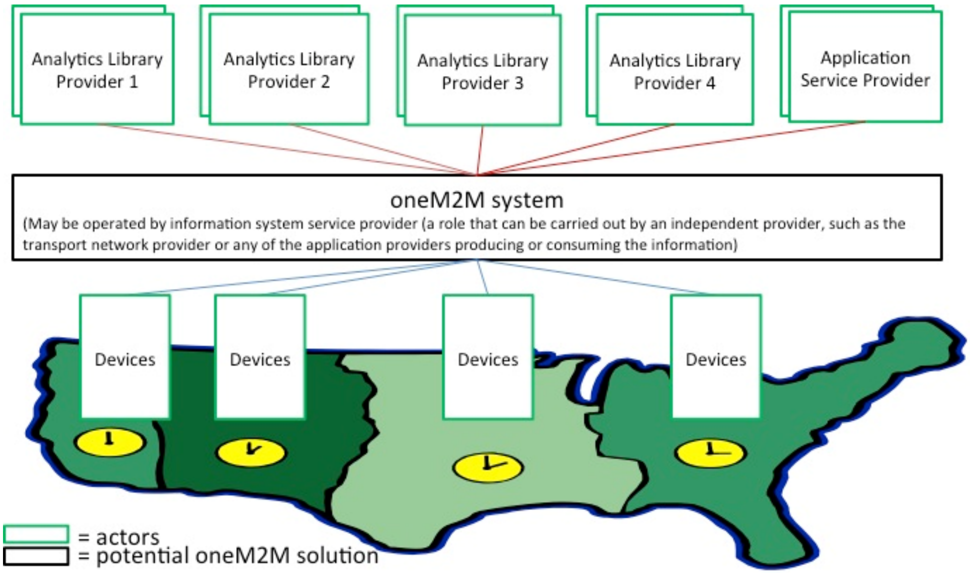
Analytics Library Provider 1
Analytics Library Provider 2
Analytics Library Provider 3
Analytics Library Provider 4
Application Service Provider
oneM2M system
(May be operated by information system service provider (a role that can be carried out by an independent provider, such as the transport network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

Figure 5.5: High level illustration of Analytics use case

5.2.9.1 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, and often have to 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) have to 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 has to 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 has to 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 20 Mb/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 has to be continuously analyzed 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 Applications (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 standardised 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

- Qualcomm (contributor), use case information extracted from SGIP/OpenSG.

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.

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 5.6 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 5.7 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 center 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 center and the smart meter.

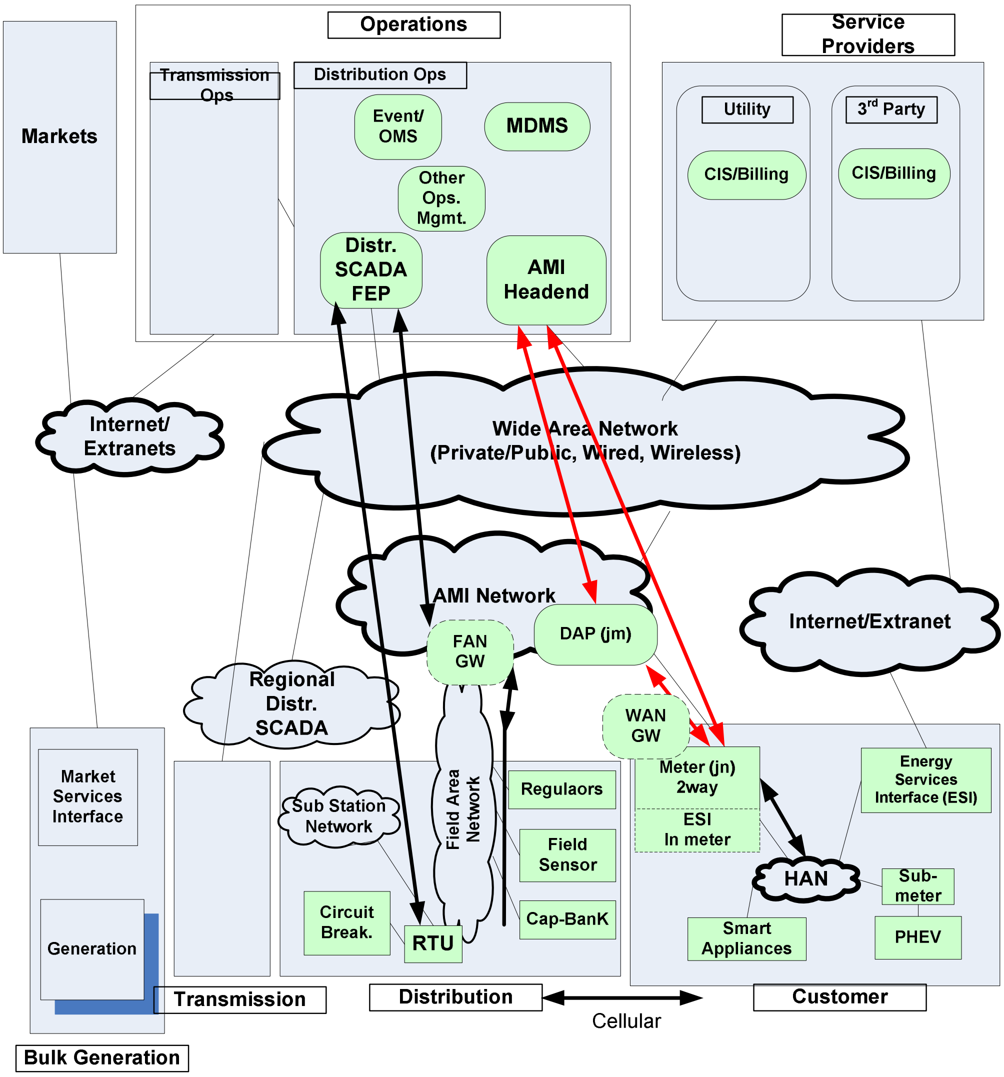

Figure 5.6: Conceptual Actors/Data Flow Diagram

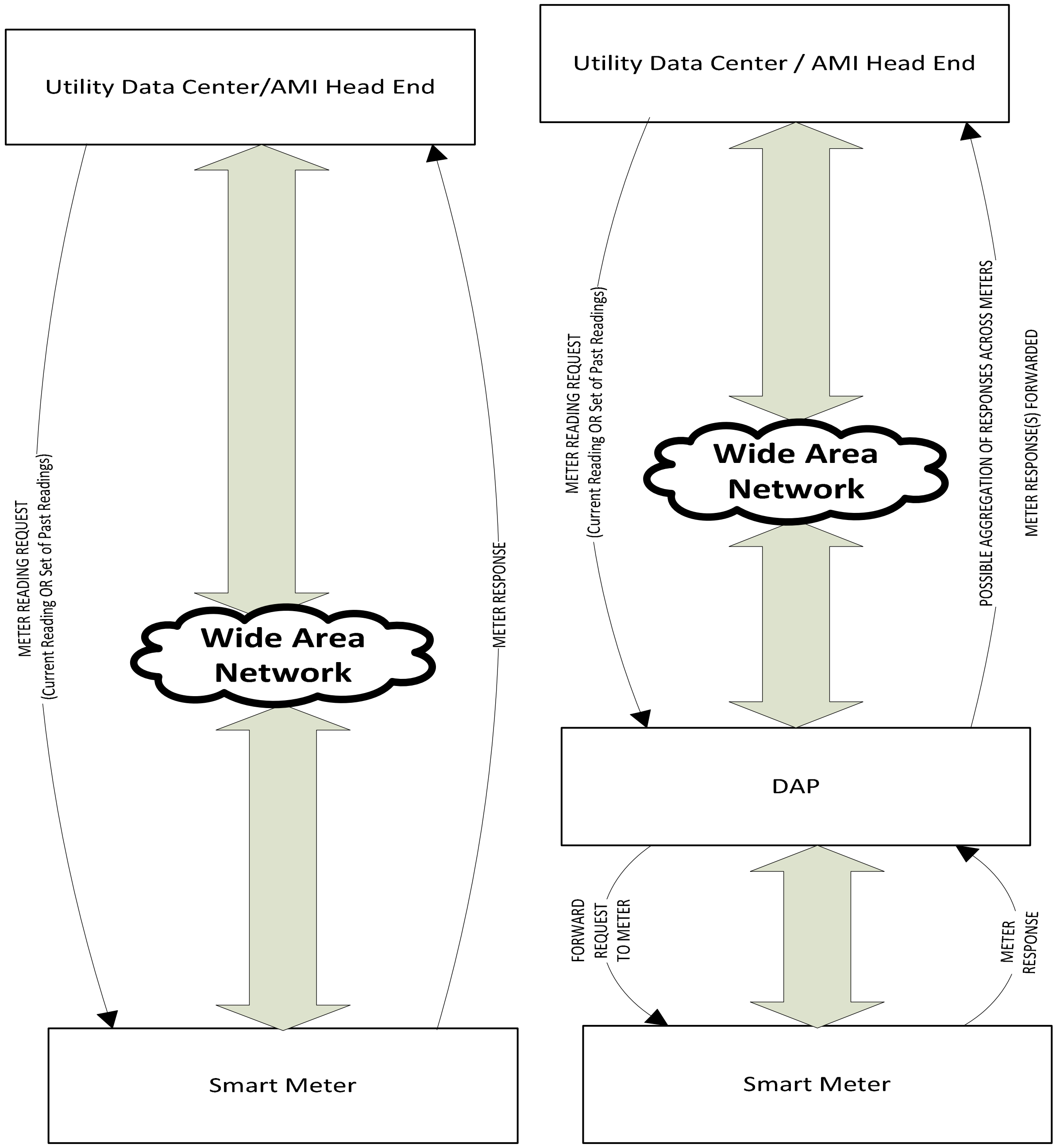
Utility Data Center/AMI Head End
METER READING REQUEST
(Current Reading OR Set of Past Readings)
METER RESPONSE
Wide Area Network
Smart Meter
Utility Data Center / AMI Head End
METER READING REQUEST
(Current Reading OR Set of Past Readings)
POSSIBLE AGGREGATION OF RESPONSES ACROSS METERS
METER RESPONSE(S)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

Figure 5.7: Typical Smart Meter Reading Flows A (on left) and B (on right)

Typically, a utility data center processing application communicates end-to-end via the AMI Headend with a smart meter data application at the edge. Figure 5.7 shows two possible flows A and B depending on whether there is a DAP entity along the path from the Utility Data Center / AMI Headend and the Smart Meter.

In flow A, the Utility Data Center/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 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 Center / 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 Center / 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. The DAP entity can subsequently buffer the data for some time, receive data from many meters, and then submit the aggregated data across meters to the Utility Data Center / 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 Center/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 Center/AMI Head End.

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 10 s to 100 s 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 Center/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 Center/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

None.

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

- Inmarsat.

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-10 MB 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 minimise 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 has to 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.16] (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 (1,5 GHz to 1,6 GHz). This band is unique as it is not attenuated by weather where other high frequency band solutions operate in. Remote terminals in this application has to 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 increase reliability. The L band satellite network has to offer geographical redundancy for downlink earth station and backhaul infrastructure.

Satellite Terminal Solution: The L band satellite terminal has to operate with extremely low power, less than 1 W idle and 20 W 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 has to continually ensure the terminal is on-net. If the terminal seems to be unable to transmit (or receive), the terminal automatically has to 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 signaling. 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

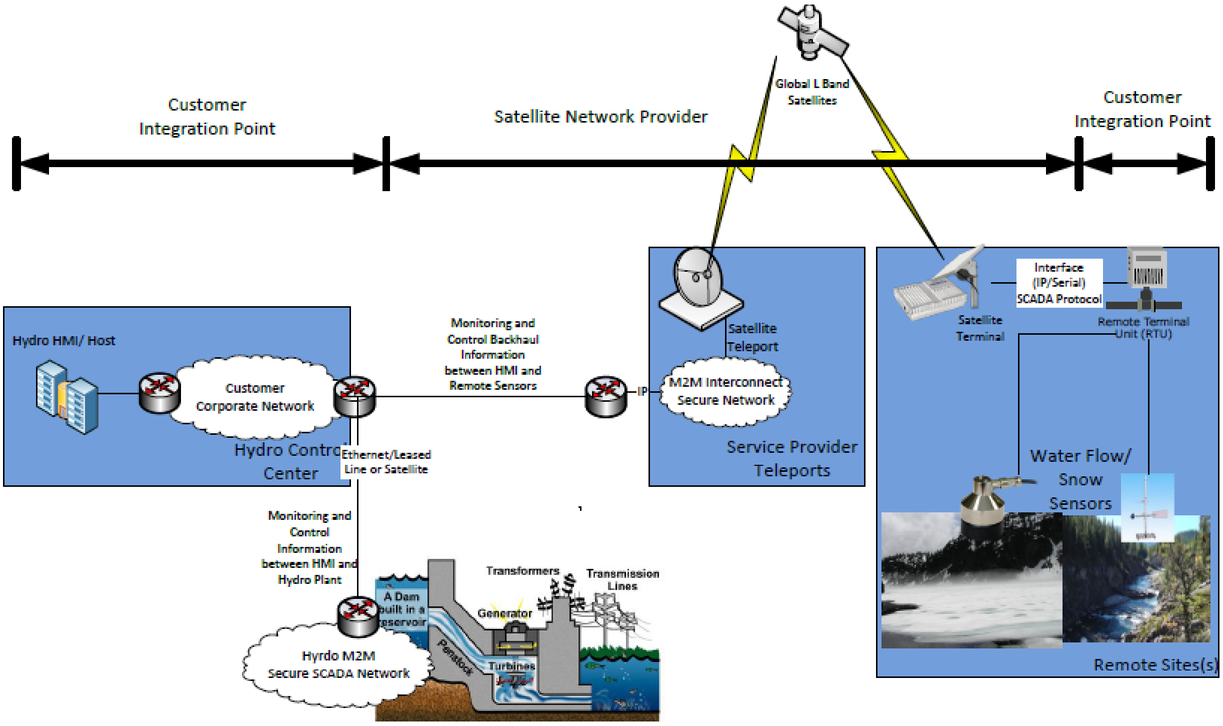

Figure 5.8: High Level Illustration of Environmental Monitoring for Hydro-Power Generation using Satellite M2M

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 has to 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

- Qualcomm.
- KT.

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.

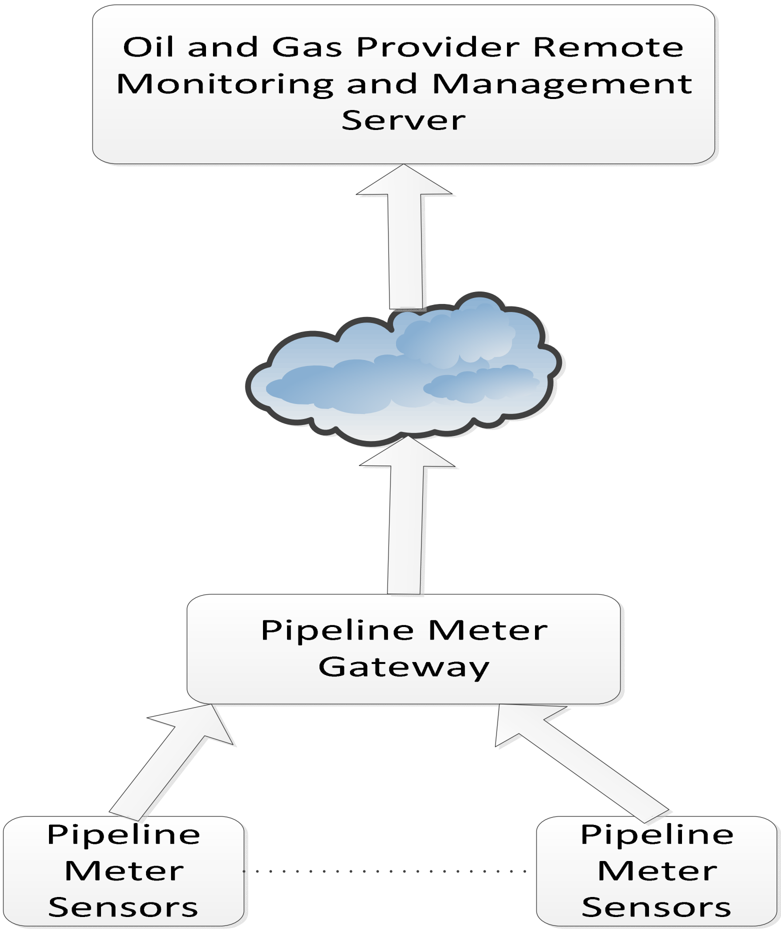

Figure 5.9: Flow - Oil and Gas Pipeline Gateway

5.5.7 Alternative flow

Alternate 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.

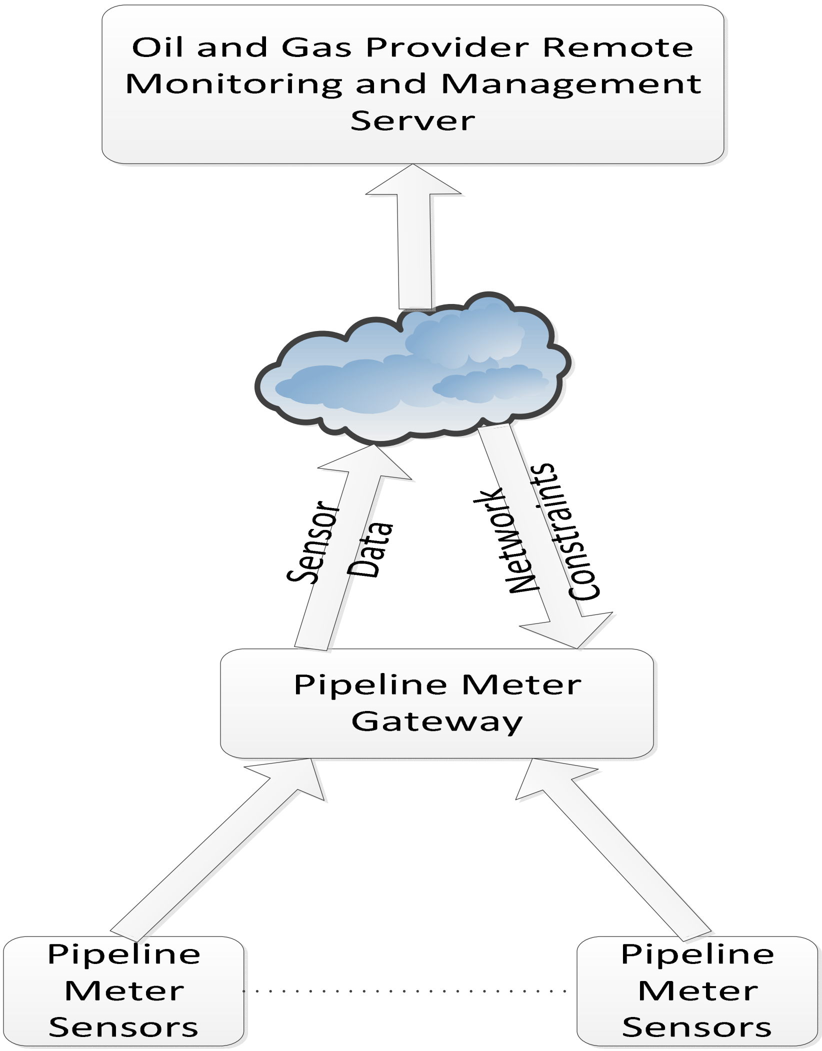

Figure 5.10: Alternate Flow 1 - Oil and Gas Pipeline gateway

Alternate 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.

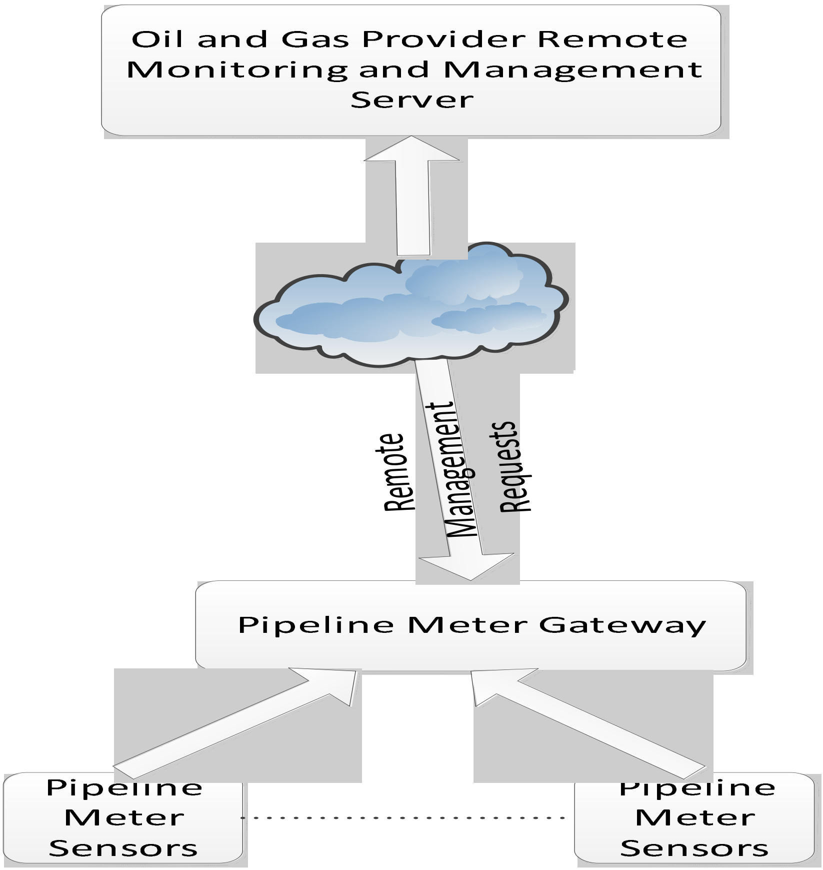
Oil and Gas Provider Remote Monitoring and Management Server
Remote Management Requests
Pipeline Meter Gateway
Pipeline Meter Sensors
Pipeline Meter Sensors

Figure 5.11: Alternate Flow 2 - Oil and Gas Pipeline gateway

Alternate 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.

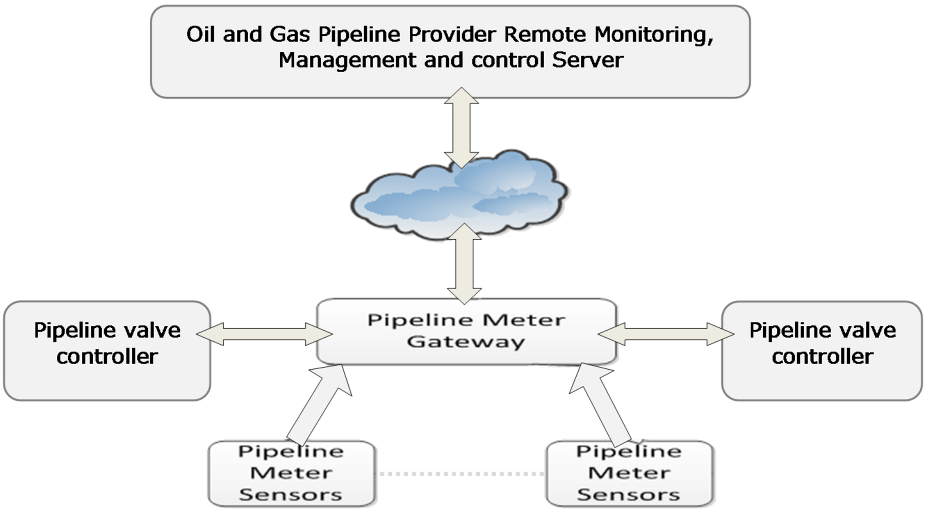
Oil and Gas Pipeline Provider Remote Monitoring, Management and control Server
Pipeline valve controller
Pipeline Meter Gateway
Pipeline valve controller
Pipeline Meter Sensors
Pipeline Meter Sensors

Figure 5.12: Alternate Flow 3 - Oil and Gas Pipeline gateway

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

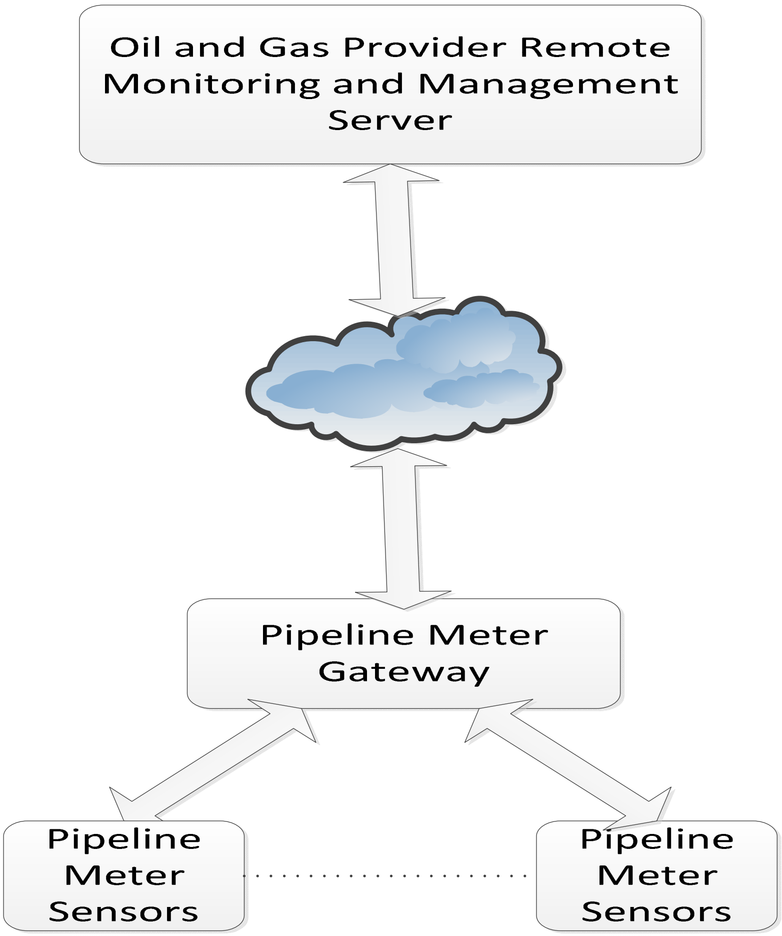

Figure 5.13: High Level Illustration - Oil and Gas Pipeline Gateway

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 multihop 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 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 requirement:

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 requirement:

3) Whenever a pipeline sensor has measurement data available, it shall be 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 100 s 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 requirement:

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, alerter, 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

- Huawei Technologies UK (ETSI).
- Huawei Technologies Co. Ltd (CCSA).
- NEC Europe Ltd. (ETSI).

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 equipments 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.

6.1.4 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, alerter 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

1) 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.

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 5 500 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 mean time, 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.

2) 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 has to 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.

3) 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 mean time 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

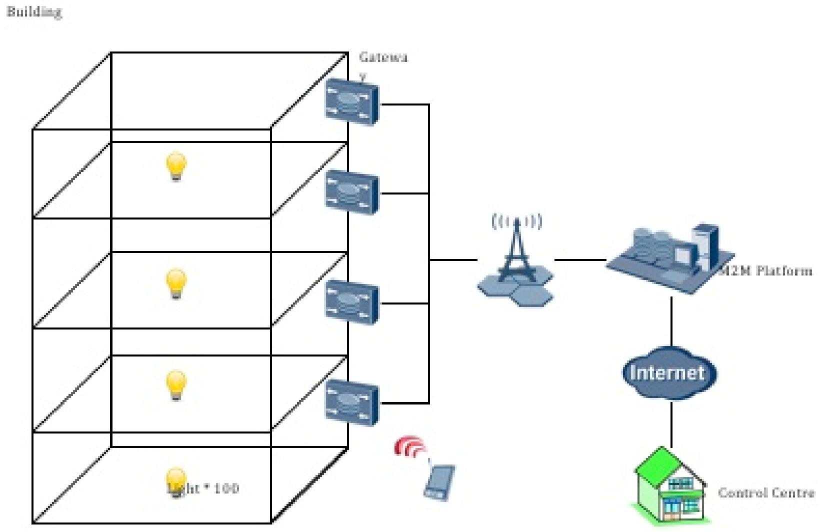

Figure 6.1: Smart Building Scenario

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.

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

- Qualcomm.
- Several scenarios also supported by guidelines [i.13] defined in Continua Health Alliance should be covered by this use case.
- Samsung SDS (as for the alternative flow with some components of the M2M System in failure).

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 a 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 in clause 7.1 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 figure 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.

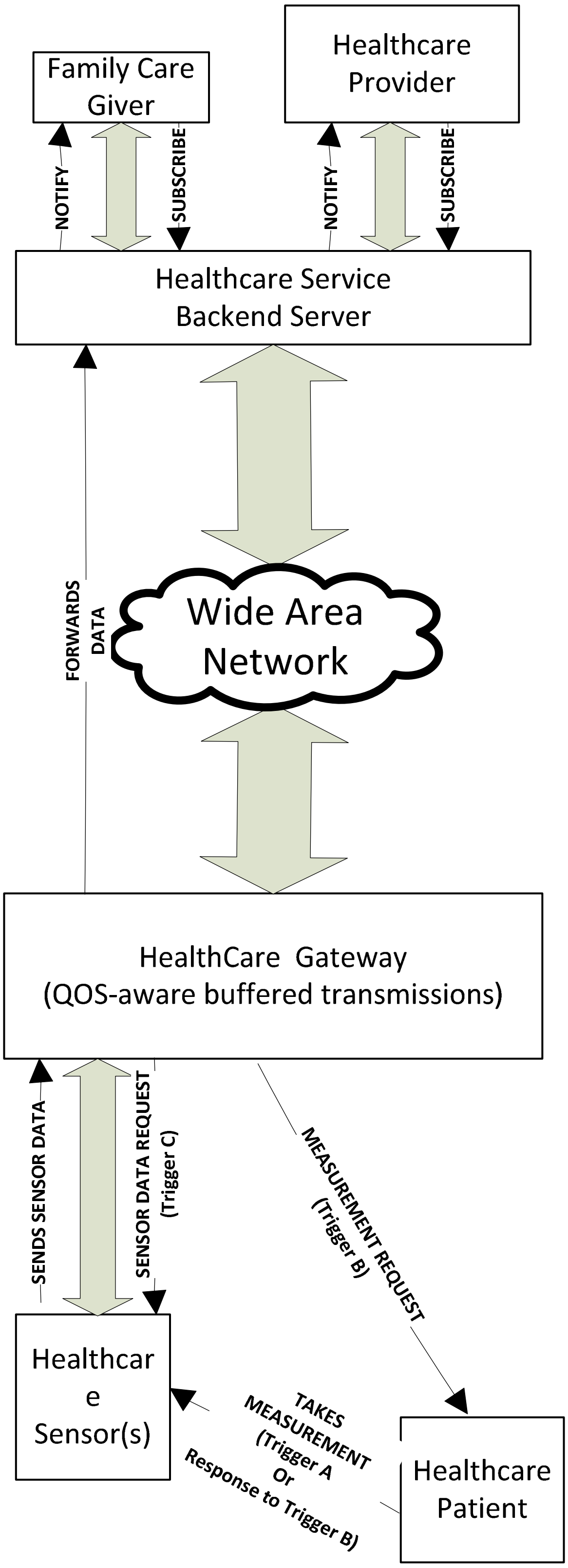
Family Care Giver
Healthcare Provider
NOTIFY
SUBSCRIBE
NOTIFY
SUBSCRIBE
Healthcare Service Backend Server
FORWARDS DATA
Wide Area Network
HealthCare Gateway (QOS-aware buffered transmissions)
SENDS SENSOR DATA
SENSOR DATA REQUEST (Trigger C)
MEASUREMENT REQUEST (Trigger B)
Healthcar e Sensor(s)
TAKES MEASUREMENT (Trigger A Or Response to Trigger B)
Healthcare Patient

Figure 7.1: Healthcare Measurement Data Processing Flow

7.1.7 Alternative flow

Alternative Flow 1- Network/Device-aware transmissions

The flow in figure 7.2 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.
- 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.

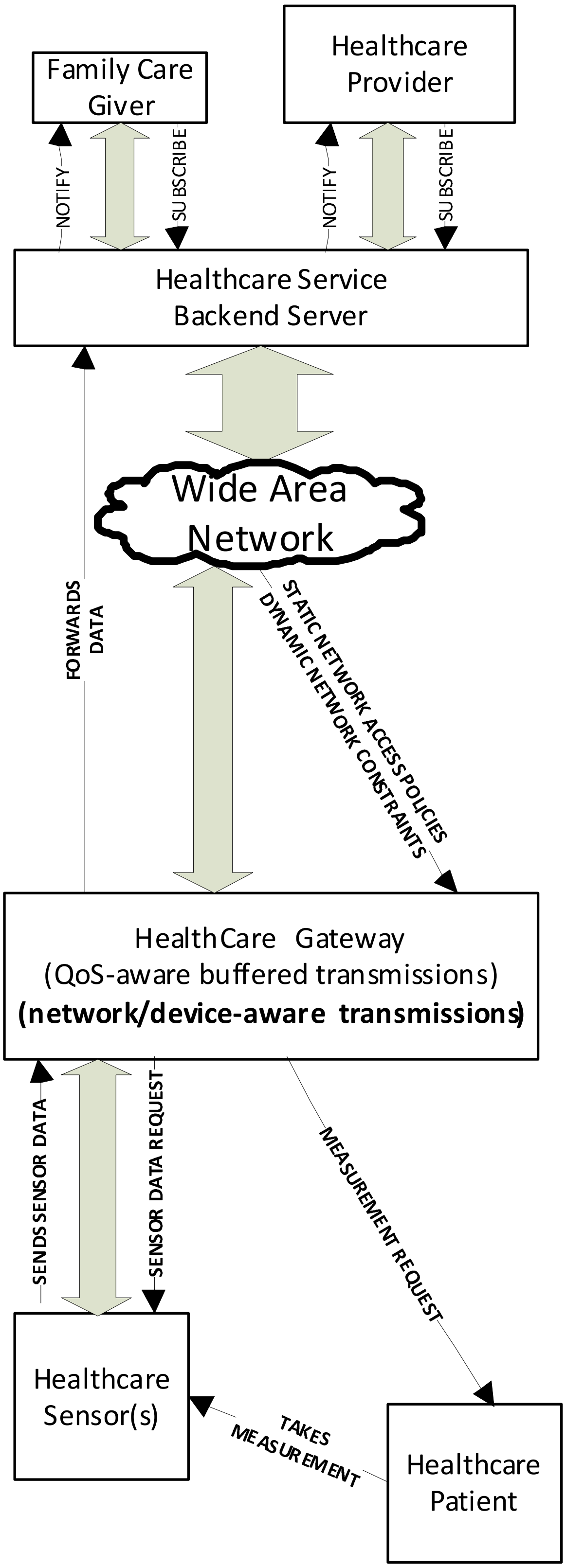

Figure 7.2: Network/Device-aware Flow

Alternative Flow 2- Remote Monitoring

Figure 7.3 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.

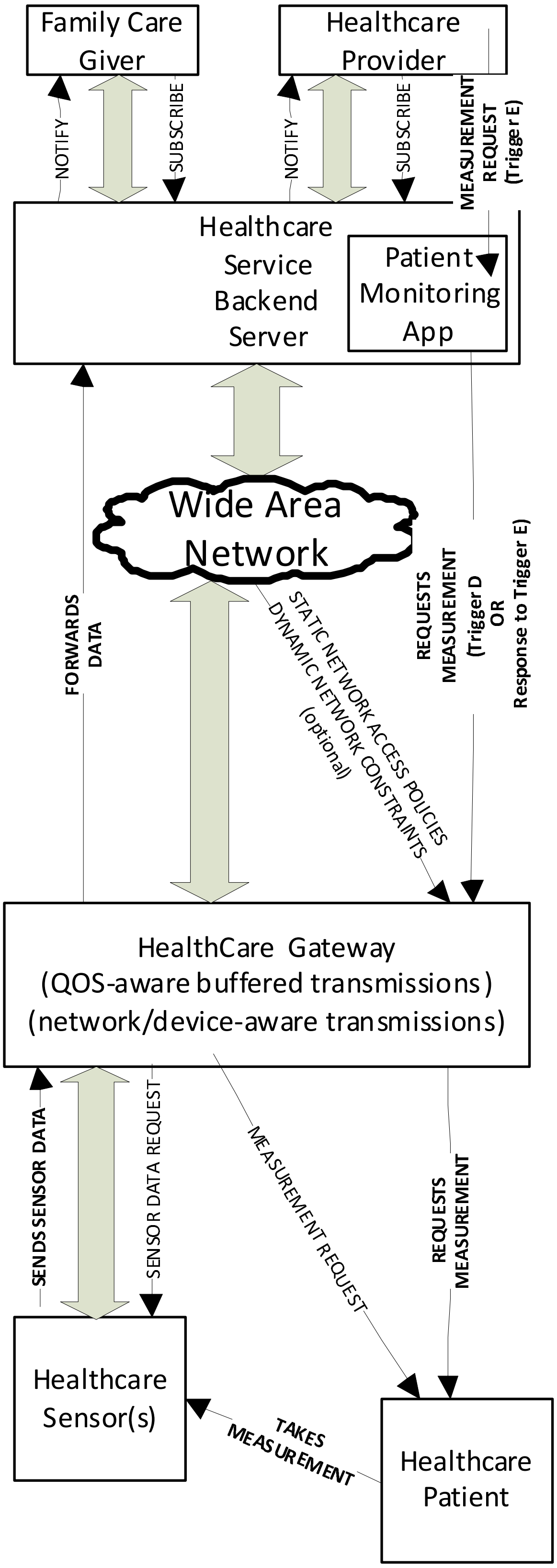

Figure 7.3: Remote Monitoring Flow

Alternative Flow 3 Local Gateway Data Analysis

Figure 7.4 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.

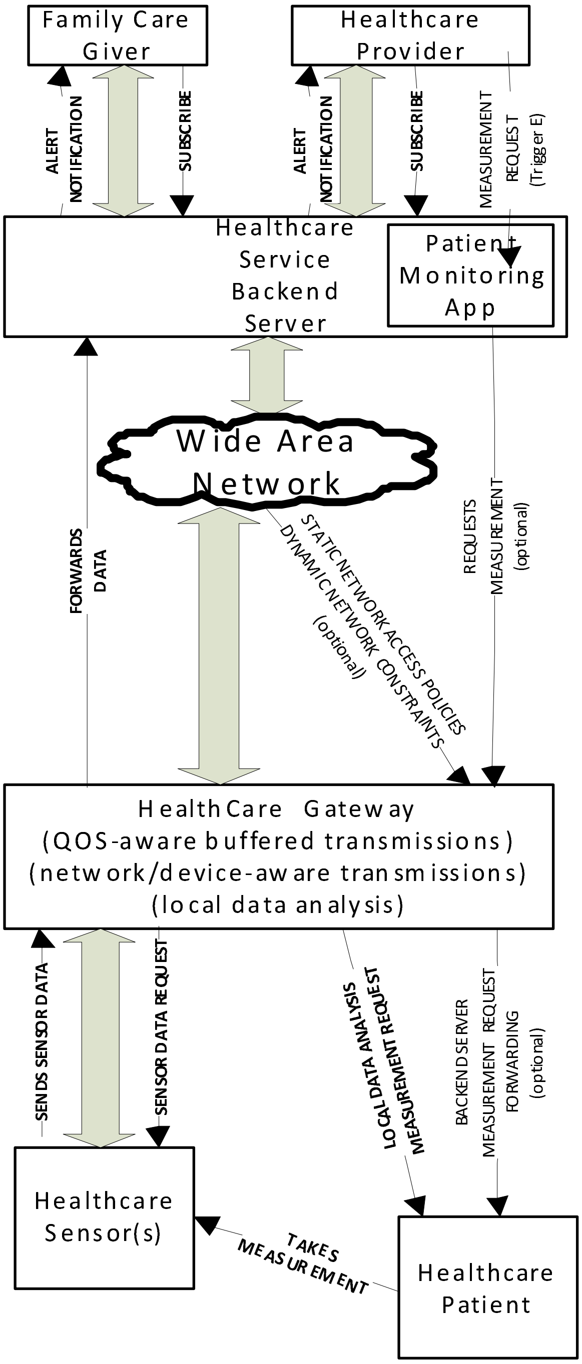
Family Care Giver
Healthcare Provider
ALERT NOTIFICATION
SUBSCRIBE
ALERT NOTIFICATION
SUBSCRIBE
MEASUREMENT REQUEST (Trigger E)
Healthcare Service Backend Server
Patient Monitoring App
Wide Area Network
FORWARDS DATA
STATIC NETWORK ACCESS POLICIES
DYNAMIC NETWORK CONSTRAINTS (optional)
REQUESTS MEASUREMENT (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 7.4: Local Gateway Data Analysis Flow

Alternative Flow 4 - Partial Failure Case

Figure 7.5 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.)

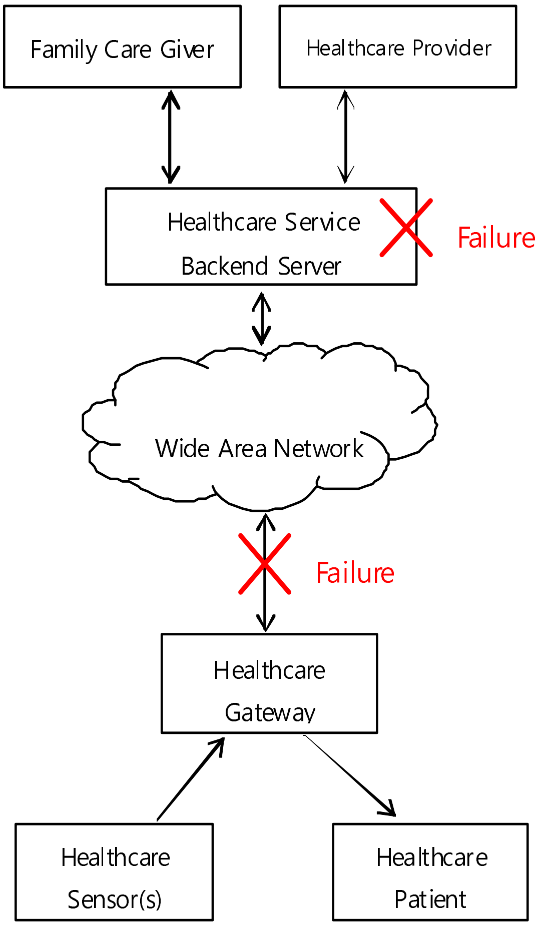

Figure 7.5: Example of failures in components of the M2M System for healthcare service

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.

7.1.9 High Level Illustration

Figure 7.6 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.

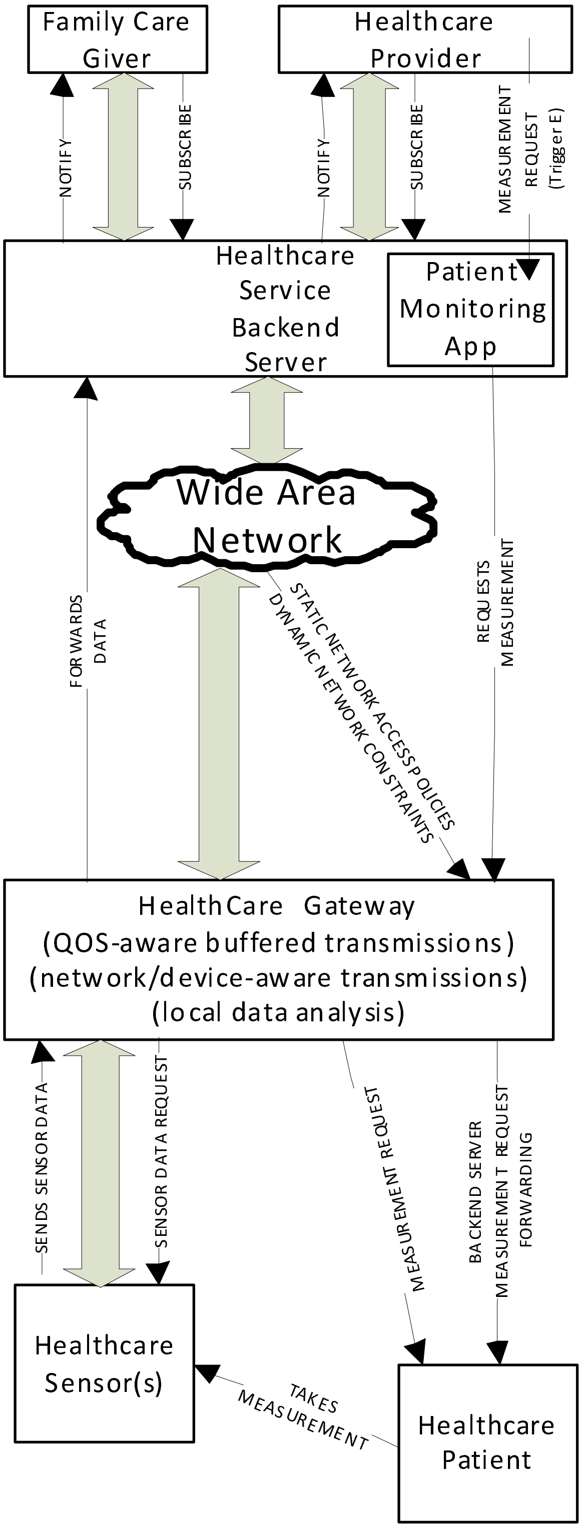

Figure 7.6: Healthcare Gateway High Level Illustration

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 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:

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.

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 Use Case on 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

- KDDI (TTC).

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.

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 ETSI TR 102 732 [i.4]. (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 center to do exercise and checks the effect by utilizing equipment which is owned by fitness center 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.

1) 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).

2) 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, etc.).

3) The mobile device is provided with the appropriate application software from the Management Server and is appropriately configured by the Management Server.

4) 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 center).

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, etc.).

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.

7.2.9 High Level Illustration

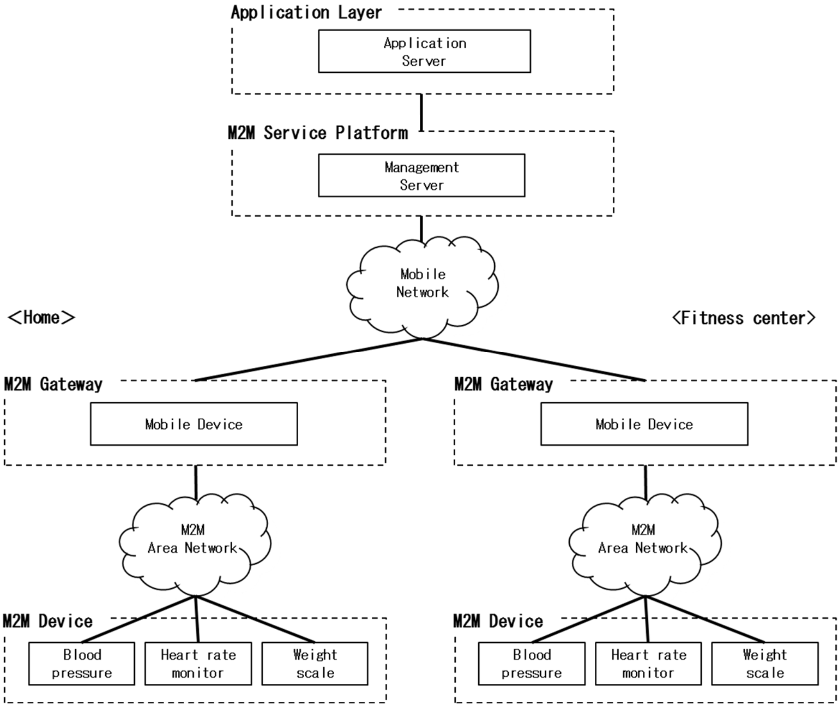

Figure 7.7: Wellness Service High Level Illustration

7.2.10 Potential Requirements

- M2M Gateway SHALL be able to detect device that can be newly installed (paired with the M2M Gateway).
- 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.
- 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 ETSI TR 102 732 [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 analyzed 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 has to 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).

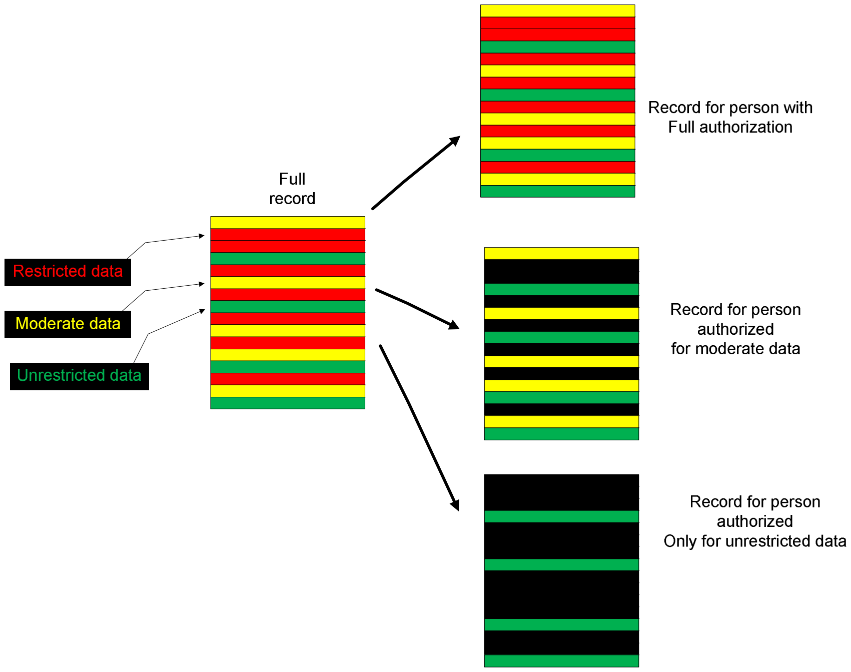
Full record
Restricted data
Moderate data
Unrestricted data
Record for person with Full authorization
Record for person authorized for moderate data
Record for person authorized Only for unrestricted data

Figure 7.8: An illustration of a process with 2 levels of redaction
Black color indicates a data field that is masked from an unauthorized user

Care has to be taken to ensure that only authorized users have access to data. Therefore, the system has to 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 has to 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.

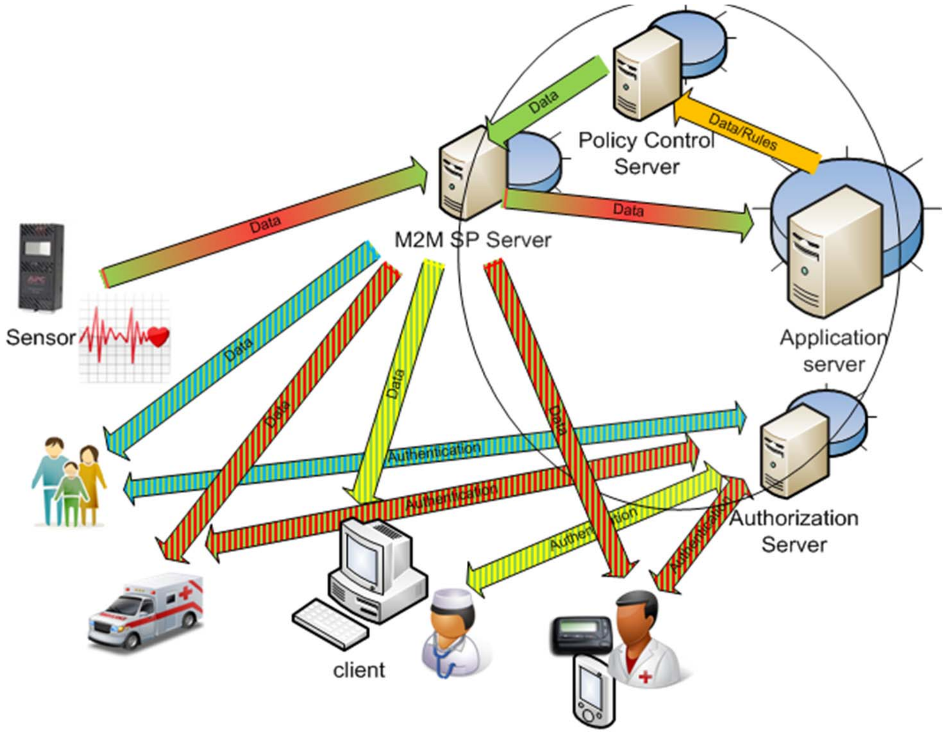

Figure 7.9: An e-Health application service capable of monitoring remote sensor devices and producing notifications and data to health care personnel based on their authorization level

7.3.2 Source

- Motorola Mobility, ETSI member.

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, has to 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.
- 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 has to encrypt the sensor data before passing the data to the service layer. Since the data has to be kept private from service layer function, the encryption keys and engine used by the application client has to 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 has to 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, analyzes 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 has to 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.

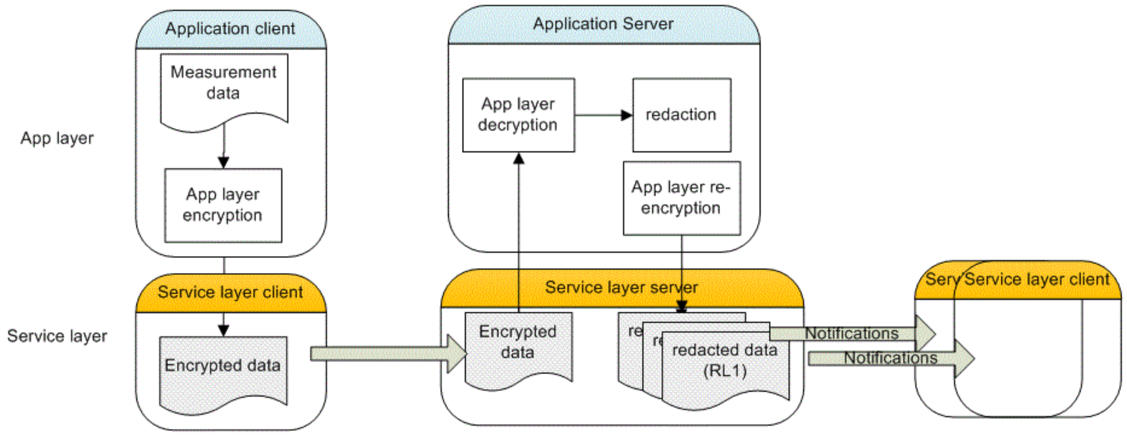

Figure 7.10: Dealing with Redaction in an M2M system separating Application layer and Service layer the Service layer functions are provided by M2M service provider, while application layer functions are provided by application provider

7.3.7 Alternative flow

7.3.7.1 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 has to first refer the user to the authorization server to assert the user's authorization level (AL) before serving the user with a response.

7.3.7.2 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 has to make sure that the user has the proper AL to issue the command.

7.3.7.3 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 has to 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 has to also be a policy engine that categorize the data based on its Criticality Level (CL).

7.3.8 Post-conditions

7.3.8.1 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.

7.3.8.2 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 has to 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 have to 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 has to 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 has to be able to accommodate response/ notifications to the users based on their level of authorization.

9) The M2M service layer has to accommodate tagging of opaque application data for various purposes, such as urgency levels, authorization/redaction levels, etc.

10) There has to 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 has to 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 have to create notifications for first-level responders.

12) Any software client, especially those performing security functions (e.g. authentication clients) has to 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.

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 center**
  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

- Cisco Systems - from public document research: "Street Light Control" use case.

8.1.3 Actors

1) Street light automation application service provider, has the aim is to adjust street light luminosity.

2) Street light devices have the aim is to sense, report, execute local and remote policies, illuminate street.

3) Traffic light application service provider, has the aim is to enhance their emergency vehicle service using street lighting.

4) Emergency services application services provider, have the aim is to brightly illuminate police action areas and brightly illuminate planned path of emergency vehicles.

5) Road maintenance application service provider, has the aim is to obtain extra street light signaling near closed roads.

6) 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).

1) "Street lights" message the Street light system that street light sensors have detected light level movement below/above threshold.

2) Street light system informs the "street light operation centre" with the street light sensor information.

3) "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.

4) Street light system messages the "street lights" with a street light control message to increase/decrease luminosity according to "street light operation centre" policy.

5) 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.

6) 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: 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).

1) "Street lights" message the Street light system that street light power sensors have detected input voltage level movement above/below threshold.

2) Street light system informs the "street light operation centre" with the street light sensor information.

3) "Street light operation centre" messages the Street light system with an alert message to "electricity service provider" according to "street light operation centre" policy.

4) Street light system informs "electricity service provider" of alert message.

5) "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.

6) 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.

7) 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).

1) "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.

2) Street light system informs the "street light operation centre" with the street light sensor information.

3) "Street light operation centre" messages the Street light system with a control message to increase/decrease luminosity according to "street light operation centre" policy.

4) Street light system messages the "street lights" with a street light control message to increase/decrease luminosity according to "street light operation centre" policy.

5) 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.

6) 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).

1) The "street light operation centre" detects through analytics that an SLA regarding minimum street light intensity is in danger of not being met.

2) "Street light operation centre" messages the Street light system with a control message to increase luminosity according to "street light operation centre" policy.

3) 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).

1) 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.

2) "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.

3) 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).

1) "Street lights" message the Street light system that street light power sensors have detected civilian or emergency vehicle entering street section.

2) Street light system informs the "street light operation centre" with the street light sensor information.

3) "Street light operation centre" messages the Street light system with a control message to increase/decrease luminosity according to "street light operation centre" policy.

4) 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).

  1) "Traffic light service provider" messages the Street light system that emergency vehicle approaching street junction from certain direction.

  2) Street light system informs the "street light operation centre" with the street junction information.

  3) "Street light operation centre" messages the Street light system with a control message to increase luminosity according to "street light operation centre" policy.

  4) 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).

  1) "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.

  2) Street light system informs the "street light operation centre" with the street junction information.

  3) "Street light operation centre" messages the Street light system with a control message to increase luminosity according to "street light operation centre" policy.

  4) 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).

    1) "Road Maintenance service provider" messages the Street light system that (9a) a road is closed, or (9b) a route diversion is activated.

    2) Street light system informs the "street light operation centre" with the road maintenance information.

    3) "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.

    4) 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).

        1) "Electricity service provider" messages the Street light system that (9a) that an overload condition exists across some area.

        2) Street light system informs the "street light operation centre" with the overload condition information.

        3) "Street light operation centre" messages the Street light system with a control message to decrease luminosity according to "street light operation centre" policy.

        4) 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

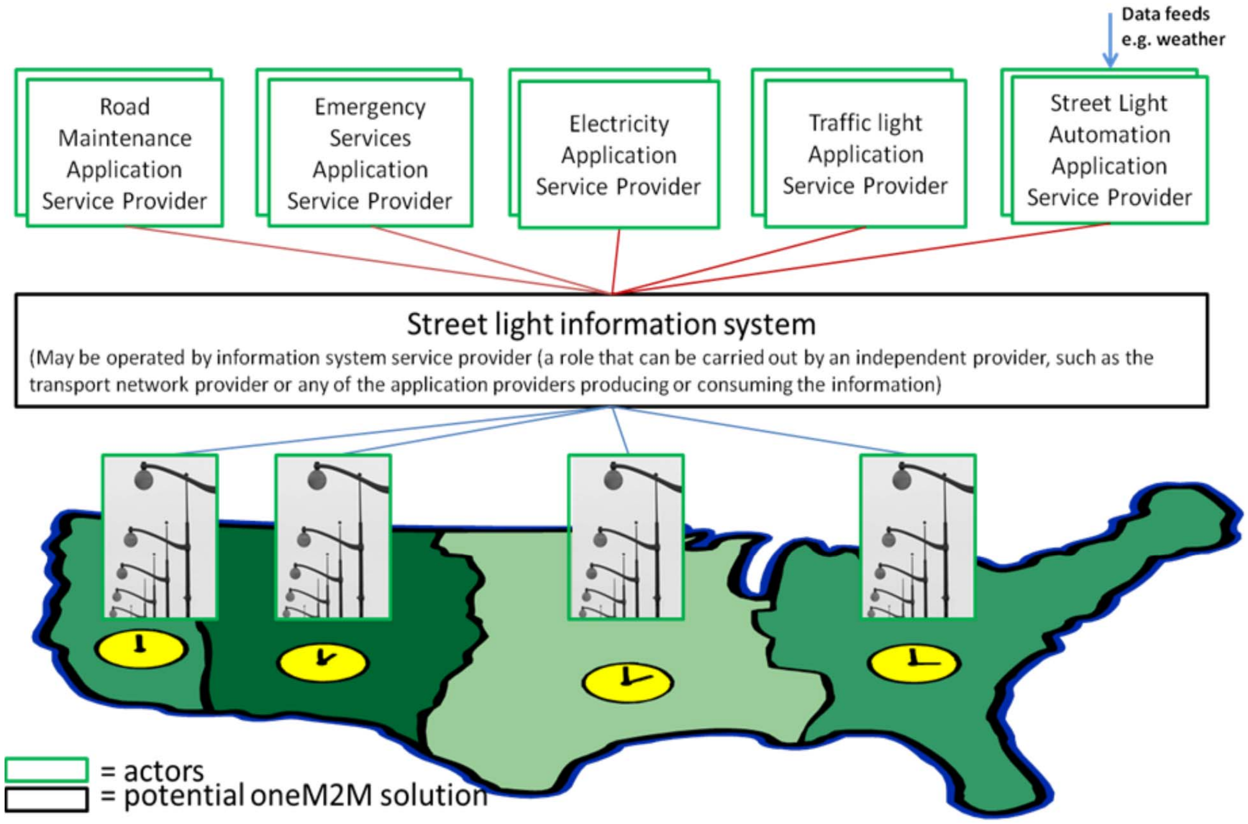
Data feeds
e.g. weather
Road Maintenance Application Service Provider
Emergency Services Application Service Provider
Electricity Application Service Provider
Traffic light Application Service Provider
Street Light Automation Application Service Provider
Street light information system
(May be operated 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 8.1: 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

1) Attack vectors and example impacts:

   - By sending false reports of sensors to applications.

   - Energy provider overdriving voltage.

2) By sending false control commands to devices:

   - Blackout to obscure crime.

3) By blocking valid messages:

   - Energy wastage.

8.2 Use Case on 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, etc.

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, etc.) 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

- NEC.

8.2.3 Actors

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

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, etc.) 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

- 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.
- 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.
- 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.
- 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.
- 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

8.3.1 Description

As seen clearly, automation already penetrates all aspects of life even in our urban life. The goal of this use case is to describe several automation services which are occurred in different urban space in different life style, bicycle/car sharing services.

Brief Features of Services

- Car Sharing Service:
  - Car Sharing is to offer a new service model for automobile transportation. Simply, Car Sharing is a self-service, on-demand alternative to car ownership; a service that is offered to urban residents (B2C) and businesses (B2B).
  - This service is mainly designed around a particular user profile - first of all, people who live in cities but do not drive a car every day and secondly tourists who live in cities but do not own a car. Thus, people who need a car at short notice but take an alternative to car ownership.
  - The brief procedure of this service is:
    1) joining the membership;
    2) unlocking the car door;
    3) driving away;
    4) parking to any reserved spot provided by the service provider and/or public; and
    5) paying as you drive (including gas, insurance, etc.).

- Bicycle Sharing Service:
    - Bicycle sharing service is also a new service in which bicycle are made available for shared use to individuals who do not own a bicycle. Generally, bicycle sharing service is run by government agencies.
    - The procedure of this service is similar to the car sharing service, but the different type of services such as healthcare service can be combined.

8.3.2 Source

- LG Electronics.

8.3.3 Actors

- **User**
    - A user who takes the ownership of the shared things which are car and bicycle.
- **Sensors (or Sensor Devices)**
    - Sensor Devices can be various based on its usage, and do not have any direct communication interfaces to the M2M Service Platform.
    - For Car Sharing Service - Door Control Sensor, Tire Pressure Sensor, Fuel Indication Sensor, GPS.
    - For Bicycle Sharing Service - Lock Control Sensor, Accelerometer, Tire Pressure Sensor, Heart-rate Sensor.
- **Smartphone**
    - A device which is an intermediate entity and is available to connect from sensors to a M2M Service Platform. The basic role is similar to the general M2M gateway, but it has some sensors and some applications (navigation) itself used by services.
- **M2M Service Platform**
    - In charge of providing common functionalities for the M2M services. It is mainly in charge of collecting the status and configuration information of sensors and controlling them via the smartphone and/or M2M gateway.
- **M2M Service Providers**
    - Companies which provide its own M2M services for the user through the M2M Service Platform. The M2M Service Providers can be various according to the types of services.
    - The providers include Car Sharing Service Provider, Insurance Company, Gas Station, Bicycle Sharing Service Provider, and Healthcare Service Provider.

8.3.4 Pre-conditions

See sub-case flows.

8.3.5 Triggers

See sub-case flows.

8.3.6 Normal Flow

1. **Sub use case 1 - Car Sharing Case**
    - **Trigger:**
        - ▪ A user wants to take an ownership of the car.

- **Pre-conditions:**
  - The user preliminary joins a membership of the Car Sharing Service.
  - Sensors built in the car are required to periodically (normal) and non-periodically (urgent) send sensor data to the M2M Service Platform based on the trigger defined by the M2M Service Providers.
  - The M2M Service Platform collects and manages data and configurations related to the services. Generally, each service has its own data and configuration set, simply called resources.
  - The M2M Service Providers in the service domain have a service agreement each other for unified services.
  - The Smartphone has a navigation and car sharing application.
- **Detailed Flow Descriptions:**

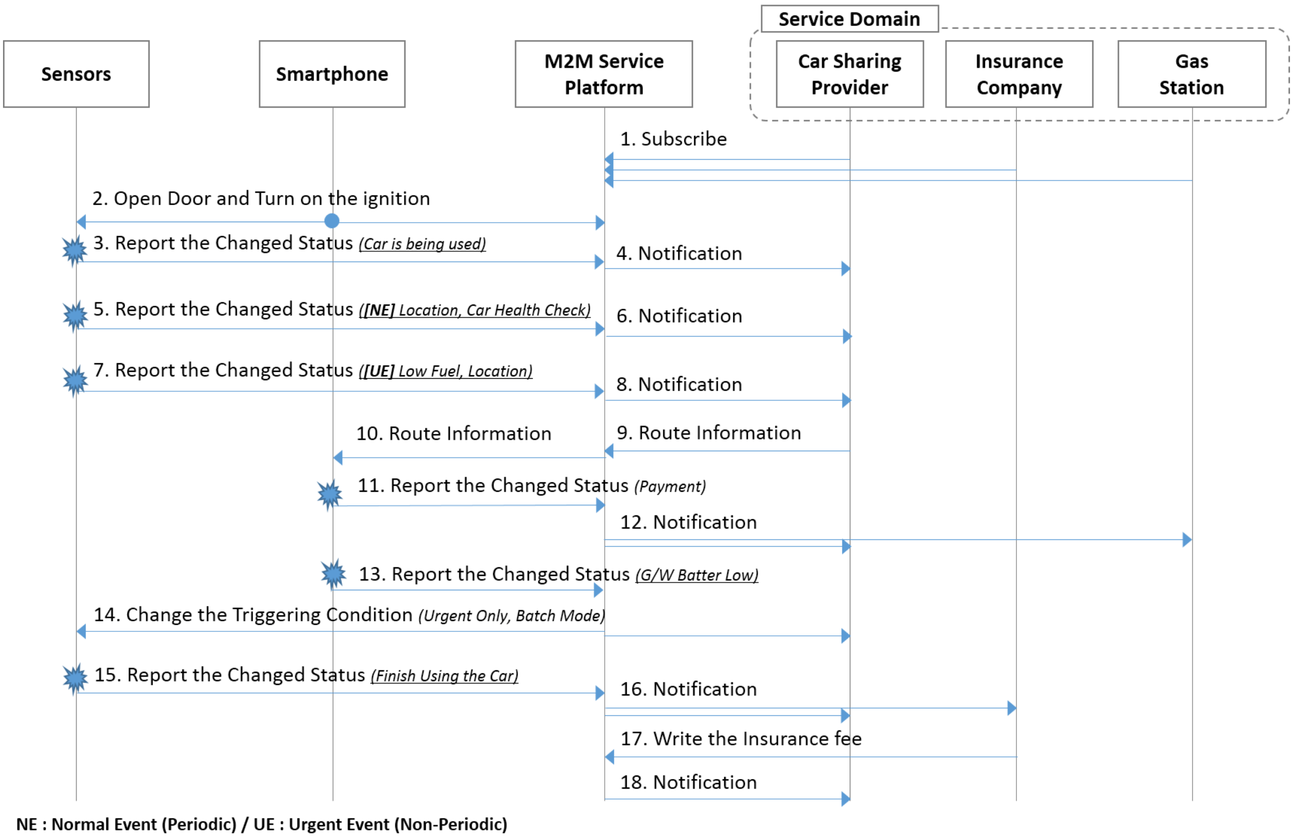
Service Domain
Sensors
Smartphone
M2M Service Platform
Car Sharing Provider
Insurance Company
Gas Station
1. Subscribe
2. Open Door and Turn on the ignition
3. Report the Changed Status (Car is being used)
4. Notification
5. Report the Changed Status ([NE] Location, Car Health Check)
6. Notification
7. Report the Changed Status ([UE] Low Fuel, Location)
8. Notification
10. Route Information
9. Route Information
11. Report the Changed Status (Payment)
12. Notification
13. Report the Changed Status (G/W Batter Low)
14. Change the Triggering Condition (Urgent Only, Batch Mode)
15. Report the Changed Status (Finish Using the Car)
16. Notification
17. Write the Insurance fee
18. Notification
NE : Normal Event (Periodic) / UE : Urgent Event (Non-Periodic)

Figure 8.2: Car Sharing Normal Flow

1) The Applications of each Service Provider in the service domain register and subscribe to changes of resources (or information) about the Car Sharing Service in the M2M Service Platform.

2) Since each resource in the M2M Service Platform is owned by the Car Sharing Provider, Insurance Company and Gas Station, if an application needs to access another resource, it shall request proper access right of the resources and grant that request if appropriate and based on the service agreement.

3) As the user finds a shared car, opens the car door and turns on the ignition using interfaces of the Smartphone such as Bluetooth and NFC, if the user is authorized.

4) The Sensors report the changed status to the M2M Service Platform via the Smartphone as a gateway when the specific condition is triggered. (Car is just being used.)

5) The M2M Service Platform notifies the Car Sharing Service Provider of the changed status.

NOTE 1: The Car Sharing Service Provider can update the situation that the car is being used on its website.

6) (Normal Reporting Case for managing the Service) The Sensors report the changed status to the M2M Service Platform via the Smartphone when the specific condition is triggered. (Periodic location reporting and car health check for maintenance reasons.)

7) The M2M Service Platform notifies the Car Sharing Service Provider of the changed status.

NOTE 2: Agreement on privacy policy of location is preliminary confirmed.

8) (Urgent Reporting Case for handling any emergency) The Sensors report the changed status to the M2M Service Platform via the smartphone as a gateway when the specific condition is triggered. (The fuel is low.)

9) The M2M Service Platform immediately notifies the Car Sharing Service Provider of the changed status.

10) The Car Sharing Service Provider finds out the nearest Gas Station according to the received location information and a service agreement between the Car Sharing Service Provider and the Gas Station, and the Provider sends the route information to M2M Service Platform.

11) The M2M Service Platform notifies the Smartphone of the route information.

12) After filling the fuel, the user virtually pays the fuel fee by using the Smartphone's NFC tag. The payment information is reported to the M2M Service Platform.

13) The M2M Service Platform notifies the Car Sharing Provider and the Gas Station of the payment information.

NOTE 3: This procedure is for the Car Sharing Provider to pay Gas Station the fuel fee instead of the user.

14) Afterwards, due to the low battery of the Smartphone (less than 30% remain), the Smartphone reports the changed status to the M2M Service Platform.

15) The M2M Service Platform automatically changes the subscription and reporting attributes of the Sensors and the Car Sharing Service Provider.

EXAMPLE: If the Platform changes the subscription attributes to "only emergency case", only emergency subscription case will be notified. The others cannot be notified, but at the end of service, batch-mode.

16) As the user arrives at the destination, and turns off the ignition, the sensors report the accumulated information, normal event subscription information, to the M2M Service Platform via smartphone.

17) The M2M Service Platform notifies the Car Sharing Provides and Insurance Company of the usage of the shared car.

18) The Insurance Company stores the insurance fee by writing onto the Car Sharing Service Provider's resource in the M2M Service Platform, in this case the Insurance Company preliminary acquires proper access right to write.

19) The M2M Service Platform notifies the Car Sharing Provides of the insurance fee.

- **Post-conditions:**
  - The User will pay as him/her drive according to the recorded data.
  - The Car Sharing Service Provider can update the position and status of the car on its website using the recorded data. Thus, next users can make use of the Car Sharing Service.

2. Sub Use Case 2 - Bicycle Sharing Service

- **Trigger:**
  - A user wants to take an ownership of the bicycle.
- **Pre-conditions:**
  - The user preliminary joins a membership of the Bicycle Sharing Service.

- The sensors built in the car and in the smartphone are required to periodically (normal) and non-periodically (urgent) send sensor data to the M2M Service Platform based on the trigger defined by the Service Provider.

- The M2M Service Platform collects and manages data and configurations related to the services. Generally, each service has its own data and configuration set, simply called resources.

- The Smartphone has a navigation and bicycle sharing application.

- The M2M Service Providers in the service domain have a service agreement each other for unified services.

- **Detailed Flow Descriptions:**

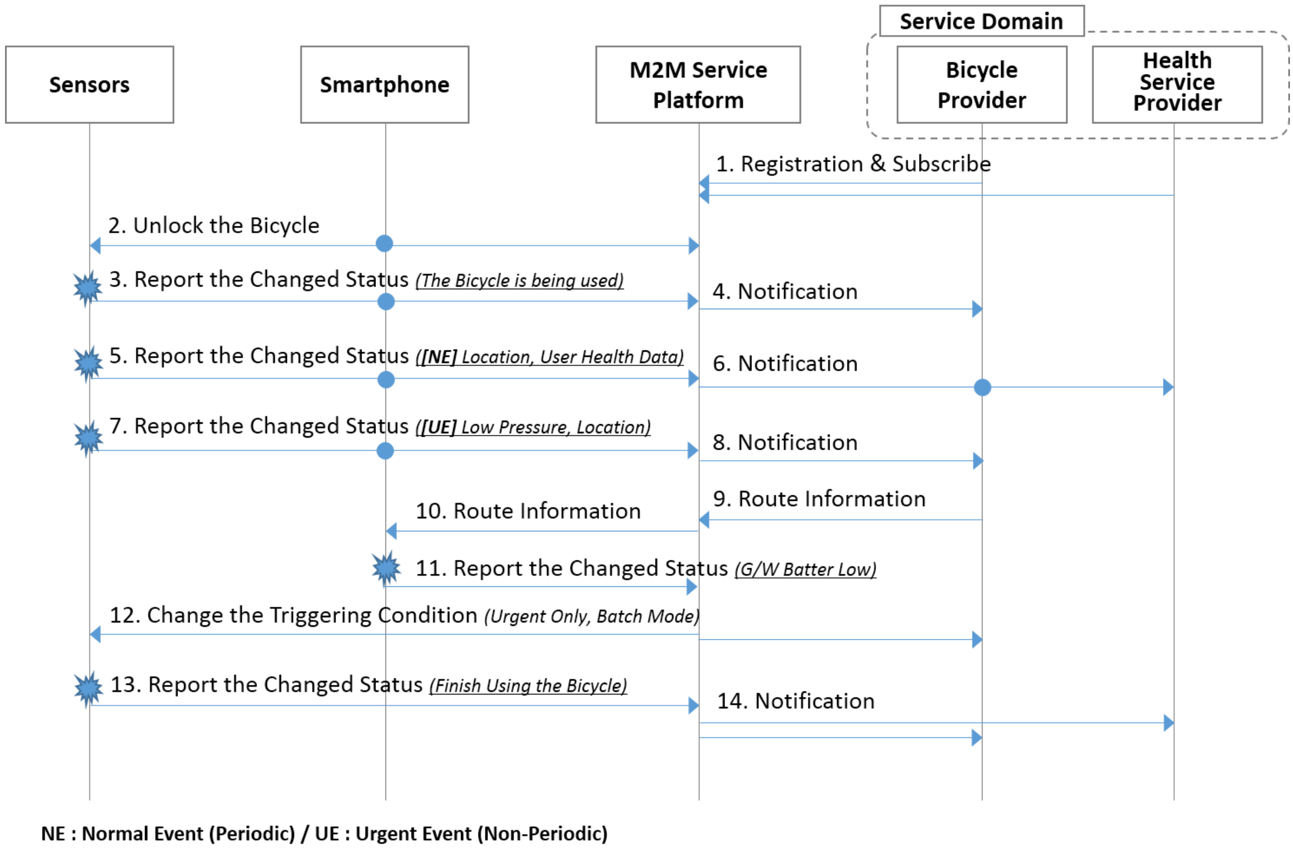
Service Domain
Sensors
Smartphone
M2M Service Platform
Bicycle Provider
Health Service Provider
1. Registration & Subscribe
2. Unlock the Bicycle
3. Report the Changed Status (The Bicycle is being used)
4. Notification
5. Report the Changed Status ([NE] Location, User Health Data)
6. Notification
7. Report the Changed Status ([UE] Low Pressure, Location)
8. Notification
9. Route Information
10. Route Information
11. Report the Changed Status (G/W Batter Low)
12. Change the Triggering Condition (Urgent Only, Batch Mode)
13. Report the Changed Status (Finish Using the Bicycle)
14. Notification
NE : Normal Event (Periodic) / UE : Urgent Event (Non-Periodic)

Figure 8.3: Bicycle Sharing Normal Flow

1) The Applications in the service domain register the service and subscribe to changes of information about the Bicycle Sharing Service.

2) Since each resource in the M2M Service Platform is owned by the Bicycle Sharing Service Provider and Health Service Provider, if an Application needs to access another resource, it shall request proper access right of the resources and grant that request if appropriate and based on the service agreement.

3) To unlock the bicycle, the user tags the locker of the bicycle through the NFC interface.

4) The Sensors report the changed status to the M2M Service Platform via the smartphone as a gateway when the specific condition is triggered (for example, the bicycle is being used).

5) The M2M Service Platform notifies the Bike Sharing Service Provider of the changed status.

NOTE 4: The Bicycle Sharing Service Provider can record the situation on its web-site that the car is being used.

6) (Normal Reporting Case for managing the Service) The heart-rate of the user is continuously collected by the heart-rate sensor on the handlebar, and the health-related information such as heart-rate, location, time is reported periodically to the Service Operator.

7) The M2M Service Platform notifies the Bicycle Sharing Service Provider and the Health Service Provider of the health Service information.

8) (Urgent Reporting Case for handling any emergency) While riding the bicycle, the tire pressure sensor detects the low pressure of the front tire, the information is immediately sent to the M2M Service Platform via the Smartphone with location information.

9) The M2M Service Platform notifies the Bicycle Sharing Service Provider of the changed status.

10) The Bicycle Sharing Service Provider finds out the nearest bike repair shop according to the received location information, and the Provider sends the route information to M2M Service Platform.

11) The M2M Service Platform forwards the route information to the Smartphone which has a navigation application.

12) Afterwards, due to the low battery of the Smartphone (less than 30 % remain), The Smartphone reports the changed status to the Service Operator. (Low battery indication.)

13) The M2M Service Platform automatically changes the subscription attributes of sensors and the Bicycle Service Provider such as delay tolerance to reduce battery-consumption.

EXAMPLE: If the Platform changes the subscription attributes to "only emergency case", only emergency subscription case will be notified. The others cannot be notified, but at the end of service, batch-mode.

14) As the user arrives at the destination and parks to the reserved spot, the Sensor reports the accumulated information and normal event subscription information to the M2M Service Platform via the Smartphone.

15) The M2M Service Platform notifies Bicycle Sharing Service Provide and Healthcare Service Provider of the usage of the shared bicycle.

- **Post-conditions:**
  - The User may pay as him/her drive according to the recorded data (not for the public service case).
  - The Bicycle Sharing Service Provider can update the position and status of the car on its website using the recorded data. Thus, next users can make use of the Bicycle Sharing Service.

8.3.7 Alternative flow

None.

8.3.8 Post-conditions

See sub-case flows.

8.3.9 High Level Illustration

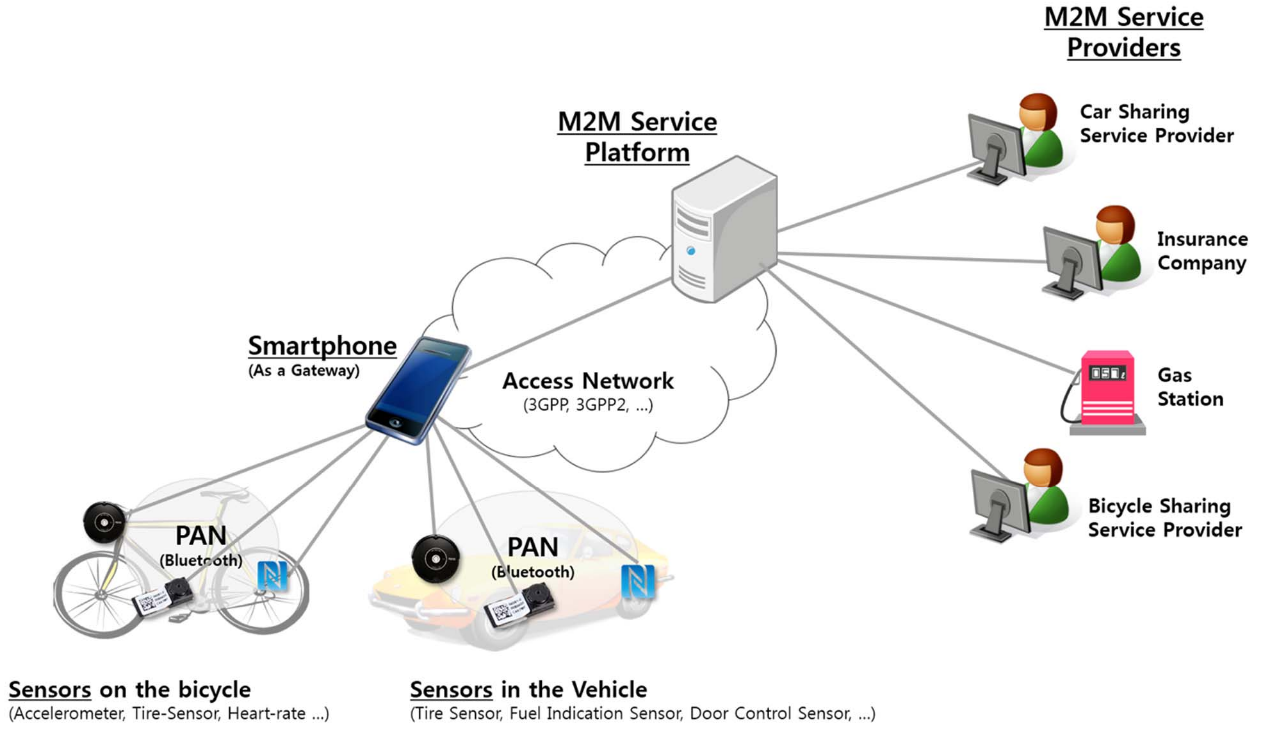

Figure 8.4: Car/Bicycle Sharing High Level Illustration

8.3.10 Potential Requirements

1) The M2M System shall support mobile/portable M2M Gateway and/or Device.

2) The M2M System shall support to distinguish the event levels for reporting and handle it differentially.

3) Note: For example, the event levels may be divided into normal and urgent event.

4) Based on the condition of the M2M Gateway and/or Device, the M2M System shall change the reporting (or subscription) mechanisms and/or configurations related to a service.

5) The M2M System shall support to process access right requests of a resource and grant the requests if the requests.

8.4 Smart Parking

8.4.1 Description

Smart parking helps one of the biggest problems on driving in urban areas; finding empty parking spaces and controlling illegal parking. Those parking spaces are wide spread and owned by different providers so that it is not easy to access at one place/time.

With smart parking service, drivers can easily find available parking spaces, pay parking fees and even can make reservations. Making parking reservations would be available for limited people such as VIPs or the disabled, since ordinary parking service needs to satisfy first-come-first-served rule.

In this use case, law enforcement authority is also included as an actor. This implies M2M technologies aims rightness/safety as well as convenience.

8.4.2 Source

- LG Electronics.

8.4.3 Actors

- M2M Service Platform:
  - This is a platform that interacts with M2M Gateways/Devices and M2M Application Service Providers.
- Smartphone:
  - This is a M2M Device acts as a car navigator and a wallet to pay parking fee by connecting parking meters.
- On-street Parking Meter:
  - This is a M2M Device installed near parking slots to charge drivers parking fees.
- In-building Parking Sensor:
  - This is a M2M Device with a small camera that can recognize a plate on cars, and is installed near disabled-only parking spaces.
- Parking Provider:
  - This is a M2M Application Service Provider who owns parking lots, in this use case there are two parking providers; in the mall and on street.
- Billing Provider:
  - This is a M2M Application Service Provider (e.g. credit card company) who provides billing service to M2M Users such as parking fee. When it issues a bill, coupons from M2M Application Service Providers are used as tokens for compensation schemes. They also can charge fines issued by police center on their bills.
- Police Center:
  - This is a law enforcement authority, one of M2M Application Service Providers, who charges fine to whom break laws.
- User:
  - This is a M2M service user who drives a car. In the second sub case, dedicated parking space, there are two users. One originally makes a reservation who is handicapped, and the other who illegally parks a car on disabled-only parking area.

8.4.4 Pre-conditions

See sub-case below.

8.4.5 Triggers

See sub-case below.

8.4.6 Normal Flow

1. **Finding Space, Parking Car & Paying Bill**
   - **Pre-condition**
     - ▪ User sets a destination as a shopping mall using the smartphone navigator, also checks availability of parking space in the building before or while driving.
   - **Triggers**
     - ▪ The car approaches near the destination.

- **Normal flow**

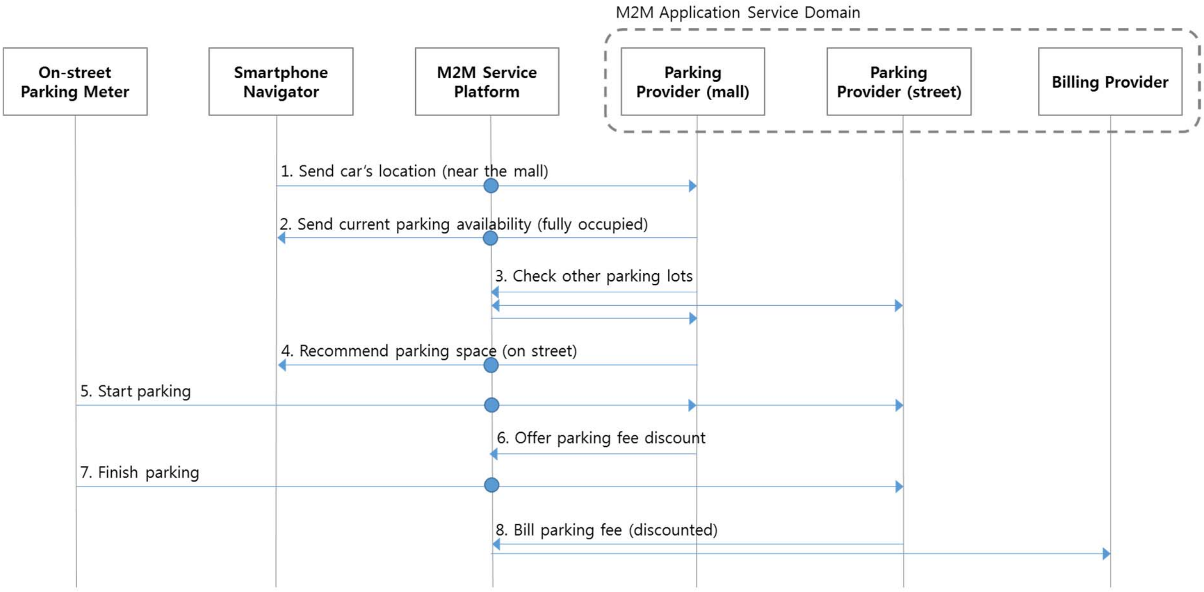
M2M Application Service Domain
On-street Parking Meter
Smartphone Navigator
M2M Service Platform
Parking Provider (mall)
Parking Provider (street)
Billing Provider
1. Send car's location (near the mall)
2. Send current parking availability (fully occupied)
3. Check other parking lots
4. Recommend parking space (on street)
5. Start parking
6. Offer parking fee discount
7. Finish parking
8. Bill parking fee (discounted)

Figure 8.5: Normal Flow - Finding Space, Parking Car & Paying Bill

1) Since the user set the mall as the destination before, when the user is near the mall, the navigator sends the location to the mall parking provider automatically.

2) The mall parking provider informs the navigator that there's no empty parking space now.

3) Based on the car's location, which is near the mall, the mall parking provider inquires availability of other parking spaces through M2M service platform.

4) There are empty spaces on street, so the mall parking provider recommends that parking space.

5) The user touches the smartphone on a parking meter to start parking. Then the street parking provider is noticed, and also the mall parking provider is.

6) The mall parking provider offers discount coupon for parking outside as a compensation.

7) The user touches the smartphone on the meter to finish parking.

8) The street parking provider bills parking fee. The bill with discount coupon is sent to billing provider through M2M service platform.

2. Dedicated Parking Space

- **Pre-condition**

  ▪ Before driving, the user (user A) makes a parking reservation for a slot in a shopping mall, which is especially for the disabled. It is normally assured because there will be fines for illegal parking on this dedicated parking space.

- **Triggers**

  ▪ None.

- **Normal Flow**

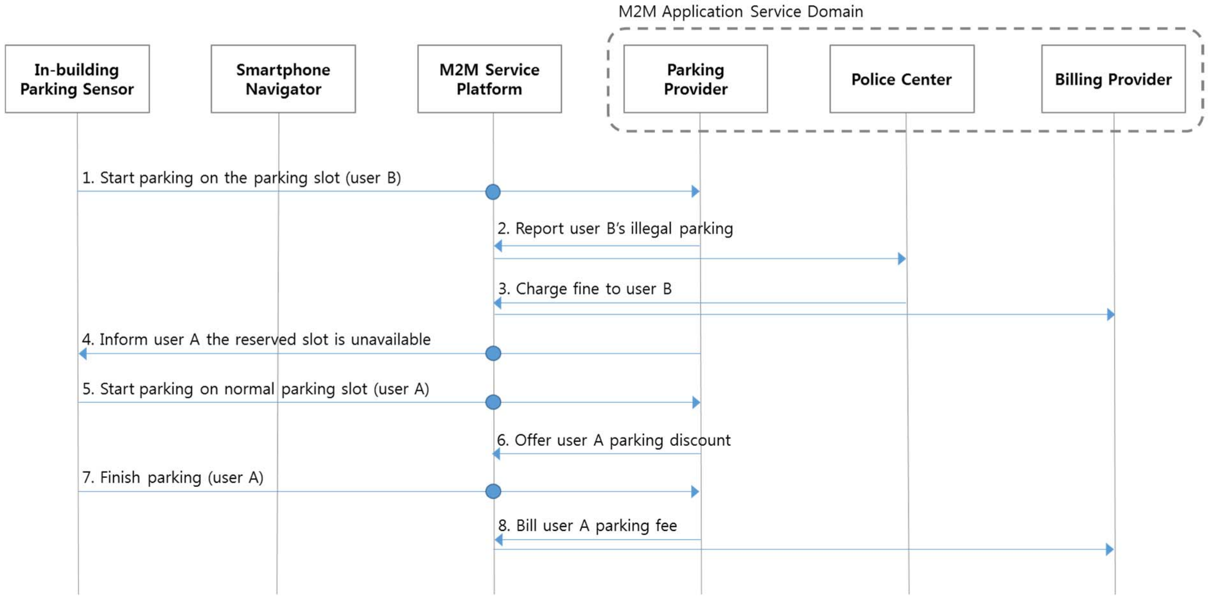
M2M Application Service Domain
In-building Parking Sensor
Smartphone Navigator
M2M Service Platform
Parking Provider
Police Center
Billing Provider
1. Start parking on the parking slot (user B)
2. Report user B's illegal parking
3. Charge fine to user B
4. Inform user A the reserved slot is unavailable
5. Start parking on normal parking slot (user A)
6. Offer user A parking discount
7. Finish parking (user A)
8. Bill user A parking fee

Figure 8.6: Normal Flow - Finding Dedicated Parking Space

1) The other user (user B) parks a car on the parking lot, which is already reserved by user A before.

2) User B's illegal parking on the disabled-only parking area is reported to police center.

3) Police center charges fine on user B.

4) User A approaches the mall and is noticed that reserved parking space is taken and only choice now is normal parking slots.

5) User A parks on a normal parking slot instead of the reserved one.

6) The parking provider offers parking discount coupon to the user A as a compensation.

7) After shopping, user A leaves the building and finish parking.

8) The parking provider bills parking fee for user A, adopting the parking coupon.

8.4.7 Alternative flow

Alternative Flow 1 - Dedicated Parking Space

- Pre-condition
  - Before driving, the user (user A) makes a parking reservation for a slot in a shopping mall, which is especially for the disabled. It is normally assured because there will be fines for illegal parking on this dedicated parking space.
- Triggers
  - None.

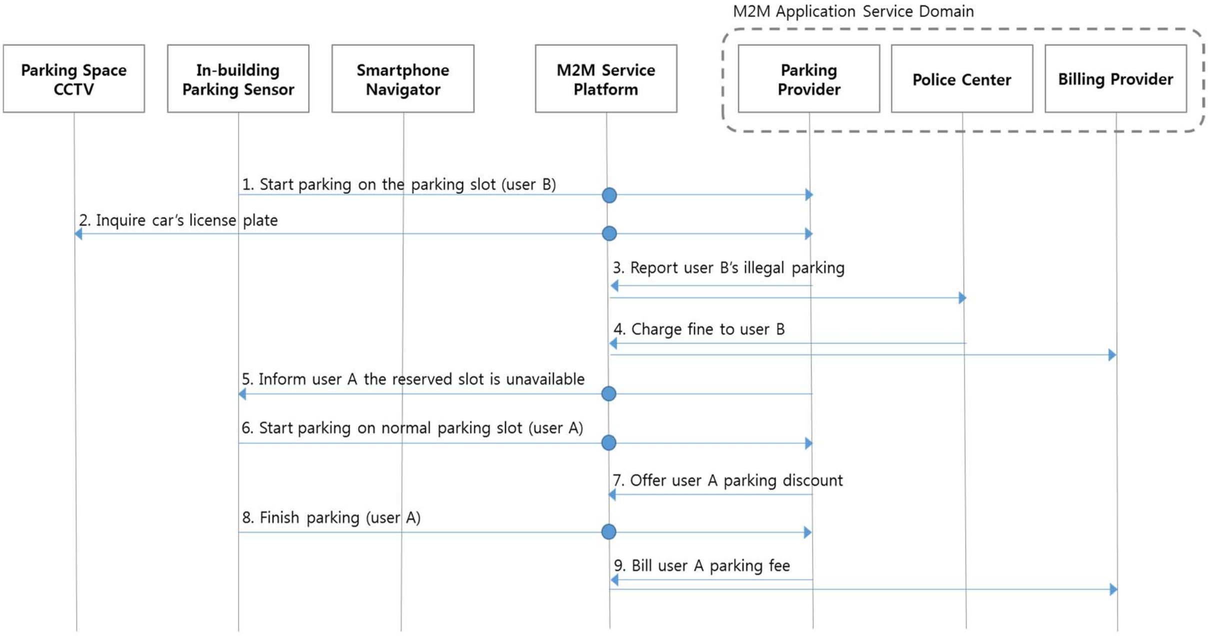
M2M Application Service Domain
Parking Space CCTV
In-building Parking Sensor
Smartphone Navigator
M2M Service Platform
Parking Provider
Police Center
Billing Provider
1. Start parking on the parking slot (user B)
2. Inquire car's license plate
3. Report user B's illegal parking
4. Charge fine to user B
5. Inform user A the reserved slot is unavailable
6. Start parking on normal parking slot (user A)
7. Offer user A parking discount
8. Finish parking (user A)
9. Bill user A parking fee

Figure 8.7: Alternate Flow 1 - Finding Dedicated Parking Space

1) The other user (user B) parks a car on the parking lot, which is already reserved by user A before.

2) The mall parking provider inquires plate number of the car to a CCTV near the parking space.

3) User B's illegal parking on the disabled-only parking area is reported to police center.

4) Police center charges fine on user B.

5) User A approaches the mall and is noticed that reserved parking space is taken and only choice now is normal parking slots.

6) User A parks on a normal parking slot instead of the reserved one.

7) The parking provider offers parking discount coupon to the user A as a compensation.

8) After shopping, user A leaves the building and finish parking.

9) The parking provider bills parking fee for user A, adopting the parking coupon.

8.4.8 Post-conditions

None.

8.4.9 High Level Illustration

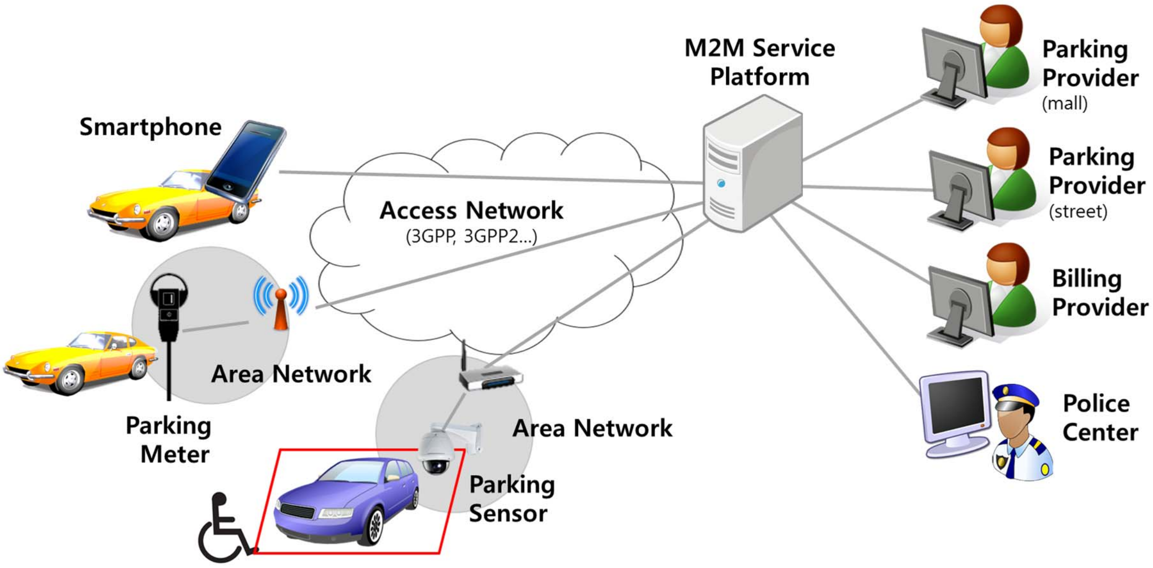

Figure 8.8: High Level Illustration of Smart Parking

8.4.10 Potential Requirements

1) The M2M System shall support mechanisms to correlate charging data/records from different M2M Application Service Providers.

2) The M2M System shall support triggering M2M Devices to report on-demand regarding collected data from other M2M Devices.

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 Equipments for public information.

8.5.2 Source

- Advanced Telecommunications Research Institute International (ARIB).
- Sumitomo Electric Industries Ltd. (TTC).
- Alcatel-Lucent (ETSI).

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. WiFi, 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 reliablesecure 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.

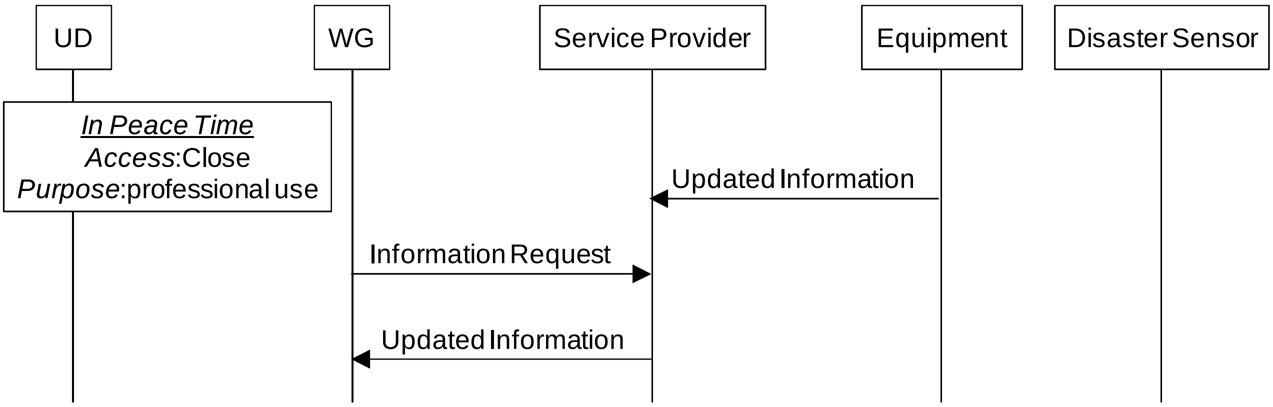

Figure 8.9: In Peace Time

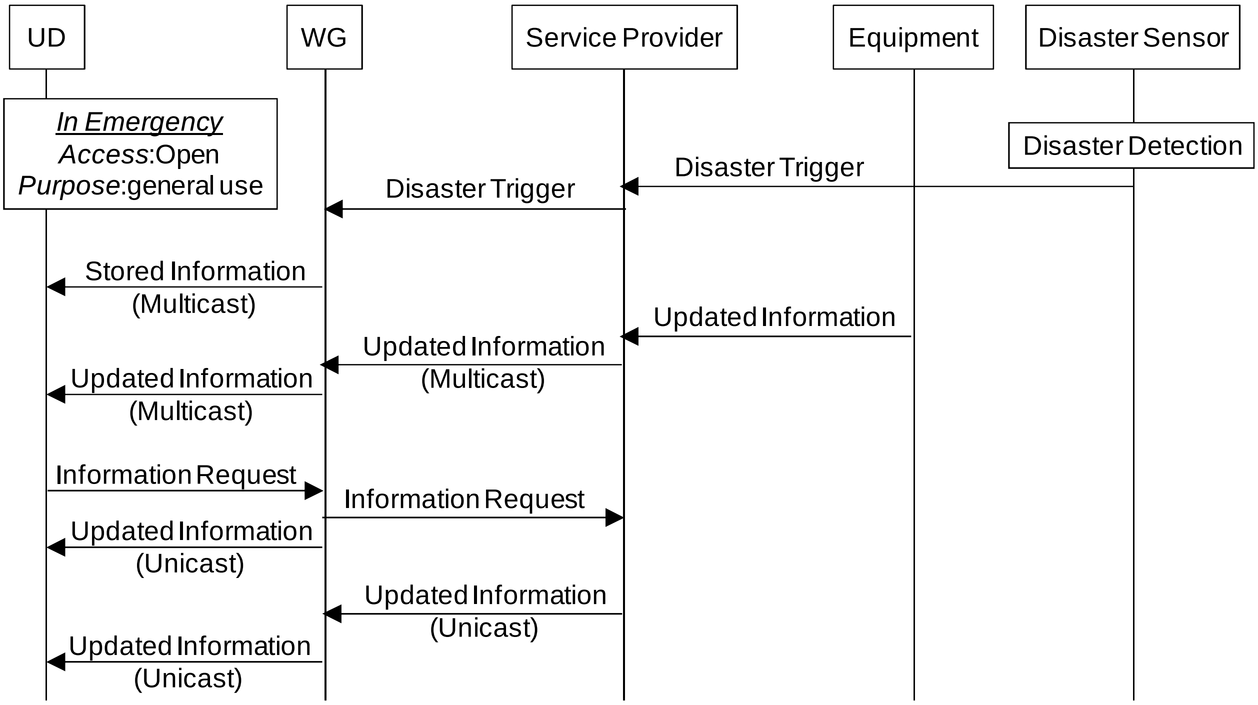

Figure 8.10: In emergency

1) WGs request the updated information from the Service Provider in peace time repeatedly and stores the information in their local DBs.

2) Disaster Sensors send messages to start the processing flow of the information delivery service to the Service Provider if they detect the disaster trigger.

3) 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.

4) 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

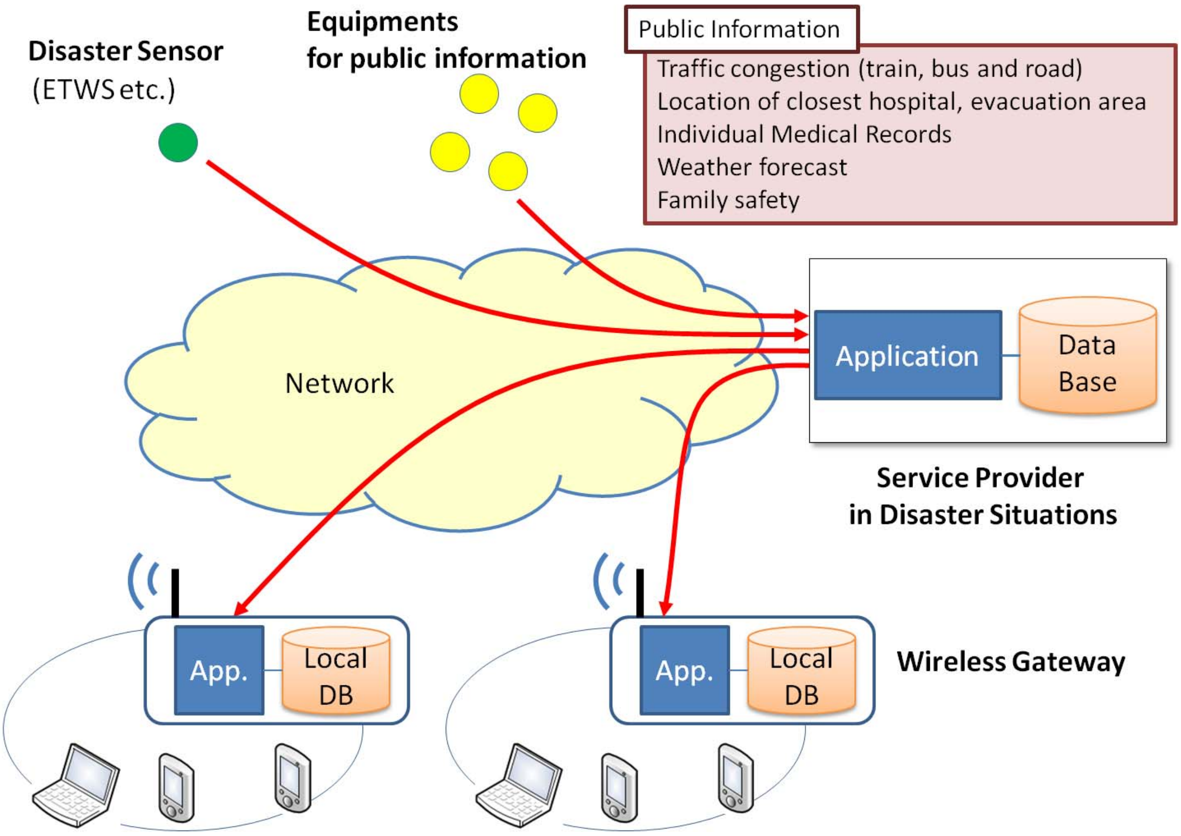

Figure 8.11: High Level System View

8.5.10 Potential Requirements

Table 8.1

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.
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.
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.

Requirement ID	Classification	Requirement Text
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.

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.

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.).

HGI-GD017-R3 [i.5] (Use Cases and Architecture for a Home Energy Management Service).

9.1.2 Source

- Fujitsu, from ETSI TR 102 935 [i.2].

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, etc.) 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

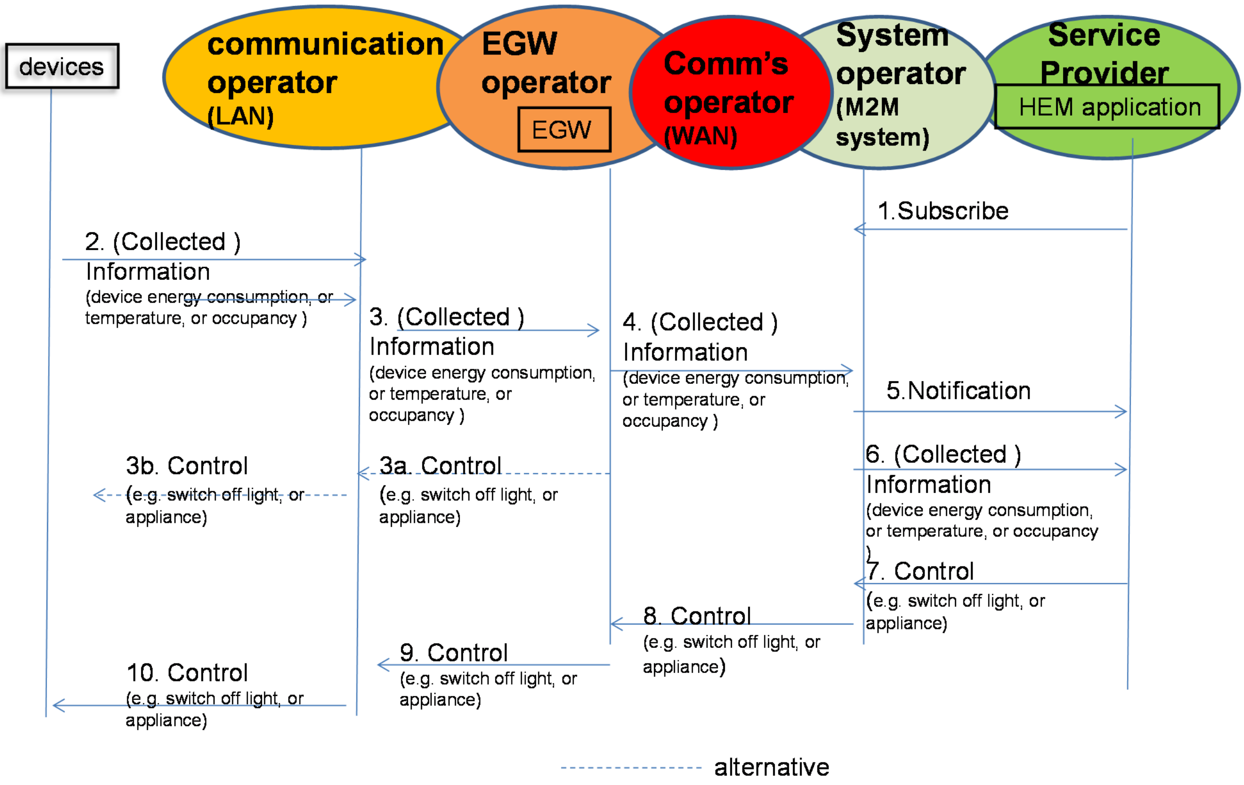
devices
communication operator (LAN)
EGW operator
EGW
Comm's operator (WAN)
System operator (M2M system)
Service Provider
HEM application
1.Subscribe
2. (Collected) Information (device energy consumption, or temperature, or occupancy)
3. (Collected) Information (device energy consumption, or temperature, or occupancy)
4. (Collected) Information (device energy consumption, or temperature, or occupancy)
5.Notification
3b. Control (e.g. switch off light, or appliance)
3a. Control (e.g. switch off light, or appliance)
6. (Collected) Information (device energy consumption, or temperature, or occupancy)
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 9.1: 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

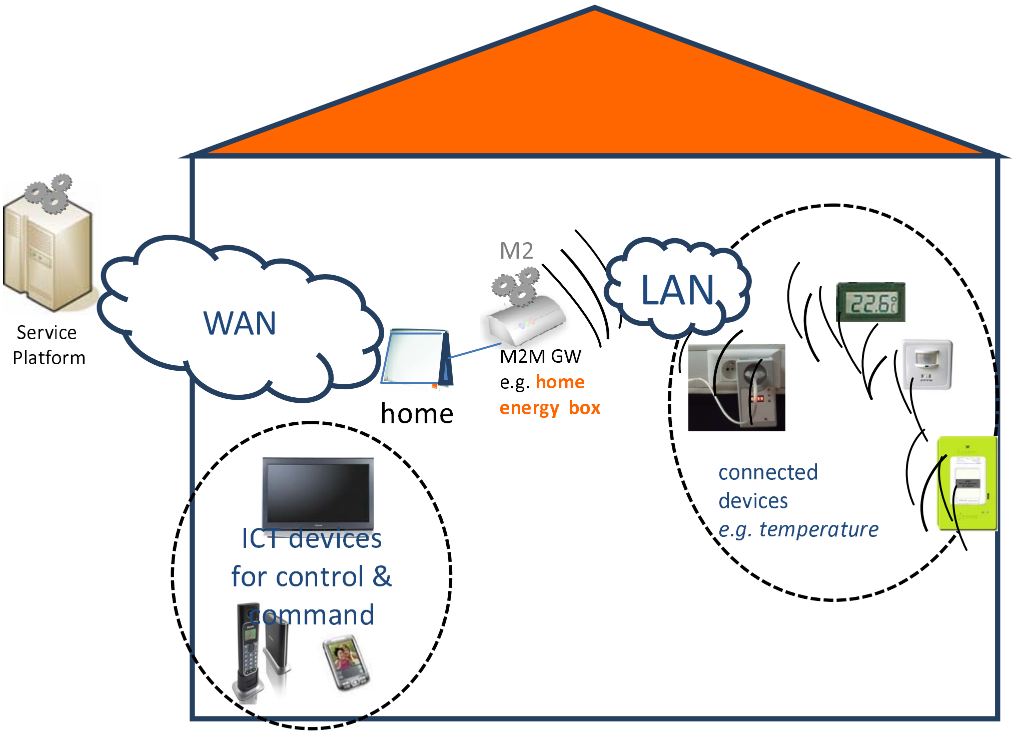

Figure 9.2: Home Energy Management System High Level Illustration

9.1.10 Potential Requirements

Similar to that of WAMS use case summarized as follows:

- Data collection and reporting capability/function.
- Remote control of M2M Devices.
- Information collection & delivery to multiple applications.
- Data store and share.
- Authentication of M2M system with M2M devices/collectors.
- Authentication of M2M devices with M2M applications.
- Data integrity.
- Prevention of abuse of network connection.
- Privacy.
- Security credential and software upgrade at the Application level.
- In addition the following requirements are needed.

- The M2M system shall support a Gateway.
- The Gateway can be per home or per multiple homes e.g. a Gateway Concentrator.

Configuration Management:

Pre provisioning of the M2M Devices and Gateways:

- The M2M System shall support mechanisms to perform simple and scalable pre provisioning of M2M Devices/Gateways.

Management of multiple M2M Devices/Gateways:

- 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.
- The HEM application shall be able to share anonymous data with energy partners to provide the consumer with special energy rates.

Support for subscribing to receive notification:

- The M2M System shall support a mechanism for allowing applications to subscribe and being notified of changes.
- The M2M System operator shall be is able to support subscription of the HEM application to subscribe.

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.

Support for store and forward:

- 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

- Fujitsu (TTC).
- KDDI.

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 controlled energy consumption.
- Gateway Device: a device installed in the user's home and receives remote control commands from the management server.
- Management Server: the server which is in charge of collecting the status of appliances and controlling the appliances via the gateway device.
- HEMS Application Server: the server which provides HEMS service for the user through the remote management server.

9.2.4 Pre-conditions

- WAN connectivity to the Gateway Device is installed.
- Service contract is required, and authentication credentials for the Management Service are installed on the Gateway device.

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

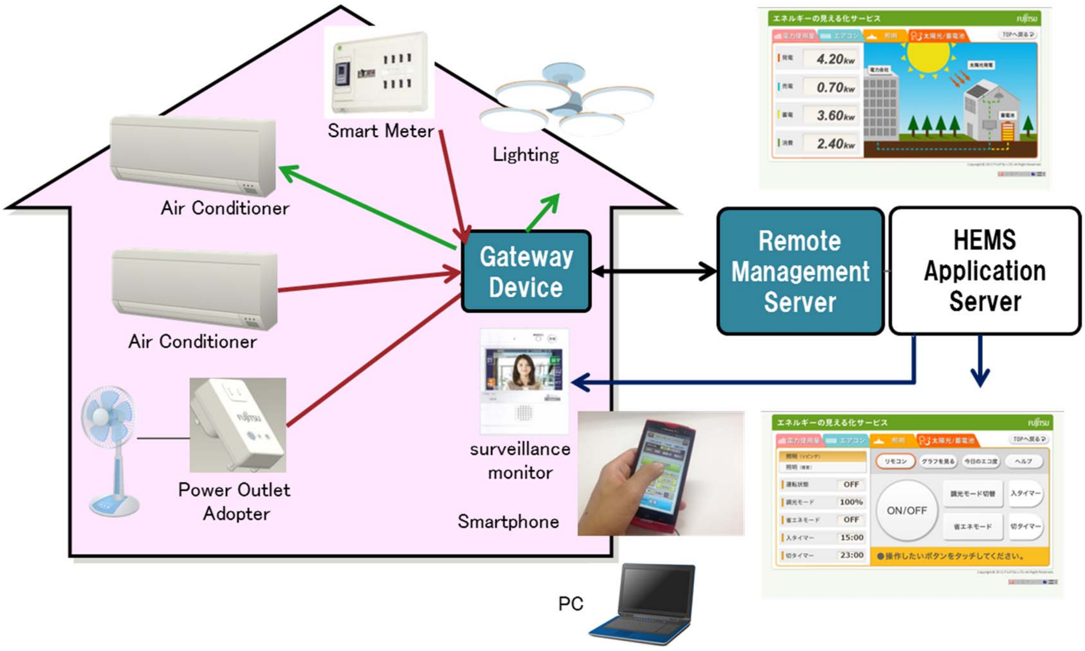

Figure 9.3: Home Energy Management System High Level Illustration

9.2.10 Potential Requirements

- Gateway Device shall have the following requirements.
- To detect the newly installed Home Appliance.
- To be provided with appropriate pre provisioning configuration which is required to host the Home Appliances?
- To support Home Appliances from multiple vendors as an abstracted object model.
- 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 ISO/IEC 15118 parts 1-4 [i.6], vehicle to grid communication; currently under development.
- EU standardisation Mandate 486 to CEN, CENELEC and ETSI (for further information refer to Mandate 486 [i.7]).
- Open 2G: using DIN specification 70121 [i.8] and ISO/IEC 15118 [i.6].
- DIN specification 70121 [i.8] defines the requirements for the communications between the Electric Vehicle (EV) and the charging EVCE).

9.3.2 Source

- Fujitsu, from ETSI TR 102 935 [i.2].

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.

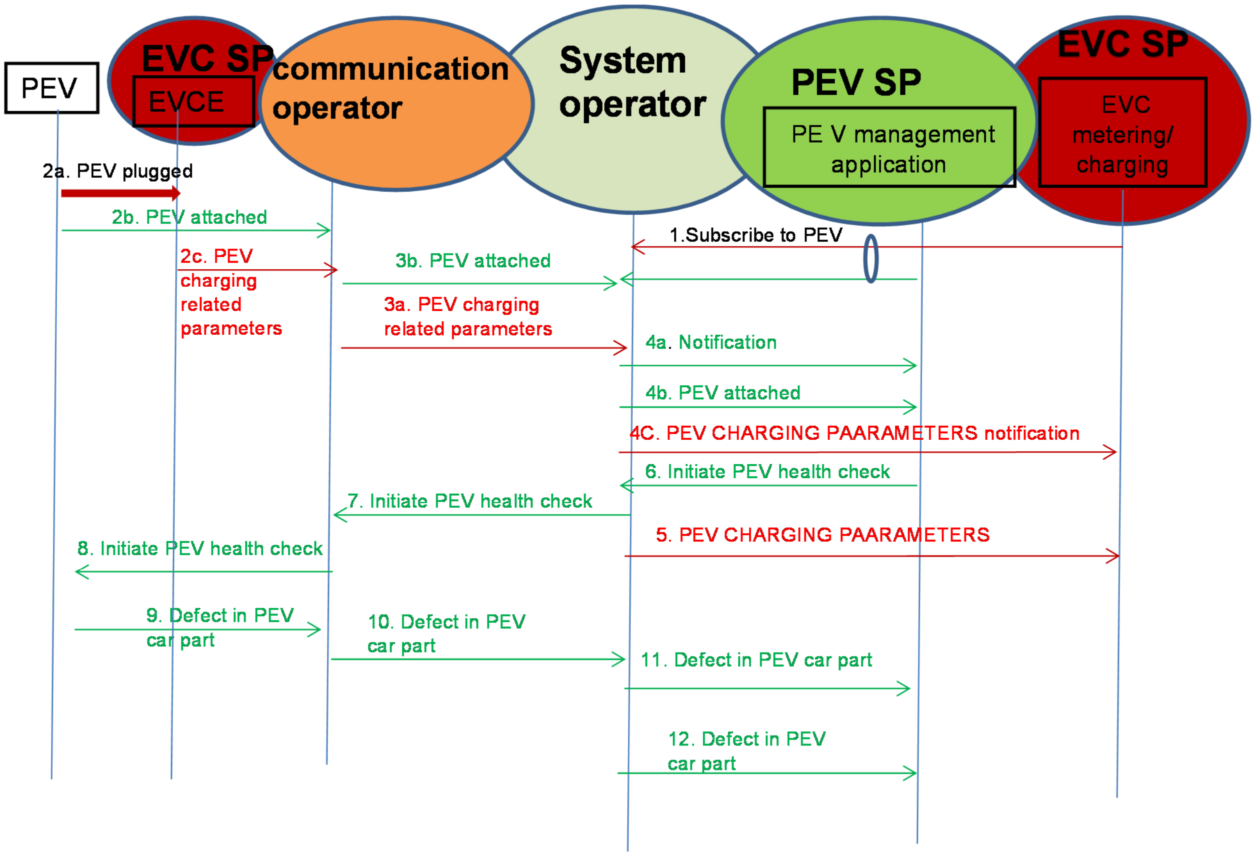
PEV
EVC SP
EVCE
communication operator
System operator
PEV SP
PE V management application
EVC SP
EVC metering/ charging
2a. PEV plugged
2b. PEV attached
2c. PEV charging related parameters
3b. PEV attached
3a. PEV charging related parameters
1.Subscribe to PEV
4a. Notification
4b. PEV attached
4C. PEV 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 9.4: 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

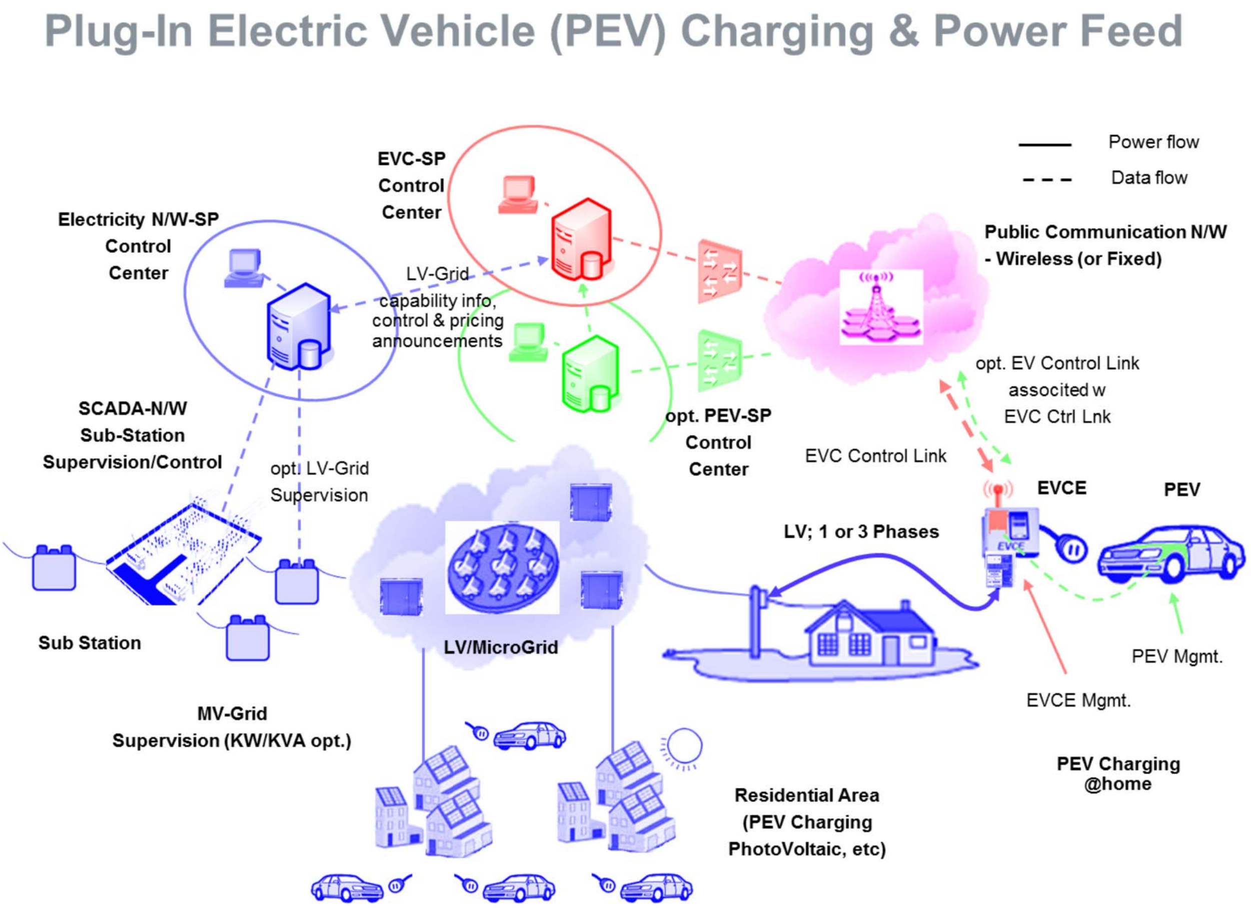
Plug-In Electric Vehicle (PEV) Charging & Power Feed
Power flow
Data flow
EVC-SP Control Center
Electricity N/W-SP Control Center
LV-Grid capability info, control & pricing announcements
Public Communication N/W - Wireless (or Fixed)
opt. EV Control Link associted w EVC Ctrl Lnk
SCADA-N/W Sub-Station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

Figure 9.5: PEV Charging High Level Illustration

9.3.10 Potential Requirements

Secure communication of the following transactions:

- SW upgrade by PEV manufacturer.
- 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.

- Collecting charging information (metering) from EVCE i.e. power feed cycle and time and charging period to the EVC-SP control center (the metering could be home owned smart meter or Utility owned).
- 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.
- Pricing info from Electricity Network SP to EVC SP.
- Fleet management control centre to collect location information of PEV.

Potential requirements are similar to those of WAMS:

- Data collection and reporting capability/function including data delivery to multiple applications.
- Remote control of M2M Devices.
- Data store and share.
- Authentication of M2M system with M2M devices/collectors.
- Authentication of M2M devices with M2M applications.
- Data integrity.
- Prevention of abuse of network connection.
- Privacy.
- 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 analyzed.

Using well-analyzed 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 analyzed 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

- Huawei Technologies UK (ETSI).
- Huawei Technologies Co., Ltd (CCSA).
- KT.

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

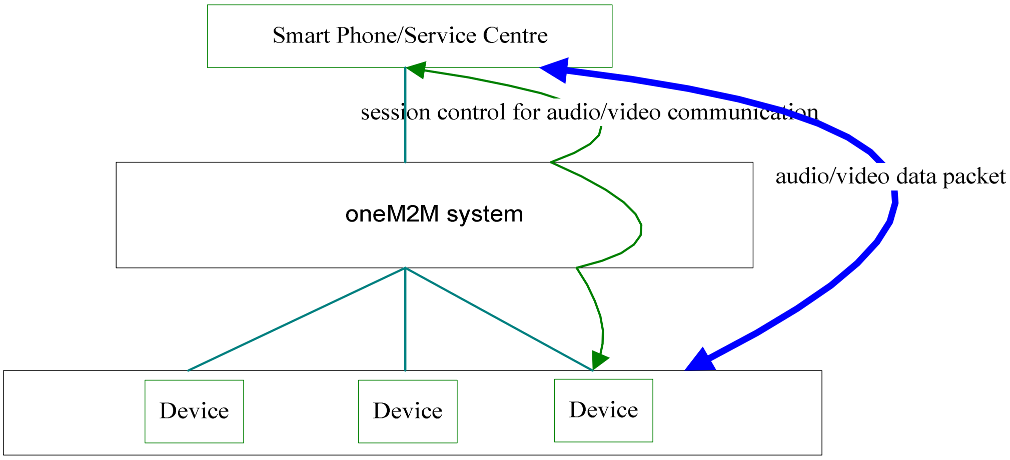
Smart Phone/Service Centre
session control for audio/video communication
audio/video data packet
oneM2M system
Device
Device
Device

Figure 9.6: 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 Use Case

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

- Fujitsu (TTC).

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 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) 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 the status change.

4) Gateway Device starts monitoring the energy consumption of the Air Conditioner.

5) When User turned off the Air Conditioner, 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 Gateway Device to report the energy consumption when the total energy consumption exceeded over the 20 kW per day.

2) Gateway Device keeps collecting data about energy consumption from home electronics (i.e. Air Conditioner).

3) When the total energy consumption exceeded over the 20 kW per day, 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

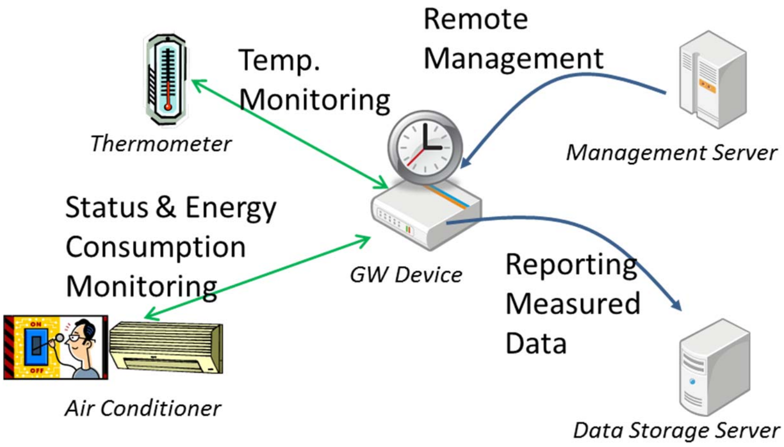

Figure 9.7: Event triggered Task Execution High Level Illustration

9.5.10 Potential Requirements

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

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

- NEC (ETSI, TTC).

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, etc.).

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

- NEC (ETSI, TTC).

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.

10 Transportation Use Cases

10.1 Vehicle Diagnostic & Maintenance Report

10.1.1 Description

The Vehicle Service Centre wants to help the vehicle owner to be aware of the status of the vehicle and remind them to maintain the vehicle in a timely manner to avoid any damages.

Hence the Vehicle Service Centre needs to obtain and analyse data from the vehicle periodically. Based on the analysis result, it will notify to the vehicle owner showing what's going on with the vehicle - in simple language and images together with some maintenance suggestions.

10.1.2 Source

- HUAWEI Technologies Co., Ltd.

10.1.3 Actors

Vehicle Owner: By reading the Vehicle Diagnostic & Maintenance Report sent from the Vehicle Service Centre, the vehicle owner would decide whether to maintain his/her vehicle.

Vehicle Service Centre: It operates a service platform for diagnostics and maintenance of vehicles, obtains and analyzes the diagnostics data from the vehicle. It will also send vehicle Diagnostic & Maintenance Report in e-mail together with maintenance suggestions to the vehicle owner.

Mobile Communication Network Operator: As the transmission medium, it supports the network services between Vehicle Service Centre and Vehicle for the information transmission.

M2M Device: It is embedded in a vehicle, which is used to send information to Vehicle Service Centre and implement diagnostics function from Vehicle Service Centre.

10.1.4 Pre-conditions

1) The vehicle supports the diagnostics pre-configured to report the diagnostics data collected from sensors within the vehicle periodically.

2) The vehicle is already ignited.

10.1.5 Triggers

None.

10.1.6 Normal Flow

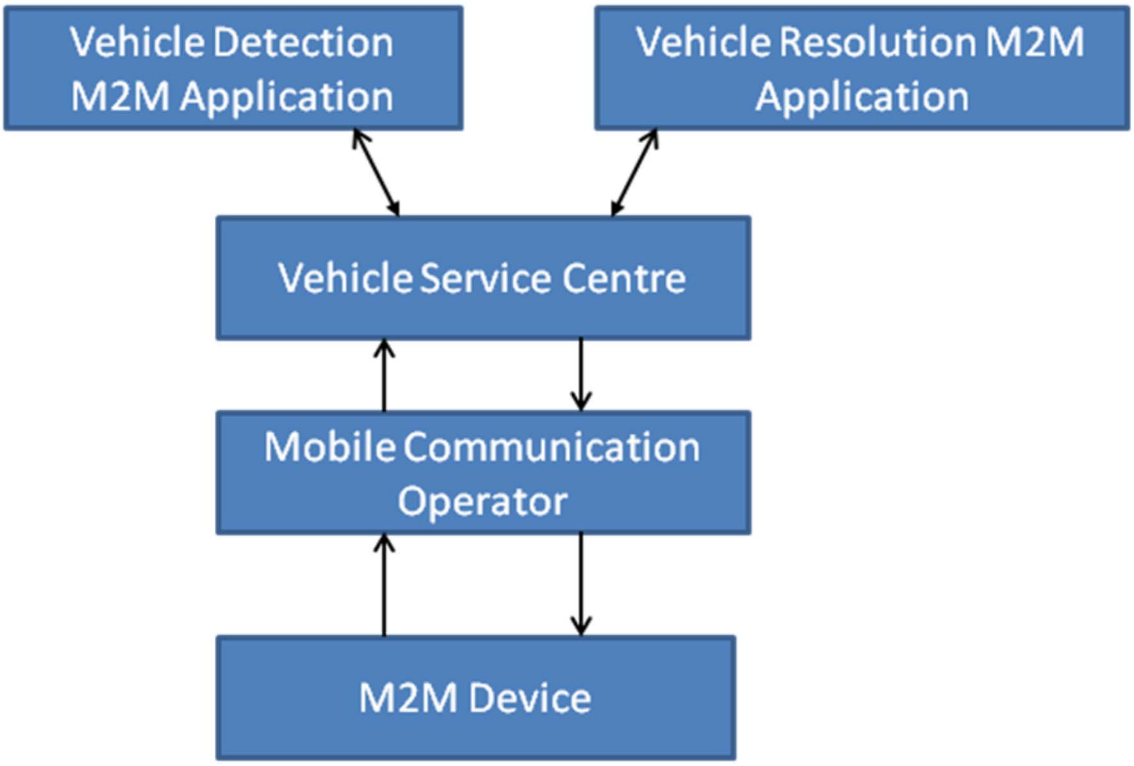
Vehicle Detection M2M Application
Vehicle Resolution M2M Application
Vehicle Service Centre
Mobile Communication Operator
M2M Device

Figure 10.1: Vehicle Diagnostics Normal Flow

1) The vehicle collects the diagnostics data from sensors within the vehicle and sends it to the Vehicle Service Centre. The diagnostics data includes information from Engine and Transmission System, Stability Control System, Air Bag System, Emission System, Antilock Brake System and so on. The information includes tyre pressure, odometer data, life of engine oil, engine and gear-box status, antilock braking system status, etc.

2) The Vehicle Service Centre sends the diagnostics data to the "Vehicle Detection M2M Application". This M2M application receives and analyzes the diagnostics data.

3) The "Vehicle Detection M2M Application" finds that the Brake pads need to be replaced. It queries the maintenance services provided by "Vehicle Resolution M2M Application" and gets the information of the company who can provide the components.

4) The "Vehicle Detection M2M Application" finally sends the Diagnostic & Maintenance Report to the vehicle owner together with the suggested component providers either by email or alert message displayed in the vehicle terminal.

5) The vehicle owner will decide whether to maintain his/her vehicle based on the Diagnostic & Maintenance Report.

10.1.7 Alternative flow

None.

10.1.8 Post-conditions

For normal flow, the vehicle owner maintains his/her vehicle according to the Diagnostic & Maintenance report in time.

10.1.9 High Level Illustration

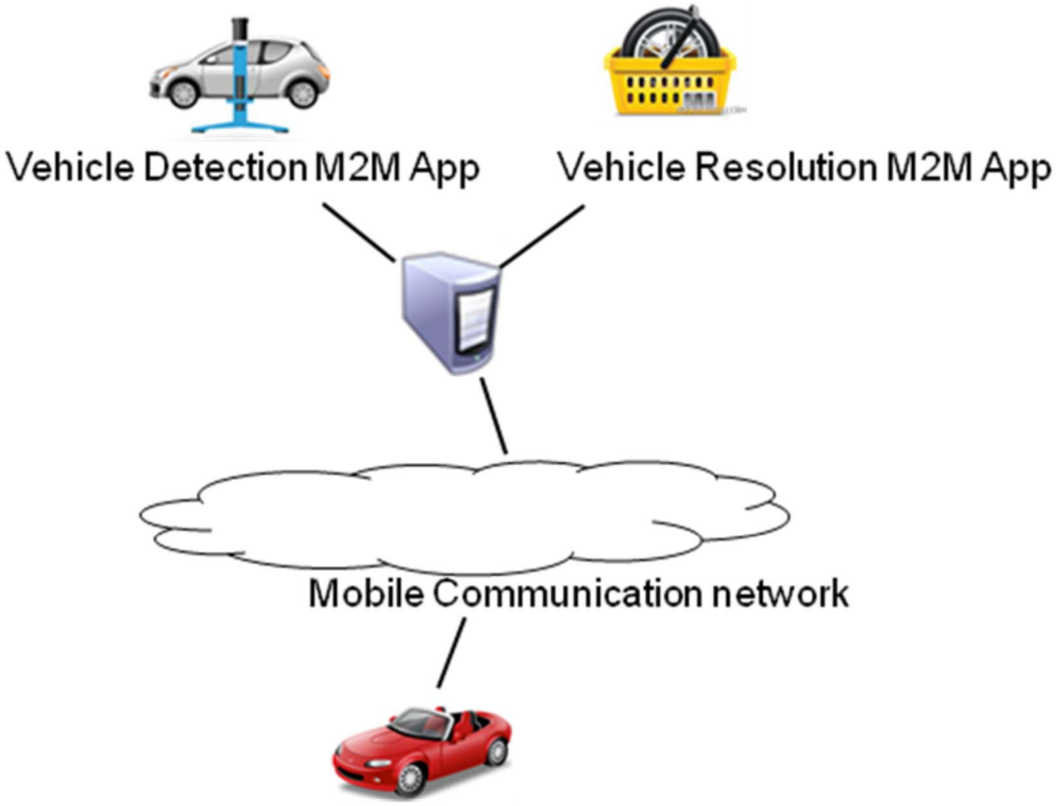
Vehicle Detection M2M App
Vehicle Resolution M2M App
Mobile Communication network

Figure 10.2: Vehicle diagnostics Normal Flow

10.1.10 Potential Requirements

1) The M2M application System shall enable the M2M Devices to exchange M2M application to diagnostic data periodically with the M2M Application in the network domain.

2) The M2M System shall enable the M2M Application to configure the notification interval in the M2M Devices.

3) The M2M system shall support a mechanism to describe the syntax and semantics format of the M2M application diagnostics data exchanged between the M2M Devices and the M2M Application in the network domain.

10.2 Use Case on Remote Maintenance Services

10.2.1 Description

This use case introduces a remote maintenance service for the automobiles (cars).

Because integrity of the cars is a matter of human life, the remote maintenance service of the car (treated as M2M Gateway in this use case) should be strongly secured.

Therefore, the integrity measurements both before and after the remote maintenance operation should also be severely performed.

One of the methods to endorse the measurement process might be guaranteed by HSM (Hardware Security Modules) in the M2M Gateway. This method provides the higher reliability level than that by the software emulator, the decision on the level of security is based on the information sent to the centre. In the HSM method, this case, the integrity measurement report is can be made by HSM through an internal the mechanism in the HSM and put in the electronic signature/ by the key in the HSM.

This use case is derived from the automobiles, but the similar case of the remote maintenance services could be considered with Medical equipment, Household applications, financial transaction terminals and Industrial control and machinery.

10.2.2 Source

- Fujitsu (TTC).

10.2.3 Actors

Relevant to the name in the figure in clause 11.2, High Level Illustration.

- Car: the machine works as a M2M Gateway in which M2M Device(s) is implemented as the parts of it.
- Center: the M2M Platform which provides remote maintenance.
- The Hardware Security Module (HSM): a module in the M2M Gateway (e.g. Trusted Platform Module) that helps determining the level of security functions to endorse the integrity measurement process and holds the electronic signature key.
- A white list: data base which is accessed by the center may be used for verifying the integrity measurement report from the M2M Gateway (car), using a secure communication protocol e.g. Trusted Network Connect TNC protocol.
- Support software: installable software module to check the integrity of the Car assisted by TPM or the emulator and to support the newly implemented M2M Device(s) (i.e. sensor(s)).

10.2.4 Pre-conditions

Center recognizes the software which is installed in the Car to shall be updated.

10.2.5 Triggers

None.

10.2.6 Normal Flow

1) Mutual authentication between the Car (M2M Gateway) and the Center (M2M Platform) is performed.

2) Center requests the Car to report the integrity check on that Car.

3) Support software which is installed in the Car runs integrity check of the Car assisted by TPM or the emulator.

4) Generated integrity status/configuration information report is endorsed by the hardware key which is protected by TPM. The present document may contain a detection of the newly implemented sensor(s) (M2M Device(s)).

5) Support software sends the report based on TNC (Trusted Network Connect, which is application level secure communication protocol) to the Center.

6) Center verifies the report securely based on the White list which is based outside the M2M network.

7) Center determines whether the Car contains the software which shall be updated.

8) Center selects corresponding software modules.

9) Center delivers the support software module to the Car.

10) The support software is applied at the Car.

11) The applied result endorsed by the device key (actual process is done by TPM or the emulator) is reported to the Center.

12) Center side confirms the completion of delivery/embedding.

13) Center side stores the sequence of operations log as certifiable evidence for indemnity.

10.2.7 Alternative flow

None.

10.2.8 Post-conditions

Newly installed software/sensor(s) is correctly identified as authorized part(s) on the Car, and working correctly with installed support software. The Car's integrity status/configuration information data which is endorsed by the hardware key which is protected by TPM or the emulator is sent to the Center side.

10.2.9 High Level Illustration

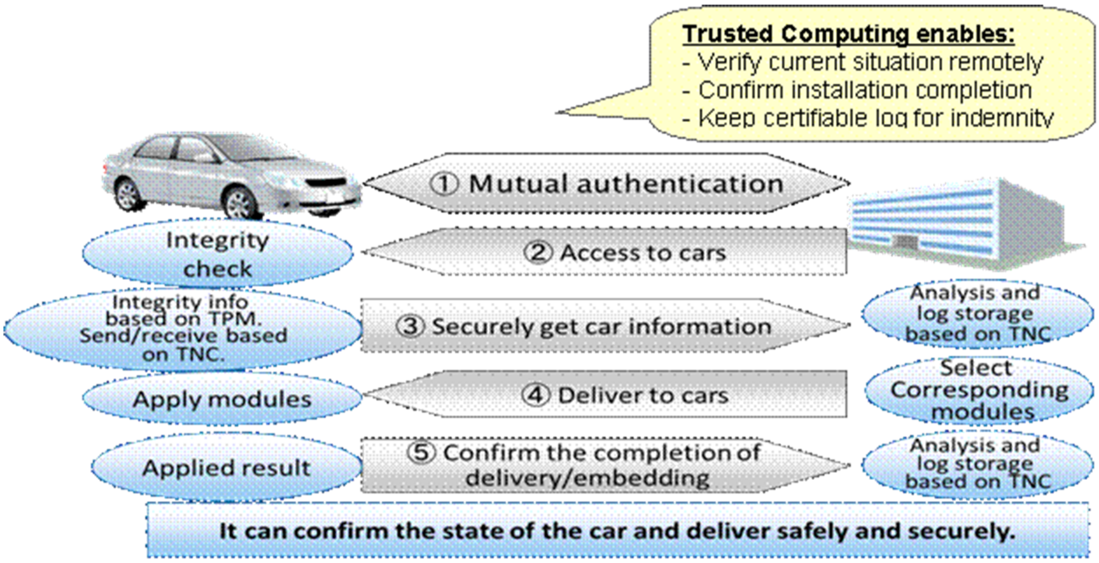
Trusted Computing enables:
- Verify current situation remotely
- Confirm installation completion
- Keep certifiable log for indemnity
① Mutual authentication
Integrity check
② Access to cars
Integrity info based on TPM. Send/receive based on TNC.
③ Securely get car information
Analysis and log storage based on TNC
Apply modules
④ Deliver to cars
Select Corresponding modules
Applied result
⑤ Confirm the completion of delivery/embedding
Analysis and log storage based on TNC
It can confirm the state of the car and deliver safely and securely.

Figure 10.3: Remote Maintenance Flow

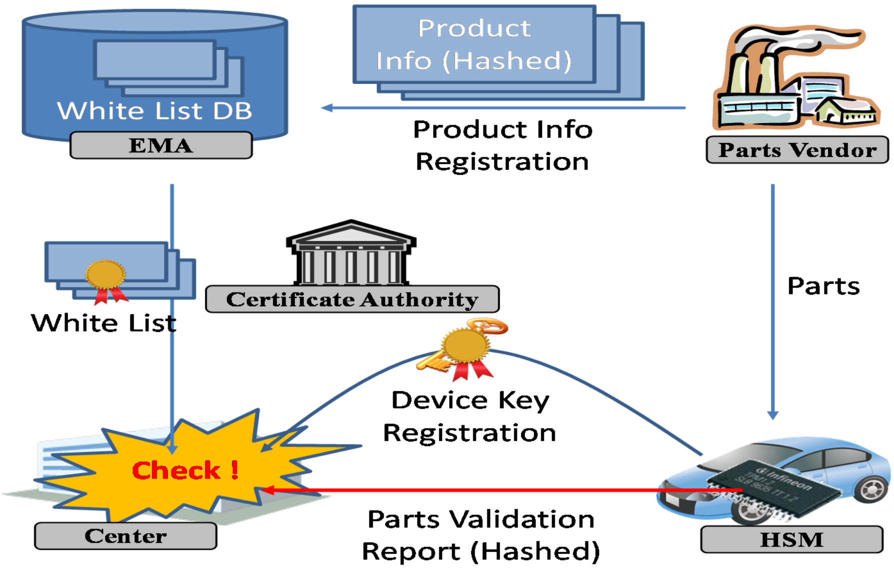

Figure 10.4: Remote Maintenance High Level Illustration

10.2.10 Potential Requirements

1) The M2M service SHALL be able to provide the mechanism for authorization for integrity-checking and installing processes of software/hardware/firmware component(s) on M2M Device(s).

2) The M2M system SHALL be able to support authentication using device key on the integrity check for M2M Device(s).

3) The M2M Device SHALL be able to support HSM (Hardware Security Module) to protect its integrity depending on the security level requirement.

10.3 Traffic Accident Information Collection

10.3.1 Description

The Intelligent Transportation System (ITS) is mainly used for avoiding collision of vehicles. If doing some extension, an ITS can also be used for other purposes such as electronic payment of road tolls, traffic information collection and broadcast, local service advertisements, etc.

It is for sure that the ITS will save a lot of lives, but some traffic accidents will occur any way. So we still need rescue teams to go to the accident sites to help the victims and police to ease the traffic jam caused by the accident. A rescue team can make a more proper rescue plan if they are able to see the scene of accident. Similarly police can make a better traffic control plan if they are able to get an overview of traffic situation near the accident site.

This use case will show how the M2M technologies can help people to timely access to the detailed information of a traffic accident.

10.3.2 Source

- China Academy of Telecommunication Technology (CCSA), ETSI TR 102 638 [i.9].

10.3.3 Actors

M2M Platform: It stores M2M data and runs M2M applications. It provides various M2M services to M2M service subscribers.

ITS Center: It is responsible for managing ITS on M2M Platform. It decides what service is provided to an ITS service subscriber.

Police Station: It is a subscriber of ITS service on M2M platform and responsible for controlling the traffic.

Rescue Center: It is a subscriber of ITS service on M2M platform and responsible for carrying out rescue missions.

ITS-Station (ITS-S): It is a kind of M2M Device installed in vehicles. It broadcast its travel status in a fixed interval in order to inform other ITS-S where it is. The ITS-S is equipped with a digital camera used for taking pictures according to the command given by a driver, ITS center or ITS-S itself. The ITS-S is able to communicate with M2M Platform through wireless network or a RSU using Dedicated Short Range Communications (DSRC).

Road Side Unit (RSU): It is a kind of M2M Gateway installed at roadside. The RSU is able to communicate with ITS-S using DSRC and communicate with M2M Platform through wired or wireless network.

10.3.4 Pre-conditions

The ITS-Ss are equipped with a digital camera.

The ITS-Ss nearby the accident site are able to connect to M2M platform through either the wireless network or a RSU.

Police Station and Rescue Center are the subscribers of ITS services.

10.3.5 Triggers

There are two ways to start an accident reporting process. One is the ITS-S involved in an accident detects the crash and then starts an accident reporting process automatically; the other is a driver in a passing by vehicle manually starts an accident reporting process through giving a command to the ITS-S in his vehicle.

10.3.6 Normal Flow

1) The ITS-S in the vehicle that is directly involved in an accident detects a crash has happened, and then starts an accident reporting process automatically.

2) An accident reporting process may also be started manually. For example, a driver of a vehicle that is passing by the accident site stops and then manually starts an accident reporting process through giving a command to the ITS-S in his vehicle.

3) The ITS-S first takes some pictures with its digital camera, and then uses these pictures together with current time and geographical coordinates to generate an accident report. The present document shall be signed by the ITS-S.

4) The ITS-S tries to connect to M2M Platform and then sends the accident report to the M2M Platform (step 1 in figure 10.5).

5) There are two ways for an ITS-S to connect to the M2M Platform. One is through wireless network; the other is through a nearby RSU using DSRC.

6) The M2M Platform receives and verifies the accident report, and then does some necessary analysis. The analysis result will be pushed to the subscribers, i.e. the Police Station and the Rescue Center.

7) The subscribers receive, verify and parse the information coming from M2M platform, and then do some necessary analysis. Based on different situation the subscribers may ask the M2M Platform to provide further information.

8) In this scenario the Police Station asks the M2M Platform to provide an overview of the traffic situation near the accident site, and the Rescue Center asks the M2M Platform to provide more visual information about the accident. These service requirements are submitted to the M2M Platform.

9) The M2M Platform receives and verifies the service requirements from Police Station and Rescue Center, and then sends data collection commands to the ITS-S that originally sends the accident report (step 2 in figure 10.5).

10) The command generated for Police Station requires the ITS-Ss near the accident site to report their travel status.

11) The command generated for Rescue Center requires the ITS-Ss around the accident site to provide pictures.

12) The ITS-S that originally sent the accident report receives the commands sent from the M2M Platform. It verifies and parses the commands, and then broadcasts the commands that should be broadcasted (step 3 in figure 10.5).

13) In this scenario the broadcasted commands are generated by the M2M platform for Police Station and Rescue Center respectively.

14) The ITS-Ss nearby the accident site receive, verify, parse and execute received commands, i.e. take pictures, get current travel status, generate reports, sign the reports and upload signed reports to M2M Platform. These reports could be sent anonymously (step 4 in figure 10.5).

15) Some commands need to be rebroadcasted within a predetermined area and predetermined period of time (step 5 in figure 10.5).

16) In this scenario the command generated for the Police Station needs to be rebroadcasted. The ITS-Ss receive this command will only report their travel status (step 6 in figure 10.5).

17) M2M Platform accumulates and verifies the reports uploaded by the ITS-Ss, and then generates a report contain visual information about the accident scene for the Rescue Center and a report about traffic situation near the accident site. These reports will be pushed to Rescue Center and Police Station respectively.

18) The Rescue Center analyzes the report about the accident scene, and then makes a proper rescue plan. The Police Station analyzes the report about traffic situation, and then makes a proper travel control plan.

10.3.7 Alternative flow

None.

10.3.8 Post-conditions

Based on the detailed information provided by the ITS service on the M2M platform, the rescue team can make a proper rescue plan, and the police can make a proper travel control plan.

10.3.9 High Level Illustration

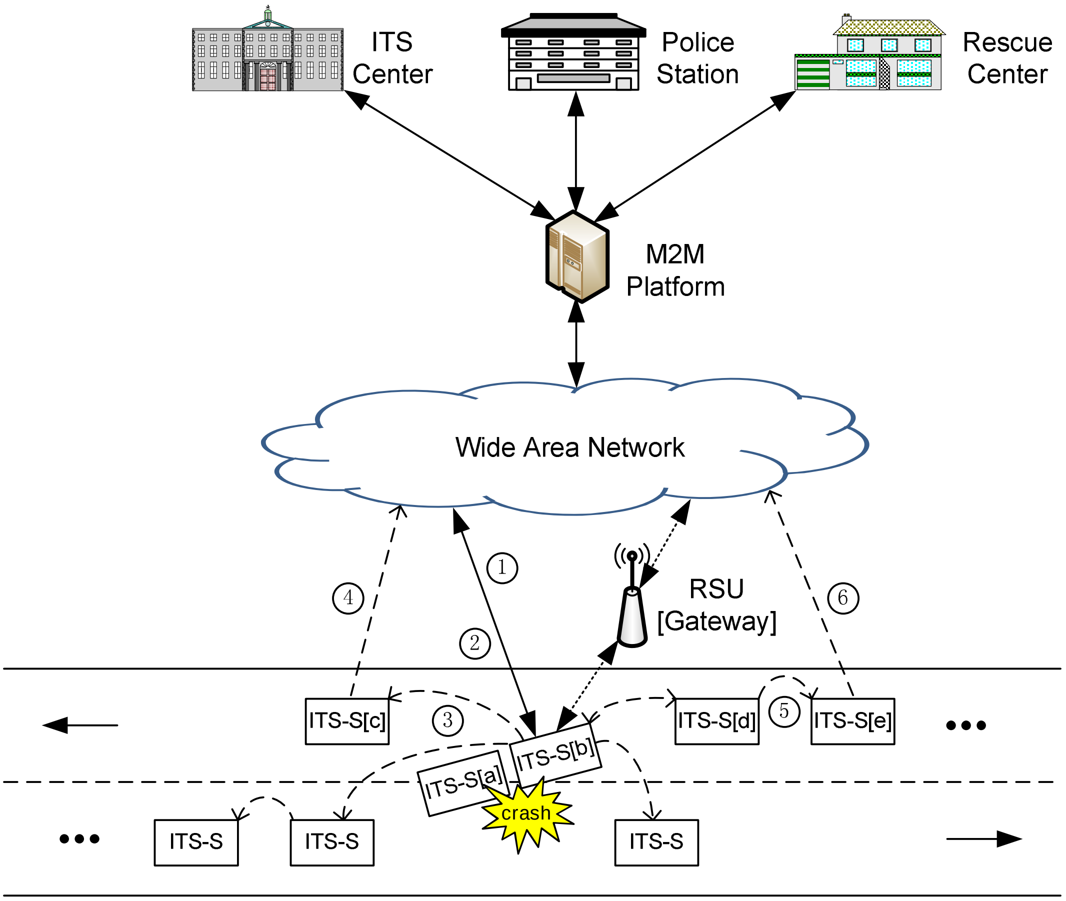

Figure 10.5: High Level Illustration of Traffic Accident Information Collection

10.3.10 Potential Requirements

1) A M2M System shall support communication between M2M Platform and a M2M device either directly or via a gateway.

2) A M2M System shall be able to exchange information between M2M applications via M2M Platform.

3) A M2M System shall be able to take actions according to the received service requests from M2M Applications.

4) A M2M system shall be able to support service requests from M2M applications for communication with QoS requirement, such as, higher delivery priority, reliable delivery, etc.

5) A M2M System shall support mutual-authentication among M2M device, M2M gateway, M2M platform and M2M Application.

6) The information sent by a M2M device or the M2M platform or a M2M application shall use cryptographic technology to ensure information authentication and information integrity.

7) A M2M system shall permit information being provided in anonymous way.

8) A command issued by a M2M System shall be able to have time expiration or geography restriction.

10.4 Fleet Management Service using DTG (Digital Tachograph)

10.4.1 Description

"DTG-based fleet management service" is the fleet management services utilizing DTG data and related service, to facilitate extensive service features of fleet management.

DTG provides vehicle data such as driving speed, RPM (Revolution Per Minute), brake's status, and mileage, etc.

DTG data management service, based on M2M gateway and DTG data management server, reports and manages DTG data in real-time to store it in the memory of M2M device in vehicle at a certain rate (i.e. one second in this case) to submit it to the national authority or transfer it to central office managing the data in a server.

The fleet management service utilizing the above mentioned service functionality provides advanced service features such as the precise quest of vehicles based on location and the tracking of cargo along with the route of the carrier vehicle, by means of the capability of remote monitoring and control of vehicle status provided by the DTG data management service.

10.4.2 Source

- ETRI.
- KCA.
- SK Telecom.

10.4.3 Actors

- DTG device manufacturer to provide DTG devices and DTG management system.
- M2M device manufacturer to provide M2M gateway and related functionalities.
- The service provider for fleet management service using DTG.
- The network provider supporting the communication for fleet management service.
- The national agency that manages and operates DTG data (in case of Korea).

10.4.4 Pre-conditions

- The DTG device records the DTG data occasionally or periodically to transfer it to an application server through M2M Gateway.
- M2M service gateway delivers the DTG data, useful to fleet management service, from terminal system to the application server.
- Application server provides fleet management service, using DTG data, to customer.
- A taxi call service provider operates fleet management service using DTG data, such as for reporting the taxi location and passenger status and for call arrangement.
- A bus traffic service provider operates fleet management service using DTG data, including for providing guide information on bus arrival/estimated time, bus schedules on web-site, and status information such as route and air pressure of tire, etc.
- A fleet management service provider of truck operates fleet management service based on vehicle information (location, route, gas, tire pressure etc.) and peripheral device information (temperature, humidity, door lock and goods weight, etc.).

10.4.5 Triggers

The following triggers could initiate the information exchanging process according to the flows described hereafter followings:

- Creation of DTG data that M2M device occasionally or periodically transfers to an application server.
- Arrangement of taxi service calls delivered to a DTG device.
- Report of information about vehicle location and route to application server.

10.4.6 Normal Flow

DTG service (Common service)

- DTG data is periodically (normally once in a second in this case) transferred and stored into DTG management server, and when in case of an event of accident, the data is stored at an immediate mode (within 10ms in this case).
- The DTG data stored in DTG device will be transferred to DTG management server periodically, and once after the engine stopped.
- The DTG management server stores DTG data and accident event file which is to be posted onto the web site of national agency.
- Analysis of DTG data and accident data to provide driving behavioural habits (quick start/stop, excessive speed) or the accident causes.

Taxi call service

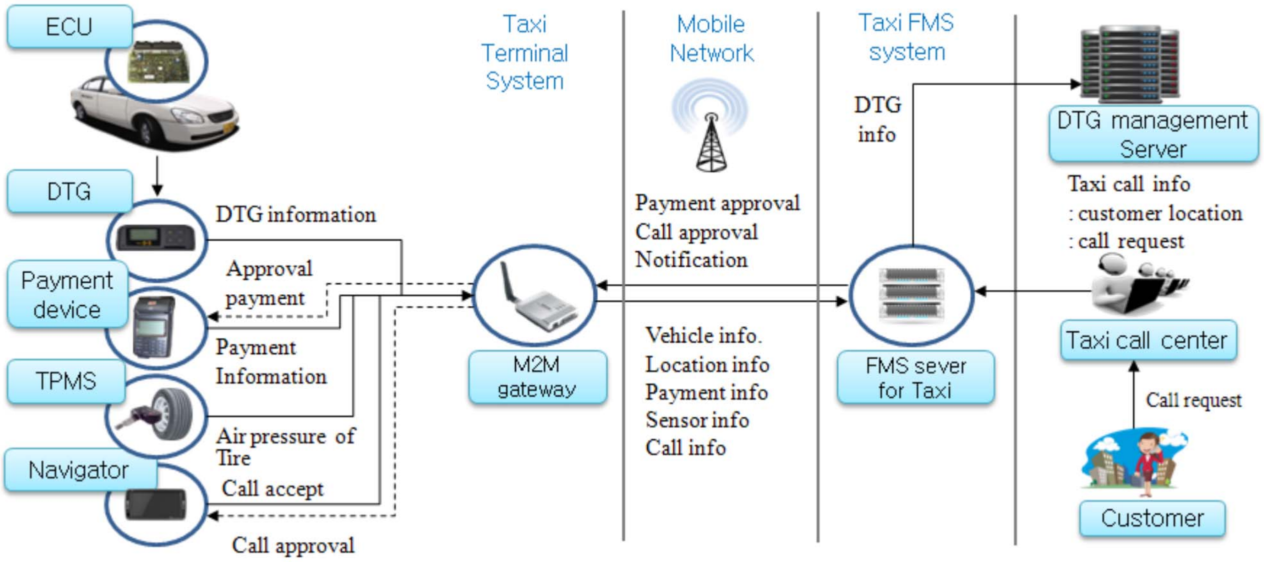

Figure 10.6: Taxi Call Service Normal Flow

- Terminal system occasionally or periodically reports location, passenger status information to application server (FMS server).
- Customer requests taxi call service to the taxi call centre through a phone call or smart phone application.
- Taxi call centre sends call request to a terminal system in the taxi through the application server.
- The taxi driver accepts the call request through the terminal system, and then the taxi will come to the customer's location.

Fleet Management Service (Truck)

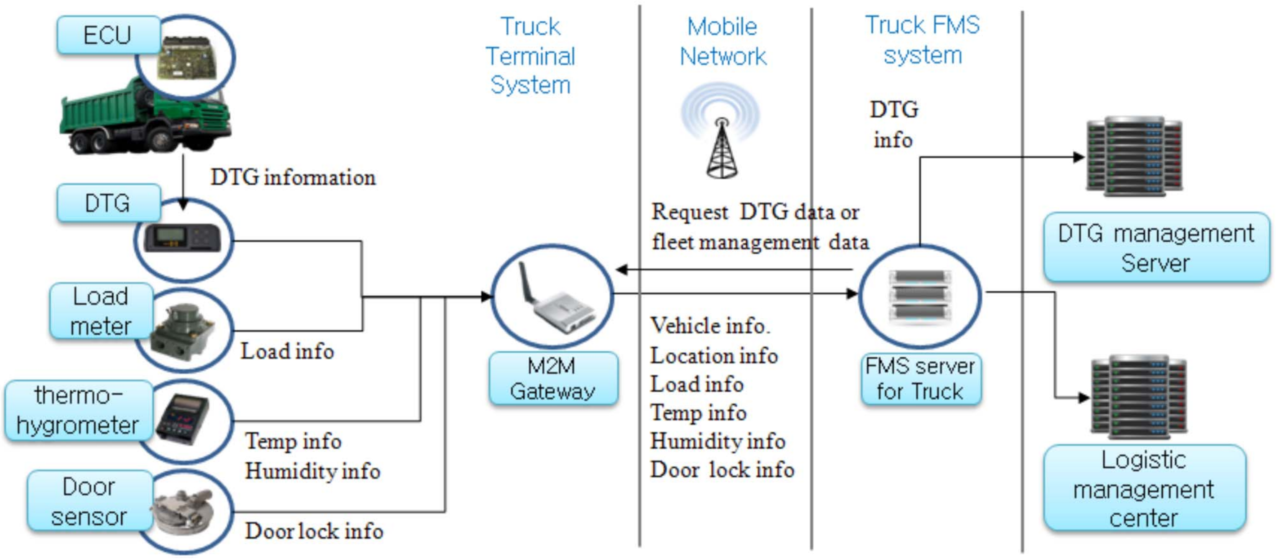

Figure 10.7: Normal Flow - Fleet Management Service (Truck)

- Terminal system occasionally or periodically reports the vehicle status information including the location, current route, ignition status, terminal version, and driver information to application server (FMS server).
- When the application server receives the information, it delivers it to logistic management center.
- Terminal system also reports the peripheral information (air pressure of tire, gas gauge, temperature, humidity, door lock etc.) to the logistics management center through the application server.
- Logistic management center can request the information about vehicle itself or peripheral device, to enforce possible controls to them when it is needed.
- Terminal system reports the emergency events, such as fire in car, unlocked doors when unattended, and puncture while driving, etc. to FMS server.

Fleet Management Service (Bus)

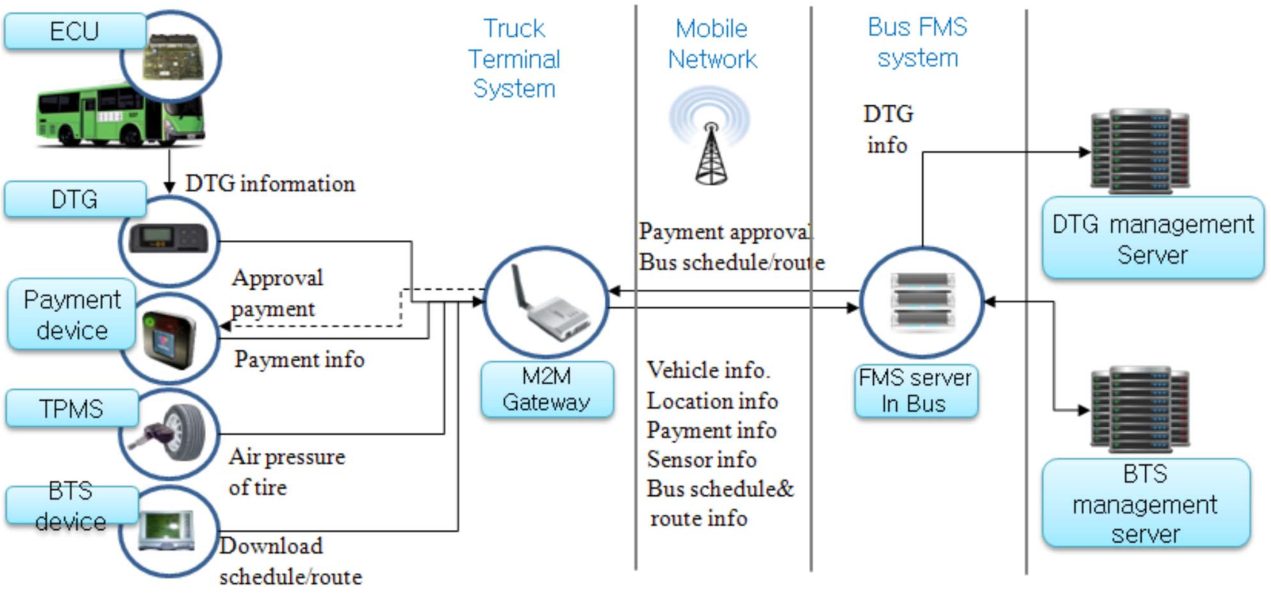

Figure 10.8: Normal Flow - Fleet Management Service (Bus)

- When the application server receives the vehicle information (engine ignition, terminal version, car S/N, and driver ID, etc.) from terminal system, it provides the received information to the BTS management server.

- BTS management server sends time schedule, route of bus and the fare information to terminal system through the application server (FMS server).
- Terminal system sets the time schedule, the route, and the fare information. And then it occasionally or periodically reports its location and the driving route to application server.
- Terminal system also reports the information about peripheral devices such as air pressure of tire, gas gauge level, and bus fare status to BTS management server occasionally or periodically.
- BTS management server provides an arrival/estimated time and a bus schedule on web-site.

10.4.7 Alternative flow

None.

10.4.8 Post-conditions

None.

10.4.9 High Level Illustration

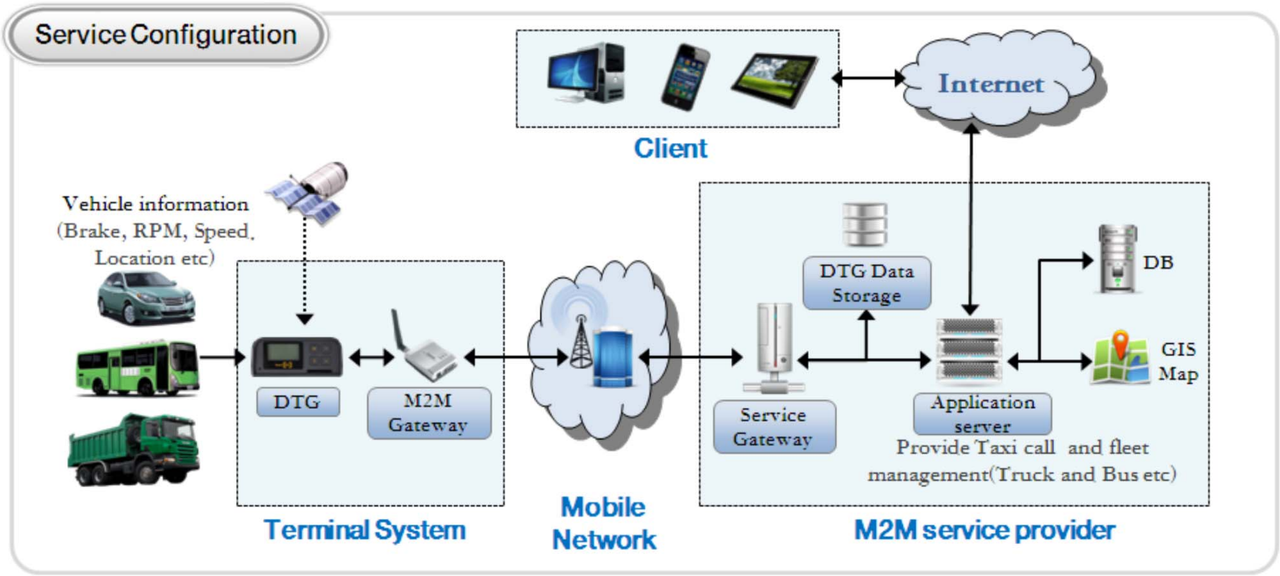

Figure 10.9: High Level Illustration Fleet Management

10.4.10 Potential Requirements

- Provisioning, installation, configuration and registration method of terminal system:
  - Especially for the case of overlapping two different system for DTG management system (owns and manages the device) and the application system using DTG data (utilising the data from the device).
- DTG/FMS data storing method and delivery protocol:
  - There is no dominant standard specifying data formats and protocols for vehicle related applications.
- Vehicle location based service method:
  - M2M service platform is expected to provide the service capability supporting location based service.
- Control, configuration, error logging, and management method for the terminal system Over The Air:
  - M2M service platform is expected to provide the service capability supporting the Over The Air management.

11 Other Use Cases

11.1 Extending the M2M Access Network using Satellites

11.1.1 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.

11.1.2 Source

- Inmarsat.
- Sierra Wireless.

11.1.3 Actors

Service Providers for M2M.

11.1.4 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 centers 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 reclosers, 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.

11.1.5 Triggers

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

11.1.6 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 center (figure 11.1).

The satellite connectivity backhauls Smart Meter data from a satellite antenna mounted on an Advanced Metering Infrastructure (AMI) concentrator to the utility's data center. 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.

11.1.7 Alternative flow

None.

11.1.8 Post-conditions

None.

11.1.9 High Level Illustration

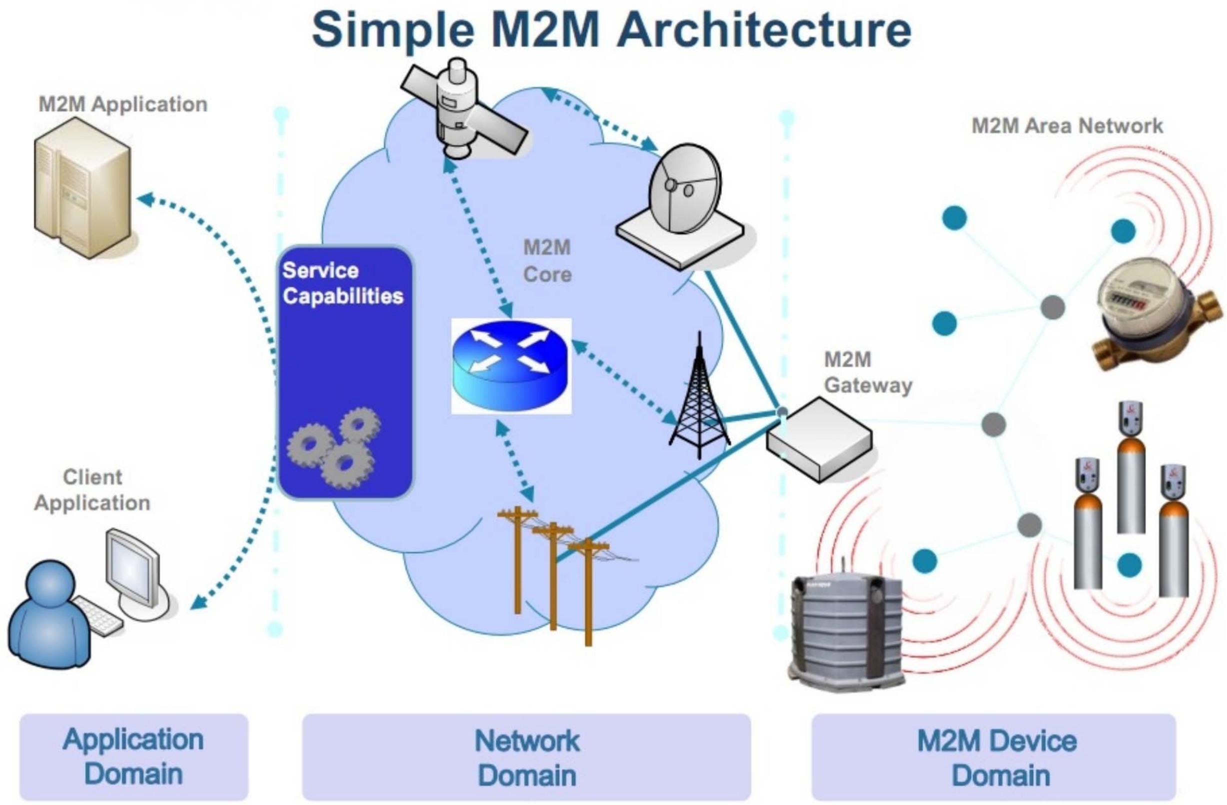

Figure 11.1: Extended Smart Metering Configuration (source: ETSI)

11.1.10 Potential Requirements

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

11.2 M2M Data Traffic Management by Underlying Network Operator

11.2.1 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.

11.2.2 Source

- NTT DOCOMO.
- NEC.
- KDDI.

11.2.3 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.

11.2.4 Pre-conditions

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

11.2.5 Triggers

None.

11.2.6 Normal Flow

Normal Flow 1:

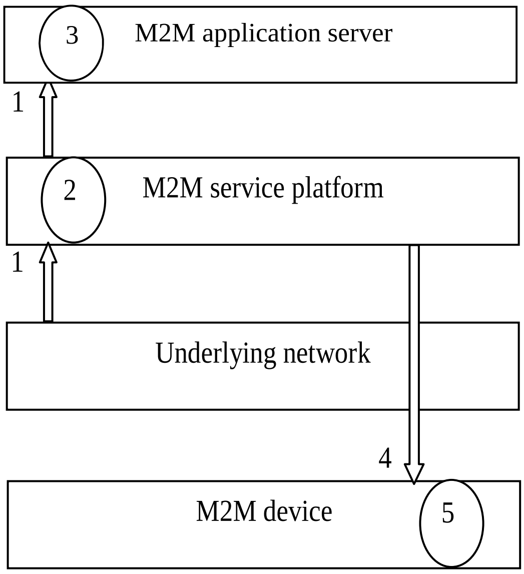

Figure 11.2: Normal Flow 1 of Data Traffic Management by Underlying Network Operator

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:

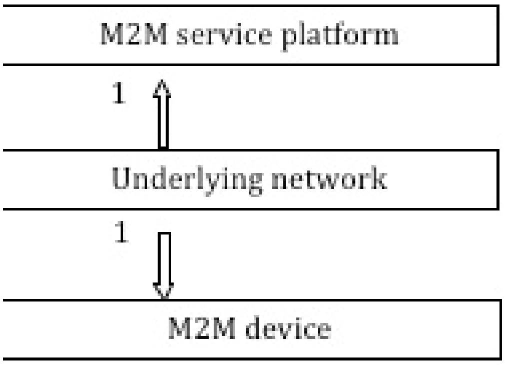

Figure 11.3: Normal Flow 2 of Data Traffic Management by Underlying Network Operator

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 behaviour, 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.

11.2.7 Alternative flow

None.

11.2.8 Post-conditions

None.

11.2.9 High Level Illustration

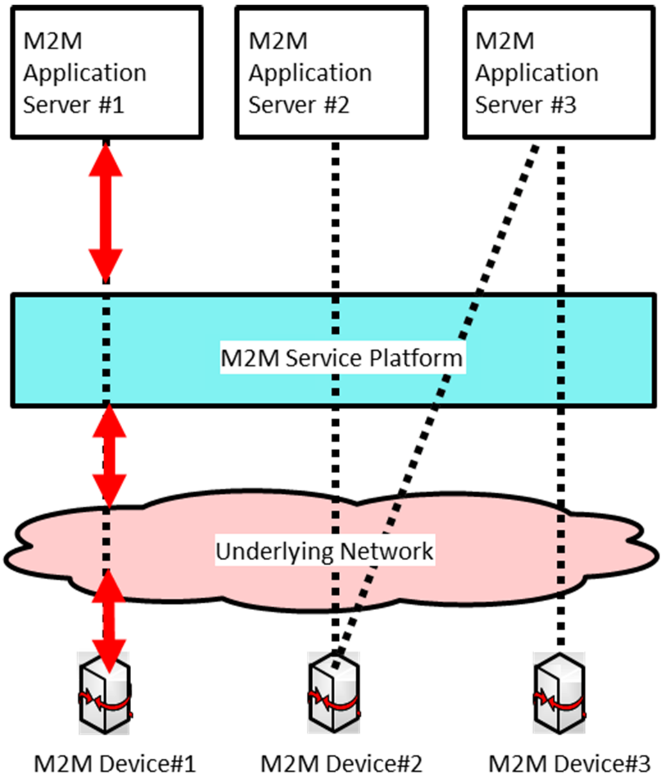
M2M Application Server #1
M2M Application Server #2
M2M Application Server #3
M2M Service Platform
Underlying Network
M2M Device#1
M2M Device#2
M2M Device#3

Figure 11.4: High Level Illustration of Data Traffic Management by Underlying Network Operator

11.2.10 Potential Requirements

- 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.
- The M2M service platform MAY SHALL be able to control M2M data transmission based on the Underlying Network data traffic condition.
- The M2M device SHALL be able to control M2M data transmission based on the Underlying Network data traffic condition.
- The M2M device SHALL control M2M application behavior implemented on top of M2M service layer when the M2M device received notification regarding Underlying Network data traffic condition from the Underlying Network.

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

11.3.1 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 ETSI TS 122 368 [i.10]. 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 ETSI TS 123 682 [i.11], the architecture study in 3GPP TR 23.887 [i.12].

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.

11.3.2 Source

- NEC.
- KDDI.

- InterDigital.
- NTT DOCOMO.

11.3.3 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 (5 min, 30 min, 1 h) 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, analyze 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.

11.3.4 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.

11.3.5 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).

11.3.6 Normal Flow

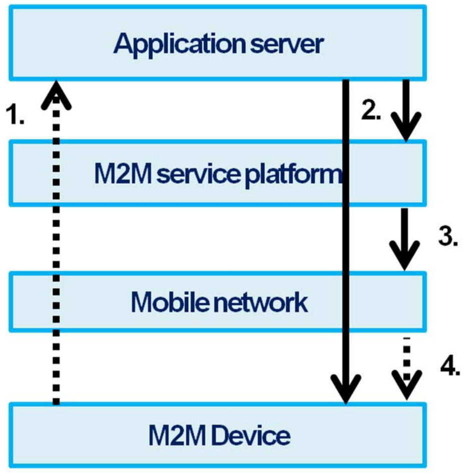

Figure 11.5: Normal Flow - Optimizing connectivity management parameters

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 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.

11.3.7 Alternative flow

None.

11.3.8 Post-conditions

The configuration parameters of the mobile network about the M2M device:

- The connection keep time: Long.

11.3.9 High Level Illustration

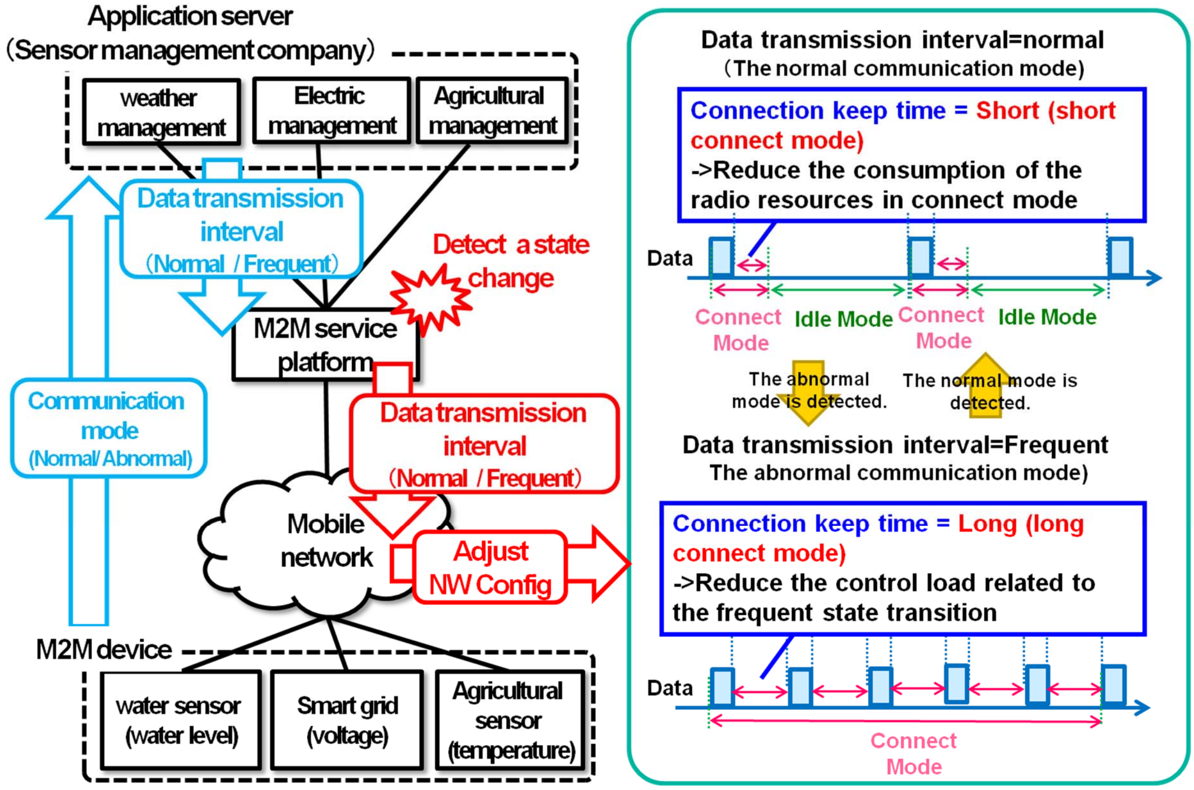
Application server
(Sensor management company)
weather management
Electric management
Agricultural management
Data transmission interval (Normal / Frequent)
Detect a state change
M2M service platform
Communication mode (Normal/ Abnormal)
Data transmission interval (Normal / Frequent)
Mobile network
Adjust 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 11.6: High Level Illustration - Optimizing connectivity management parameters

11.3.10 Potential Requirements

- 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.
- The M2M service platform MAY be able to compute the information with which the Underlying Network should be provided by analyzing 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.

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

11.4.1 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 ETSI TS 122 368 [i.10]. 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 ETSI TS 123 682 [i.11], the architecture study in 3GPP TR 23.887 [i.12].

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.

11.4.2 Source

- NEC.
- KDDI.
- NTT DOCOMO.

11.4.3 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, analyze 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.

11.4.4 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.

11.4.5 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).

11.4.6 Normal Flow

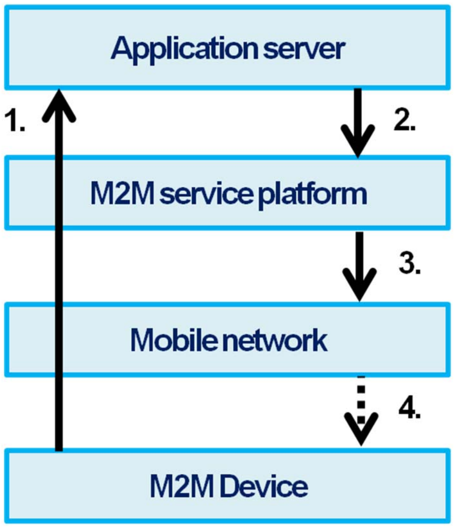

Figure 11.7: Normal Flow - Optimizing mobility management parameters

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.

11.4.7 Alternative flow

None.

11.4.8 Post-conditions

The configuration parameters of the mobile network about the M2M device:

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

11.4.9 High Level Illustration

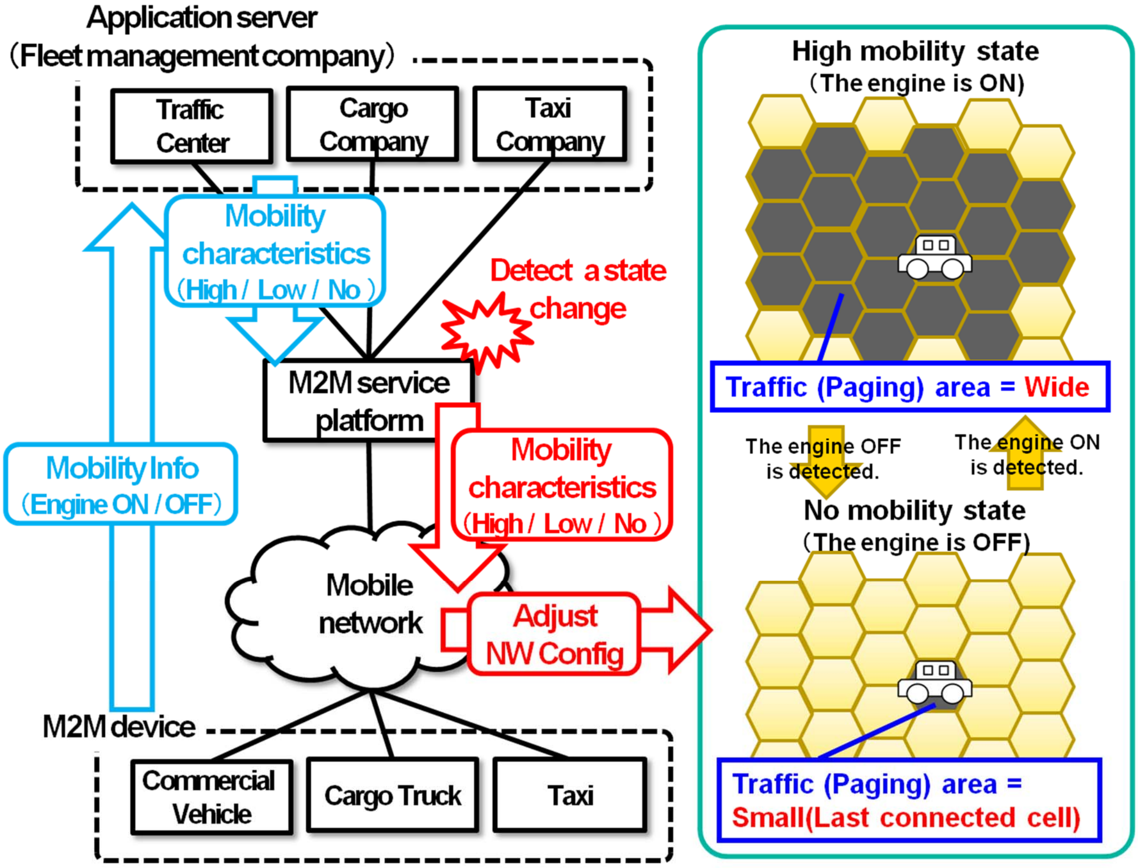
Application server
(Fleet management company)
Traffic Center
Cargo Company
Taxi Company
Mobility characteristics (High / Low / No)
Detect a state change
M2M service platform
Mobility Info (Engine ON / OFF)
Mobility characteristics (High / Low / No)
Mobile network
Adjust NW Config
M2M device
Commercial 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 11.8: High Level Illustration - Optimizing mobility management parameters

11.4.10 Potential Requirements

- 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.
  - How to utilize such information by the cellular network is the cellular operator implementation dependent and outside the scope of oneM2M.
- The M2M service platform MAY be able to compute the information with which the Underlying Network should be provided by analyzing 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.

11.5 Sleepy Node Use Case

11.5.1 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 analyzes 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.

11.5.2 Source

- InterDigital Communications.
- Sprint.

11.5.3 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.

11.5.4 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.

11.5.5 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).
- Status 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.

11.5.6 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 has to 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.

5) The device returns to a sleep state.

11.5.7 Alternative flow

None.

11.5.8 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.

11.5.9 High Level Illustration

None.

11.5.10 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 11.1

Temp req. nr.	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.
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.
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.
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.
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.

Temp req. nr.	Submitted req. number	Initial submitter	Requirement
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

A. 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.

B. 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.

11.6 Use Case on collection of M2M System data

11.6.1 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.

11.6.2 Source

- China Unicom.
- Huawei technologies.

11.6.3 Actors

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

11.6.4 Pre-conditions

None.

11.6.5 Triggers

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

11.6.6 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 Center.

11.6.7 Alternative flow

None.

11.6.8 Post-conditions

None.

11.6.9 High Level Illustration

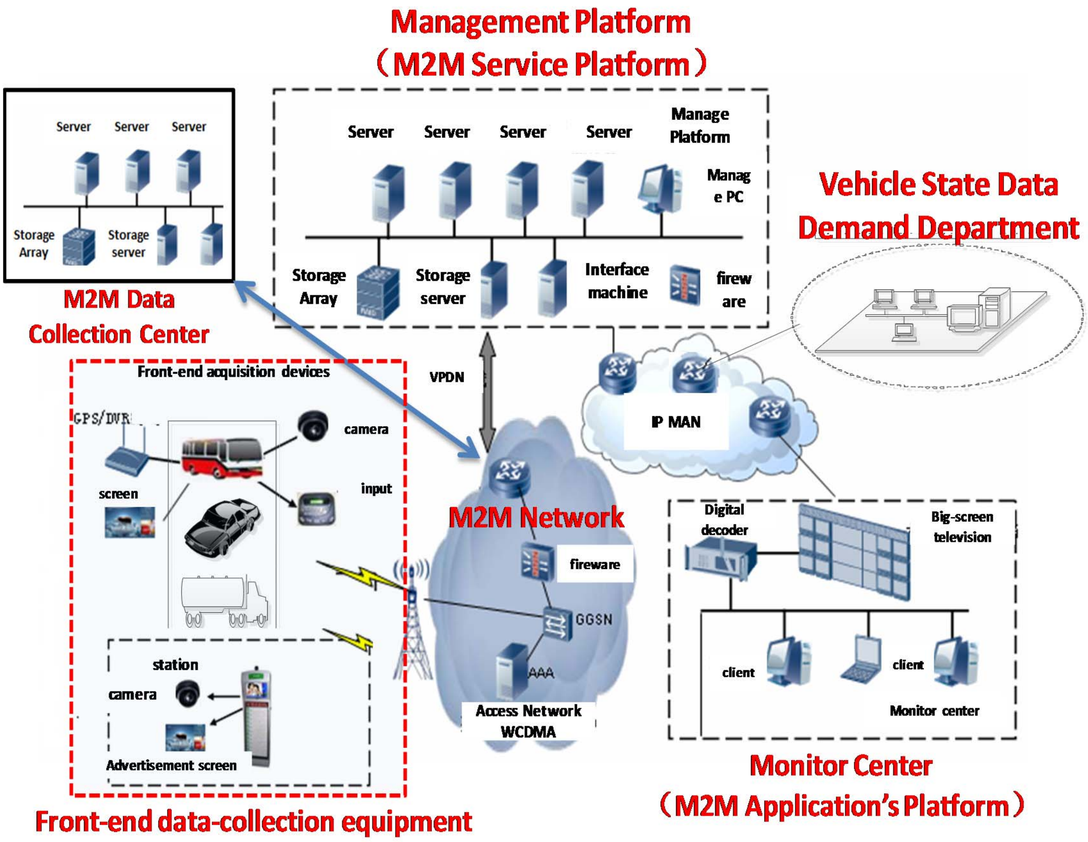

Figure 11.9: Vehicle Operation Management System

- 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 Center: 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 center, automobile and parts manufacturers, government regulatory platform, etc.
- M2M System Data Collection Center: use built-in data collectors resided in Network Equipment, M2M Platform, Costumed M2M Modules and Costumed M2M Terminal Devices to collect M2M System data.

11.6.10 Potential Requirements

M2M System should support M2M System data collection.

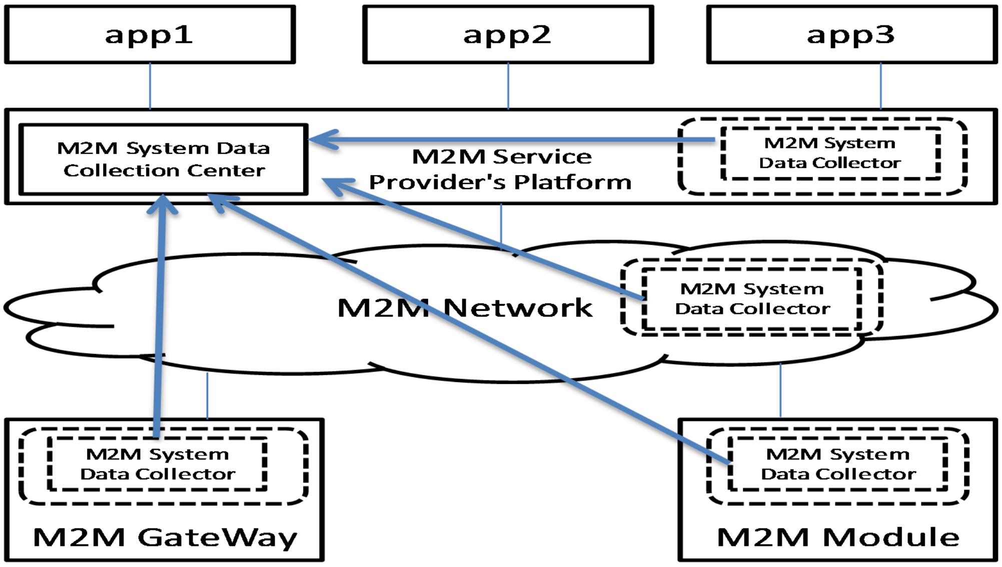
app1
app2
app3
M2M System Data Collection Center
M2M Service Provider's Platform
M2M System Data Collector
M2M Network
M2M System Data Collector
M2M System Data Collector
M2M GateWay
M2M System Data Collector
M2M Module

Figure 11.10: M2M System Data Collection Processing Flow

As illustrated in figure 11.10, we suggest that M2M System data collector should Reside in:

- M2M Service Providers' Platform.
- M2M Network Equipment.
- M2M Devices and Gateways.
- M2M Communication Module.

11.7 Leveraging Broadcasting/Multicasting Capabilities of Underlying Networks

11.7.1 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.

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 WiFi).

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.

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 neighborhood burglar alarms and alerts the M2M Application on the subscribed usersM system. For example, unifie.
- 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.

11.7.2 Source

- NEC Corporation (TTC).
- NEC Europe (ETSI).

11.7.3 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.

11.7.4 Pre-conditions

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

11.7.5 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.

11.7.6 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. analyzes 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.

5) 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.

11.7.7 Alternative flow

None.

11.7.8 Post-conditions

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

11.7.9 High Level Illustration

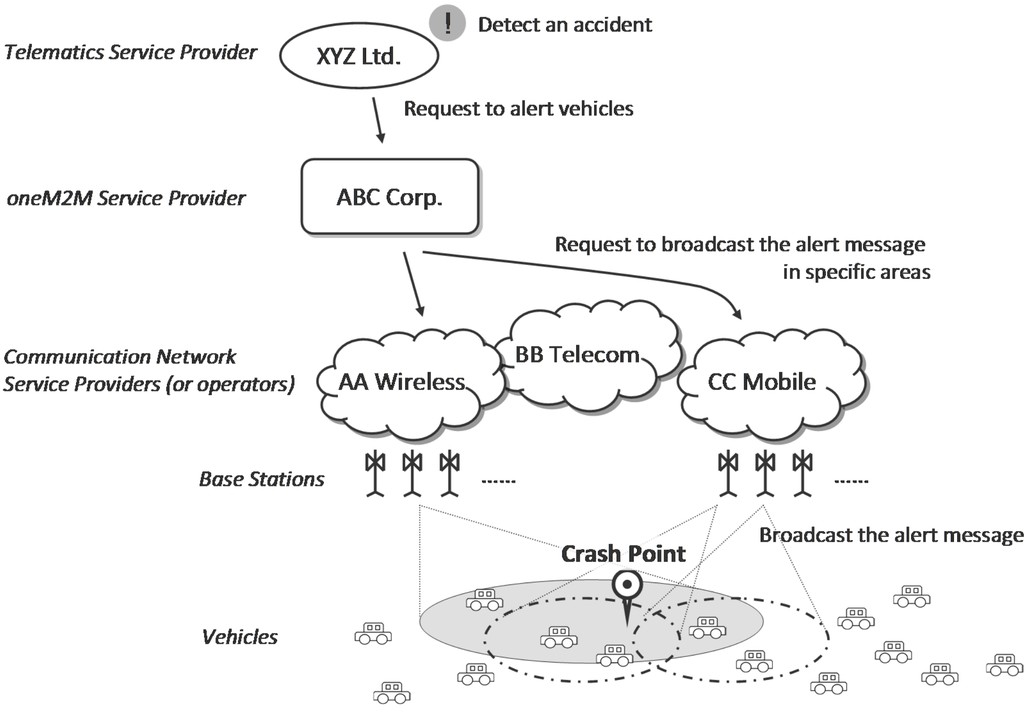
Detect an accident
Telematics Service Provider
XYZ Ltd.
Request to alert vehicles
oneM2M Service Provider
ABC Corp.
Request to broadcast the alert message in specific areas
Communication Network Service Providers (or operators)
AA Wireless
BB Telecom
CC Mobile
Base Stations
Broadcast the alert message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

Figure 11.11: High level illustration 1

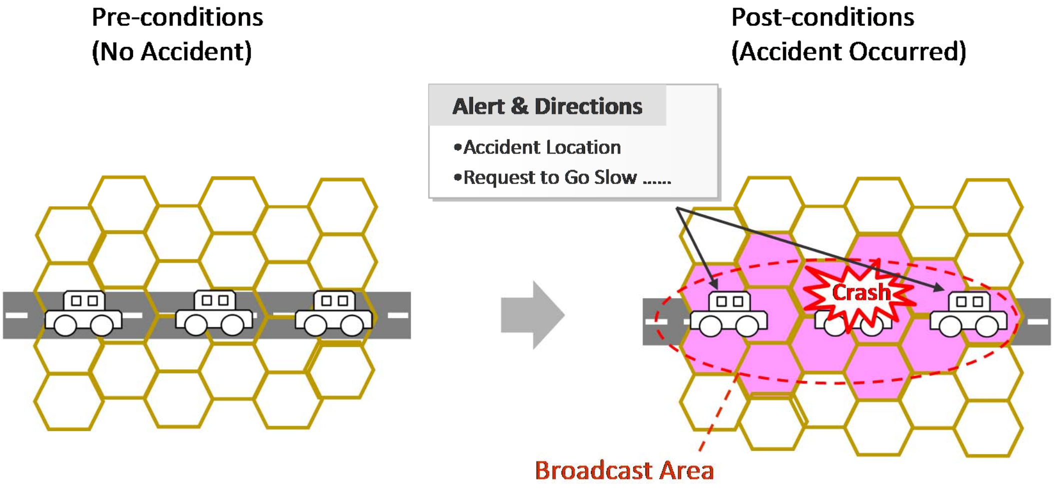

Figure 11.12: High Level Illustration 2

11.7.10 Potential Requirements

- oneM2M System SHALL be able to leverage broadcasting and multicasting capability of Underlying Networks.
- 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.

- 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.
- 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.
- oneM2M System SHALL be able to receive information on broadcasting/multicasting capability/functionality of each underlying network.
- 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.
- oneM2M System SHALL be able to analyze a message from a M2M Application to determine broadcast parameters.
- 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.

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

11.8.1 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. eUICC [i.15] 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.

11.8.2 Source

- China Telecom.
- Huawei.

11.8.3 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 (EU)

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.

11.8.4 Pre-conditions

- EU uses equipment remote maintenance service provided by EP.
- EP 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.

11.8.5 Triggers

None.

11.8.6 Normal Flow

Equipment's lifetime can be summarized as in figure 11.13.

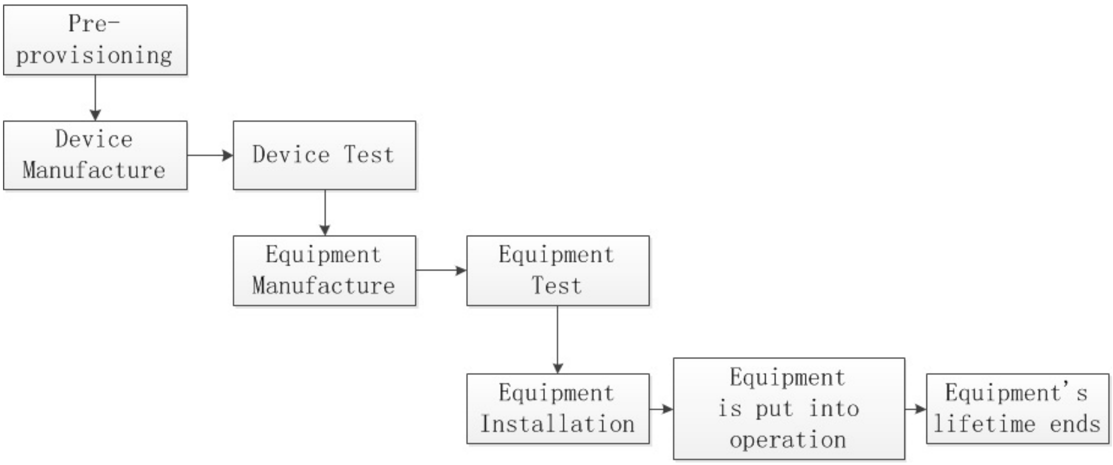

Figure 11.13: Equipment lifetime

M2M service provisioning for equipment with built-in M2M device mainly consists of the following scenarios:

- Pre-provisioning Scenario.
- 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.

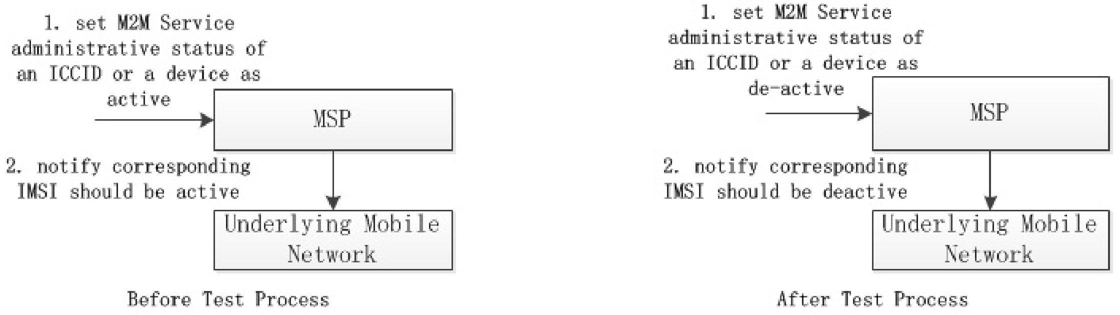
1. set M2M Service administrative status of an ICCID or a device as active
MSP
2. notify corresponding IMSI should be active
Underlying Mobile Network
Before Test Process
1. set M2M Service administrative status of an ICCID or a device as de-active
MSP
2. notify corresponding IMSI should be deactive
Underlying Mobile Network
After Test Process

Figure 11.14

(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.

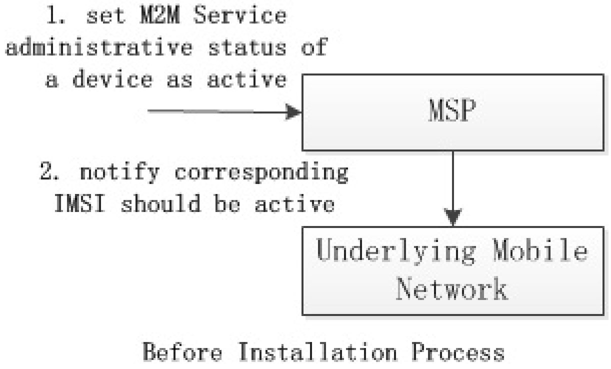
1. set M2M Service administrative status of a device as active
MSP
2. notify corresponding IMSI should be active
Underlying Mobile Network
Before Installation Process

Figure 11.15

(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.

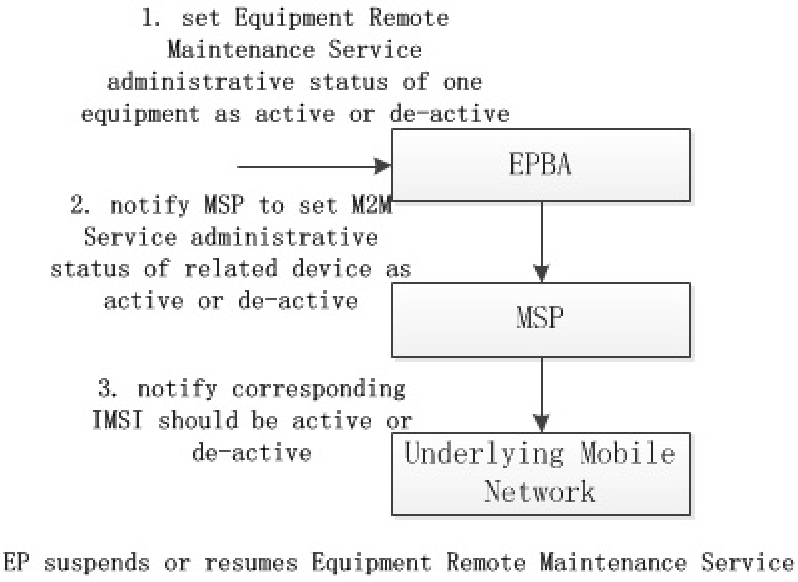
1. set Equipment Remote Maintenance Service administrative status of one equipment as active or de-active
EPBA
2. notify MSP to set M2M Service administrative status of related device as active or de-active
MSP
3. notify corresponding IMSI should be active or de-active
Underlying Mobile Network
EP suspends or resumes Equipment Remote Maintenance Service

Figure 11.16

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.

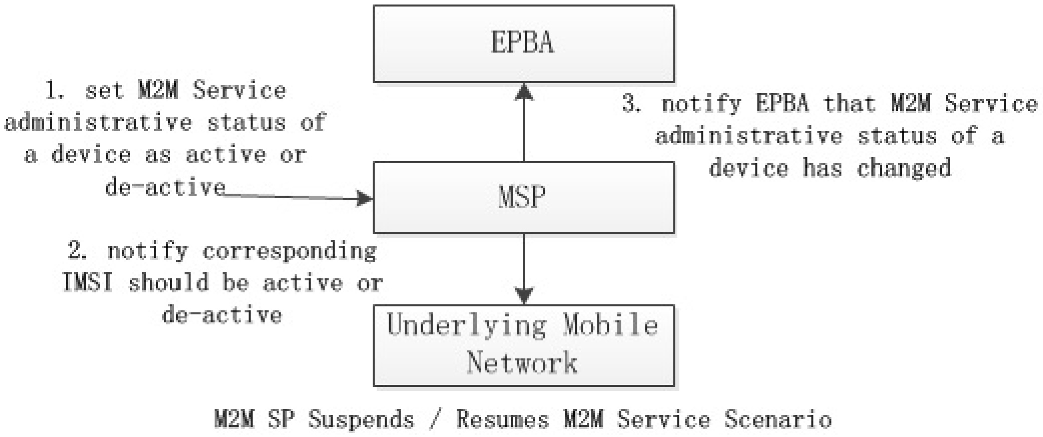
EPBA
1. set M2M Service administrative status of a device as active or de-active
3. notify EPBA that M2M Service administrative status of a device has changed
MSP
2. notify corresponding IMSI should be active or de-active
Underlying Mobile Network
M2M SP Suspends / Resumes M2M Service Scenario

Figure 11.17

(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.

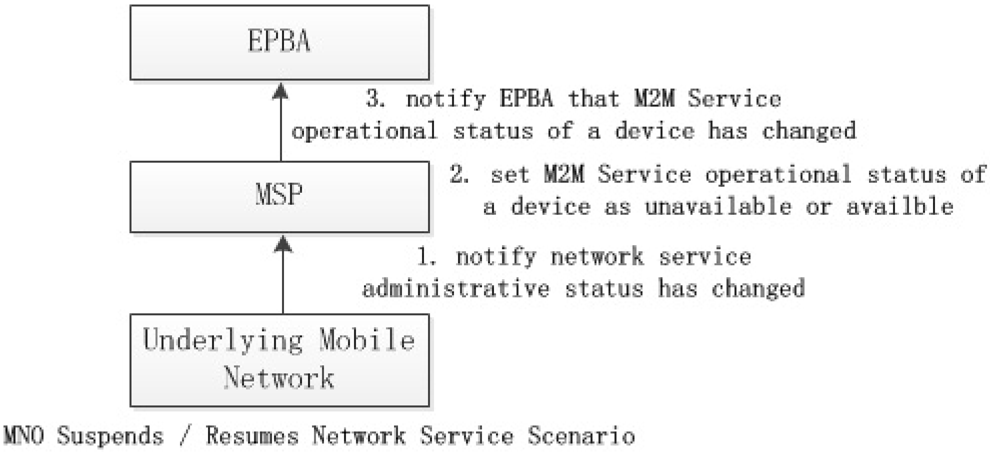
EPBA
3. notify EPBA that M2M Service operational status of a device has changed
MSP
2. set M2M Service operational status of a device as unavailable or availble
1. notify network service administrative status has changed
Underlying Mobile Network
MNO Suspends / Resumes Network Service Scenario

Figure 11.18

(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 administrative 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.

11.8.7 High Level Illustration

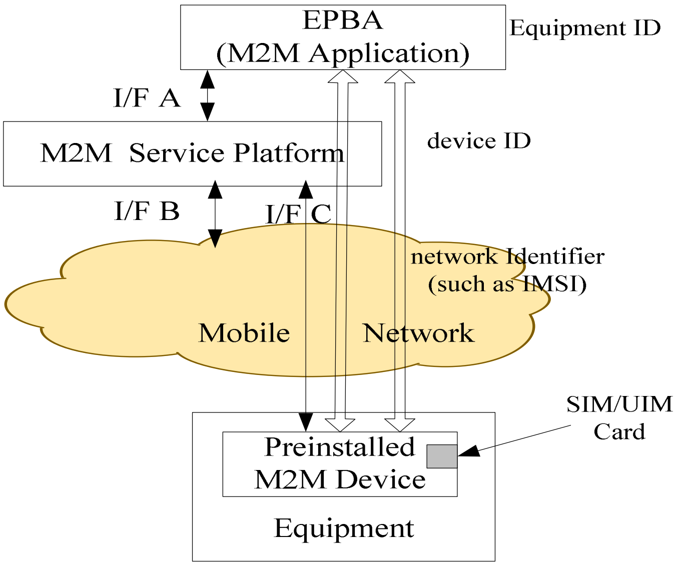

Figure 11.19: High Level Illustration

11.8.8 Service Model

EP provides equipment remote maintenance service to EU. 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.

11.8.9 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.

11.8.10 Potential requirements

1) The M2M System shall identify and manage M2M Service status of devices.

NOTE 1: 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.

NOTE 2: 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 3: Different MNOs may expose different kinds of network identifiers to the M2M System. It's up to MNO.

3) 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.

4) 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.

5) 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.

6) The M2M System should support M2M Application to activate or de-activate M2M Service administrative status of a device.

History

Document history		
V1.0.0	May 2015	Publication