WiMAX Forum Correspondence
Service Provider Working Group

20 December 2010

To: Roger Marks, Chair, IEEE 802.16 Working Group <r.b.marks@ieee.org>

Subject: Draft WiMAX Forum Machine to Machine Communications Requirements Spec

The Service Provider Working Group (SPWG) in the WiMAX Forum (WMF) has recently completed the Draft Specification on *Requirements for WiMAX Machine to Machine Communications*. It is attached for your information. We hope that this document will be informative to the IEEE 802.16 Working Group and will be taken in to consideration in the development of the IEEE P802.16n and P802.16p draft standards (on *Higher Reliability Networks* and *Enhancements to Support Machine-to-Machine Applications*, respectively).

Although the draft is not yet formally approved, it is our view that the technical content is quite stable. However, we welcome any comments or feedback that you may have, and we can consider such feedback during a future revision. We further request you to share the scope and the schedule of the work in your relevant development activities. We would be pleased to receive your information in January 2011, if possible.

Best regards

Asan Khan, Asan_Khan@cable.comcast.com, SPWG Chair
Chungwoo Hwang, cwhwang@kt.com, SPWG Vice-Chair
Ivan Bernikov, IBernikov@yotateam.ru, SPWG Vice-Chair

Requirements for WiMAX Machine to Machine (M2M) Communication

2010-12-20

DRAFT-T31-127-Rxxx-v01-O

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO ANY OTHER MEMBER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, EACH MEMBER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

This document is subject to the WiMAX Forum IPR Policy and may contain Necessary Claims that are subject to licensing disclosures or other licensing statements as listed in Appendix [IPR]. However, the listed Necessary Claims may not be all Necessary Claims contained in the document. Each WiMAX Forum member expressly acknowledges that the WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. Each member acknowledges that it is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such, technologies, standards, and specifications, including through the payment of any required license fees.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion.

TABLE OF CONTENTS

1 Introduction (Informative)

This document is the first of a three-stage, end-to-end network system architecture specification for broadband wireless networks based on WiMAX Forum Certified™ products. This document specifies recommendations and requirements for such networks from the perspective of network operators intending to deploy WiMAX networks. It describes business and usage scenarios, deployment models, and functional requirements. Architectural details shall be specified in stage-2 and stage-3 specifications based on the requirements outlined in this document.

Machine to Machine (M2M) service is a data communication between devices through a WiMAX access network, or between a device and a server in the core network through a WiMAX access network that may be carried out without any human interaction. Common characteristic of M2M applications may include:

- Large number of devices;
- Bursts of data transmission;
- Stationary or low mobility application;
- Automatic resource connection and release from the devices.

For M2M communication, two different modes of communication can be identified:

1. An M2M Device communicates with one or more servers,
2. An M2M Device communicates with another M2M Device.

Note: This second communication mode is outside the scope of this document.

2 Objective and Scope

The objective of this document is to define requirements to support Machine to Machine Service over WiMAX System. The WiMAX Machine to Machine Service supports WiMAX network and device [].

The scope of the work item is as follows:

- To define use cases for M2M communications over the WiMAX network
- To define the requirements for M2M communications over WiMAX network

3 Abbreviations, Definitions, and Conventions *(Informative)*

3.1 Conventions *(Informative)*

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in Ref [3] RFC 2119.

3.2 Abbreviations and Acronyms (*Informative)*

API	Application Programming Interface
ASN	Access Service Network
CSN	Connectivity Service Network
GPS	Global Positioning System
M2M	Machine to Machine
NAP	Network Access Provider
NSP	Network Service Provider
PLC	Power Line Communication
QoS	Quality of Service

3.3 Definitions (*Informative)*

3.3.1 M2M ASN

The M2M ASN is an access service network that supports M2M service capability.

3.3.2 M2M CSN

The M2M CSN is a core service network that supports M2M service capability.

3.3.3 M2M Device

A WiMAX device that is capable to provide M2M service(s) and can communicate with M2M server.

3.3.4 M2M Features

The M2M Feature is a network capability to support a specific characteristic associated with M2M applications. One or more M2M features may be invoked in support of a M2M application.

3.3.5 M2M Group

The M2M Group is a group of M2M devices that has one or more M2M features that belong to the same M2M Subscriber.

3.3.6 M2M Server

A server that runs M2M applications.

3.3.7 M2M Service

The M2M Service provides functionalities that enable the M2M device to communicate with the M2M server, e.g. network access and rejection, waking up device, and device provisioning. The M2M network entity supports an interface that can be accessed by the M2M Device.

3.3.8 M2M Subscriber

A M2M Subscriber is a legal entity having a contractual relationship with the service provider to provide service to one or more M2M Devices.

3.3.9 WiMAX M2M System

The WiMAX M2M System is a WiMAX System that supports M2M features.

4 References

[1] 3GPP TS 22.368: "Service Requirements for Machine-Type Communications", stage 1, Rel 10.

[2] 3GPP TR 23.888: "System Improvements for Machine-Type Communications", stage 2, Rel 10.

[3] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”.

5 Use Cases (Informative)

5.1 Use Case 1 - Fleet Management

5.1.1 Short Description

Fleet Management application is defined as the remote monitoring of a vehicle fleet. It can be efficiently deployed using the WiMAX wireless technology.

5.1.2 Actors

John – a member of car sharing service.
WiCAR – a company which provides car sharing service to registered members.
WiMAX service provider.
Car alpha – one of the cars are owned by WiCAR.
Blackbox – securely located in car alpha.
Auto Management Server.

5.1.3 Pre-conditions

Car alpha has a built-in Blackbox. The Blackbox of car Alpha is equipped with WiMAX module which is certified in the network of WiMAX Service Provider and interworking with various car sensors that can identify an occurring event.

5.1.4 Post-conditions

The Blackbox sends information to the Auto Management Server. The information (e.g. GPS coordinate, tire pressure, odometer reading, etc) is used to track the car and car condition.

5.1.5 Normal Flow

1. John reserves the Car alpha either online or by telephone.
2. John goes to the location of the car and starts Car alpha.
3. The Blackbox performs device authentication over the WiMAX network for WiMAX access service.
4. As John drives the Car alpha, the Blackbox collects information (e.g. location, speed, car maintenance data, etc) and sends them periodically to the Auto Management Server in headquarter of WiCAR via the WiMAX network.
   Note: The Management server may send any information to the Blackbox.
5. John arrives at the destination and locks the Car alpha's. The trip information (e.g. driving time, miles, gas usage, etc) will then be transmitted to the Auto Management Server and the member's account is automatically charged.

5.1.6 Alternative Flow

1. A car moves out of the WiMAX coverage.
2. The WiMAX Module in the Blackbox fails to communicate to the Auto Management Server over the predefined intervals.
3. The WiMAX Module in the Blackbox waits until it is able to scan the WiMAX signal.
4. The car moves into the WiMAX coverage.
5. Once the WiMAX Module in the Blackbox senses that the WiMAX network is available, it sends the stored information to the Auto Management Server.

5.2 Use Case 2 - Vending machine

5.2.1 Short Description

Vending machine allows a customer to buy products such as soft drink, cigarette, and flower from the machine in a self service manner.

5.2.2 Actors

John – customer who wants to buy a drink.
Tommy – machine items supplier who wants to get paid for any goods dispensed.
WiMAX Service Provider.
Vending Machine.
Order Management Server.

5.2.3 Pre-conditions

Tommy runs several soft drink vending machines. The Vending machine shall only dispense a selected soft drink when the coin is inserted. The Vending machine is equipped with a WiMAX module which is certified in the network of WiMAX Service Provider and with various sensors that can identify an occurring event. The WiMAX module is activated and authorized successfully over the WiMAX Service Provider network. The availability of a particular item is based on the sensor of whether one item is still in place inside the vending machine.

5.2.4 Post-conditions

If a correct purchase has taken place, the Vending machine dispensed purchased merchandise.

5.2.5 Normal Flow

1. Once the machine detects that an item is out of stock, the Vending Machine reports “out of stock” to the Order Management Server.
2. The Order Management Server processed the info and sent an out of stock notification to Tommy. The Order Management Server may acknowledge the receiving of the notification.
3. Tommy restocks the Vending Machine.

5.2.6 Sub Flow

1. The Vending Machine stores daily sales data in its internal database.
2. At a pre-configured evening time, the Vending Machine sends a message (e.g. SMS, email or MMS) containing daily sale report to Tommy.
3. Tommy knows which products have been sold and the total daily revenue.

5.3 Use Case 3 - Smart Metering

5.3.1 Short Description

Smart Metering is used to monitor and control utilities (e.g. electricity, gas, and water) consumption. The Smart Meter collects utilities consumption in the house and provides usage information to a utility company.

5.3.2 Actors

John - a consumer who has an electricity subscription.
Smart Meter - an intelligent electricity metering device with WiMAX capability.
Utility Company.
Metering Server – a server is located in a utility company premise.

5.3.3 Pre-conditions

The Smart Meter is installed and configured to provide metering information periodically to the Smart Server located in the Utility Company. The Smart Meter is equipped with WiMAX module which is certified in the network of WiMAX Service Provider. The Smart Meter can communicate with the home appliances using various technologies (e.g. Bluetooth, Zigbee, Power Line Communication (PLC), WiMAX, WiFi, etc).

5.3.4 Post-conditions

The Smart Meter provides metering information to Metering Server and John can see the retrieved information from Metering Server.

5.3.5 Normal Flow

1. John bought a refrigerator and a washing machine which support green energy. The home appliances are PLC enabled ones.
2. John subscribed to a smart meter with the Utility Company.
3. The agent of Utility Company visited and installed a Smart Meter in John's house.
4. The Smart Meter starts communicating with the application of home appliances (e.g. the refrigerator and the washing machine) in his house via Power Line Communication.
5. The Smart Meter collects the information from the home appliances and sends the small bursts of information to Metering Server at preconfigured time over secure WiMAX network.

6. The smart meter can transmit emergency messages at any time and with a higher priority than preconfigured messages.

5.3.6 Sub Flow

1. John wants to monitor the electricity consumption in his house.
2. John logs in to the web portal of Utility Company via his PC or his mobile device.
3. John can see the consumption and cost data transmitted by Metering Server.

5.3.7 Alternative Flow

1. John bought a refrigerator and a wash machine which support green energy. Those appliances are certified by the Utility Industry.
2. John decided to apply for a smart meter subscription for power efficiency in his house.
3. The Utility Company agent visits and installs Smart Meter in John's house.
4. Smart meter starts communicating with the application of home appliances (e.g. the refrigerator and the wash machine) in the house via Power Line Communication.
5. The Smart Meter collects the information from the home appliances and sends the information to the Metering Server at preconfigured time.
6. The Smart Meter fails to send the information to Metering Server (e.g. can't get network access due to congestion or information lost).
7. The Smart meter re-sends the information when the air link is recovered.

5.4 **Use Case 4 - Surveillance Video**

5.4.1 Short Description

Surveillance Cameras are extensively used in the market, such as in home security, healthcare monitoring, outdoor security, to transmit wireless video to a server or a device. It allows for remote observation of objects. The wireless broadband connection can promise wider bandwidth to transmit multimedia contents in high quality.

5.4.2 Actors

John – a home owner.
Surveillance Camera.
WiMAX Service Provider.
WiMAX enabled Device.
SiCom server – located in home or Home Security Company.

5.4.3 Pre-conditions

Surveillance Camera was installed in home environment. The Surveillance Camera is equipped with WiMAX module which is certified in the network of WiMAX Service Provider. It is also equipped with a motion sensor that can sense an object's movement. The Camera will be ON, either continuously or when it detects an object within the environment. The relevant

surveillance application is running on a WiMAX enabled Device to control the surveillance camera.

5.4.4 Post-conditions

Surveillance Camera transmits wirelessly and securely video stream. The video is stored in the SiCom server for monitoring by the Home Security Company.

5.4.5 Normal Flow

1. John has installed Surveillance Cameras in his home and set it as "always-on" mode. John configured the destination of video streaming with the address of SiCom server.
2. The WiMAX module is activated and authorized over WiMAX Service Provider network.
3. The video recorded by Surveillance Camera is transmitted to the SiCom server in real time.
4. John wants to observe the home environment while he is away. John invokes security application on his device (e.g. mobile terminal, Laptop, etc) and the device is connected to the SiCom server.
5. The SiCom server forwards the video to John's device and adopts the encoding rate based on device capability.
6. John is watching the optimized video of his home environment.

5.4.6 Sub Flow

1. John has changed the mode as "away event" when leaving for work.
2. The Camera is automatically turned off and activates movement sensor.
3. The sensor detects a movement in a room.
4. The Camera is turned ON then sends an alarm notification to the SiCom server or pre-configured address.

5.4.7 Alternative Flow

1. John has installed Surveillance Cameras in his home and set it as "always-on" mode. John manually configured the destination of video streaming with the address of SiCom server.
2. The WiMAX module is activated and authorized over WiMAX Service Provider network.
3. The video recorded by Surveillance Camera is transmitted to the SiCom server in real time.
4. John wants to observe home environment while he is away. John invokes the security application on his device (e.g. mobile terminal, Laptop, etc) and the device is connected to SiCom server.
5. The video quality becomes poor due to congestion in the WiMAX network of the Service Provider.
6. The Surveillance Camera receives the updated QoS attributes from the SiCom server or from the WiMAX network and adopts a lower video quality.

7. After some time, the congestion eases. The SiCom server provides another QoS attributes update to the Surveillance Cameras.
8. The Surveillance Camera receives the updated QoS attributes from the SiCom server or from the WiMAX network and adopts a higher video quality.

5.5 Use Case 5 – Remote Diagnostics (Informative)

5.5.1 Short Description

Monitor and analyze patient's medical status during the way to the hospital for emergency treatment.

5.5.2 Actors

John – Patient who needs emergency treatment.
Tommy - Doctor waiting in the hospital.
WiMAX Service Provider.
Ambulance equipped with WiMAX enabled medical devices.
Hospital server.

5.5.3 Pre-conditions

Ambulance equipped with WiMAX enabled medical devices measures electro-cardiograph and other medical data while the ambulance is moving towards hospital. These medical devices send John's medical status to medical server located in the hospital. John's medical information is sent to the relevant doctors for immediate treatment and Tommy prepares emergency treatment applicable to John's current medical status. As John arrives hospital, Tommy starts instant treatment as prepared.

5.5.4 Post-conditions

After the emergency treatment, medical server saves patient's medical information and this information are used for future treatment.

5.5.5 Normal Flow

1. Medical data is sent through WiMAX network.
2. Data size sent is usually very large and requires high uplink throughput.
3. Data needs to be sent in vehicular condition which requires seamless connection with fast mobility.

5.5.6 Sub Flow

1. Medical data is saved in Hospital Server.
2. Saved medical data is used for future treatment.

5.6 Use Case 6 – Traffic Information

5.6.1 Short Description

Bus Management System (BMS)/Bus Information System (BIS) provides real-time arrival information of buses in each bus stop.

5.6.2 Actors

John – Passenger waiting for bus.
Bus A – Bus with BMS/BIS terminal.
WiMAX Service provider.
BMS/BIS terminal with WiMAX and GPS enabled.
BMS/BIS server located in the bus company.
Bus stop with a WiMAX enabled display showing the estimated arrival time of buses.

5.6.3 Pre-conditions

BMS/BIS terminal is installed in each bus. BMS/BIS terminal is equipped with WiMAX module which is certified in the network of WiMAX Service provider, and GPS module which can track the exact location of BMS/BIS terminal.

5.6.4 Post-conditions

BMS/BIS terminal sends GPS coordinate to BMS/BIS server located in the bus company.
BMS/BIS server sends estimated arrival time of the bus to the bus top which has WiMAX enabled display.

5.6.5 Normal Flow

1. BMS/BIS terminal receives exact coordinate via GPS module.
2. BMS/BIS terminal sends GPS coordinate to BMS/BIS server via WiMAX Service Provider.
3. BMS/BIS server receives coordinate information of Bus A.
4. BMS/BIS server sends estimated arrival time of Bus A to the Bus stop.
5. John is informed when Bus A will arrive.

5.7 Use Case 7 – Mobile Payment

5.7.1 Short Description

Mobile Payment allows credit card payment at any location within WiMAX coverage.

5.7.2 Actors

John – Customer who wants to make a payment.

Tommy – Delivery service person with a WiMAX enabled credit card checker.
Credit card checker provided with a WiMAX M2M capabilities.
WiMAX Service Provider.
Billing server located in the credit card company.

5.7.3 Pre-conditions

John needs to make payment for item ordered out from his office. John does not have enough money but carries his credit card. Tommy delivers ordered item to John and asks for the payment. Payment is made with credit card checker equipped with WiMAX module which is certified in the network of WiMAX Service Provider. Credit card information is sent to billing server located in credit card company. Billing server checks credit card information and makes authentication for the credit card.

5.7.4 Post-conditions

After Billing server authorizes payment, a receipt is issues to John.

5.7.5 Normal Flow

1. Credit card checker reads credit card information.
2. Credit card checker sends credit card information via WiMAX Service Provider.
3. Billing server receives credit card information from the WiMAX SP.
4. Billing server confirms credit card payment and informs credit card checker.
5. Receipt is issued from credit card checker.

6 Machine to machine communication Aspects (Informative)

6.1 M2M Applications

The list of M2M applications depends on the vertical market where they are adopted.

Industry	Example application	Description
Transportation/Automotive	Vehicle/Asset Tracking	This category includes public and private transportation business. The example of public transportation business is bus and train operators. The example of private transportation is equivalent to logistics.(e.g. DHL, etc)
Security & Safety	Home Alarm, Surveillance	This category includes CCTV cameras and other remote sensors that may monitor the presence of

		person or functions of equipment.
Smartgrid and Smart Metering	Electricity, Gas, Water, industrial metering	This category includes metering applications provided by utilities operators.
Healthcare	Monitoring vital signs, Remote diagnostics, supporting of seniors or handicapped	This category includes hospitals and other entities applications that provide healthcare services either their premise or remotely.
Remote Management/Control	Industrial Automation, Vending machine, Elevator control, Traffic Lighting, Flood management, Telemetry	This category includes manufacturing, in-vehicle, in-building and roadside machines.
Telematics	Roadside assistance & remote diagnosis	This category includes automobile systems that combine Global Positioning System (GPS) technology and other wireless communication systems for automatic roadside assistance and remote diagnostics
Mobile Payment	Credit card or debit card payment	This category includes the street meter post payment, the vending machine payment and credit card swipe for any wireless payment.

6.2 M2M Features

6.2.1 Low Mobility Feature

The Low Mobility feature is used by the M2M Devices that are configured in a fixed location or move within a specific defined geographic distance.

6.2.2 Time Controlled Feature

The Time Controlled feature is used by the M2M Devices that are configured to send or receive data only at certain pre-defined access time and avoid unnecessary signalling outside this pre-defined access time.

6.2.3 Monitoring Feature

The Monitoring feature is used by the M2M devices to inform the network of tampering or damage to the M2M device.

6.2.4 Small Data Transmission Feature

The Small Data Transmissions is used by the M2M Devices that send or receive small data bursts.

6.2.5 Low Power Consumption Feature

Low power consumption is used for M2M device that are designed to have low operational power over long periods of time. This feature is required for example for battery-limited M2M devices, i.e., those that have no access to power sources or those with infrequent human interaction so that replacement of the battery is costly or not feasible.

6.3 M2M Communication with M2M Server Scenarios

6.3.1 M2M server(s) operated by the WiMAX Operator

The M2M server may reside in the M2M CSN. In communication scenarios where the M2M sever resides in the CSN, the WiMAX operator (the same NAP & NSP) is responsible for deploying the M2M communication services and thus, the M2M server will offer the web portal interface for the M2M subscriber (M2M application) as shown in Figure 1.

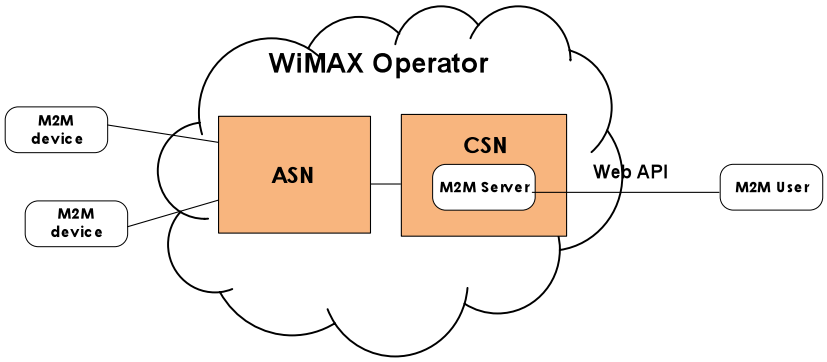

Figure 1: M2M device communicates with M2M server within CSN.

6.3.2 M2M Server not operated by the WiMAX Operator

In communication scenarios where the M2M server resides outside the CSN, the WiMAX operator provides optimized data transport for the M2M device. The M2M operator may

deploy M2M communication service as shown in Figure 2. Note: the M2M Server may be operated by a separate operator; therefore, a standardized API will be needed to interconnect the M2M Server and the CSN network entity.

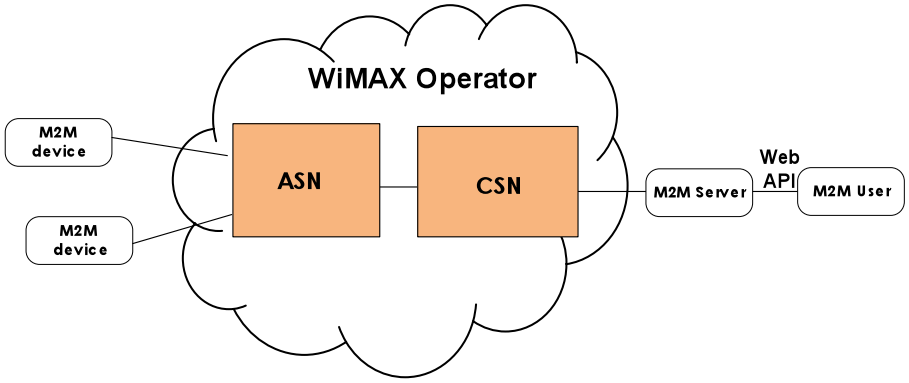

Figure 2: M2M device communicates with M2M server outside CSN.

7 Requirements (Conditional Normative)

7.1 Service Requirements

7.1.1 General Requirements

[R-001] The WiMAX M2M Service SHALL support point to point communication from the WiMAX M2M Server to the M2M Device.

[R-002] The WiMAX M2M Service SHALL support point to point communication from the WiMAX M2M Device to the M2M Server.

[R-003] The WiMAX M2M Service SHOULD support point to multipoint communication from the WiMAX M2M Server to the M2M Device or M2M Group.

[R-004]The WiMAX M2M Service MAY support point to multipoint communication from the WiMAX M2M Device to the M2M Server.

[R-005] The M2M device SHALL be able to use one or more M2M Features for a given M2M Application.

[R-006] The WiMAX M2M Service SHALL provide a mechanism for the network operator to restrict the usage of each M2M Feature.

[R-007] The WiMAX M2M Service Provider SHALL be able to control M2M service access initiated either by the M2M Server or By M2M Devices.

[R-008] The WiMAX System SHALL support different priority levels for M2M Application traffic (e.g., alarm message).

[R-009] The WiMAX M2M Service SHALL inform the subscriber or a designated party of the enabled/disabled status of any M2M feature.

R-[010] The WiMAX M2M Service SHALL be able to inform the subscriber or designate party of status of any M2M feature.

7.1.2 Naming, identification and Addressing Requirements

[R-011] The WiMAX Network SHALL be able to identify each M2M Device and its M2M Group if configured.
Note: The device identity within the WiMAX Network should be identified based on MAC address of the device.

[R-012] A M2M Device SHALL be able to subscribe to one or more M2M Groups.

[R-013] The M2M device SHALL have unique identifier in the WiMAX Network.

[R-014] Communication with a M2M Device that has either private non-routable IPv4 address or public IPv4 or IPv6 address SHALL be supported.

7.2 Functional Requirements

7.2.1 System Requirements

[R-015] The M2M Subscriber SHOULD be allowed to subscribe to multiple M2M features (e.g. Time Control and Low Mobility).

[R-016] The WiMAX Network SHALL be able to activate and provision M2M Service on a particular M2M Device.

[R-017] The WiMAX Network SHALL be able to de-activate and de-provision M2M Service on a particular M2M Device.

[R-018] The WiMAX Network SHALL provide a mechanism to reduce network congestion or overload from large numbers of M2M Devices simultaneously or near simultaneously attempting data or signaling transmission. For example:

- Air interface access control

- Core Network access control
- M2M Server access control
- Universal Service Interface access control

[R-019] The M2M device MAY notify the M2M Server of its connection preference (e.g. maintain the L1/L2 or L3 connection or discard the L1/L2/L3 connection when not interacting with the M2M Server). Note: It is assumed when in idle mode, the default is to maintain the L3 connection.

[R-020] Based on a trigger indication from the M2M Server, the M2M System SHALL support a mechanism to trigger the M2M Device to initiate communication (i.e. network initiate or mobile initiate method) with the M2M Server.

7.2.2 Low Mobility Requirements

[R-021] The WiMAX M2M System SHALL support the capability to reduce the frequency of mobility management traffic.

[R-022] The WiMAX M2M Service SHALL enable the M2M service provider to define the frequency of location updates performed by the M2M Device.

[R-023] The WiMAX M2M service provider SHALL be able to define mobility configuration (e.g. fixed, low mobility, high mobility) for each M2M Device.

7.2.3 Time Controlled Requirements

[R-024] The WiMAX M2M Service SHALL be able to restrict service access (e.g. WiMAX network (re)entry or setup data connection) to be available only on certain defined time.

[R-025] The WiMAX M2M Service SHALL be able to restrict access by terminating the connection (e.g. de-registration or release of a data connection) at the end of defined access time periods.

[R-026] The WiMAX M2M Service SHALL support the modification of the defined access time periods for the M2M Device.

[R-027] The WiMAX M2M Service SHALL be able to reject access requests outside the defined access time periods.

7.2.4 Monitoring Requirements

[R-028] The WiMAX M2M Device SHALL report the event that may indicate possible theft (e.g. removing of WiMAX SIM) or damage.

[R-029] The WiMAX M2M Service SHALL be able to define which monitoring events to detect (e.g. change of location, unable to connect to the M2M device).

[R-030] The M2M Subscriber MAY select one or more of the available follow-up actions to be performed by the system when an event is detected.

7.2.5 Small Data Transmission Requirements

[R-031] The WiMAX system SHALL support the transmission of small data bursts while reducing signaling overhead, network resource allocation and establishment.

[R-032] The WiMAX M2M service provider SHALL be able to configure the maximum size of small data burst transmitted to the M2M device.

7.2.6 Low Power Consumption Requirements

[R-032] The WiMAX M2M System SHALL support a mechanism to save power consumption on M2M devices that are designed for low power consumption (e.g. invoke idle and sleep mode of operation).

7.3 Roaming Requirements

[R-034] The M2M subscriber SHOULD have similar user experience of subscribed M2M feature when roaming while utilizing WiMAX Service.

7.4 Accounting and Management Requirements

7.4.1 Accounting Requirements

[R-035] The M2M System MAY be able to count M2M Device initiated signaling per signaling type (e.g. mobility signaling such as location update, connection set up signaling, M2M feature activation/de-activation).

[R-036] The M2M System SHALL be able to generate bearer accounting information per M2M device or group based on the criteria in the M2M feature subscription (e.g. volume, time of day, location).

7.4.2 Operation and Management Requirements

[R-037] The WiMAX Network SHALL support over the air activation and provisioning of M2M Device.

[R-038] The WiMAX Network SHALL support over the air de-activation and de-provisioning of M2M Device.

[R-039] The WiMAX M2M Server SHALL support mechanism for the M2M Device to activate and deactivate M2M Features e.g. over the air or web-based.

7.5 Security Requirements

[R-040] The WiMAX System SHALL support the M2M Device only authentication.

[R-041] The WiMAX Network SHALL support integrity protection and privacy of M2M application traffic which requires secure connection e.g. NIST (National Institute of Standard Technology) Action Plan 2 for Wireless standards for Smart Grid.

7.6 Regulatory Requirements

Lawful Interception must always be done in accordance with the applicable national/regional laws and technical regulations.

R-[042] WiMAX M2M Service implementation SHALL comply with the Lawful Intercept requirements of [Recommendation and Requirements for Networks based on WiMAX Forum Certified Products, 080717_SPWG_Req_Release_1.5.doc].

R-[043] The WiMAX network SHALL be able to perform lawful intercepts based on identification of specific M2M devices, M2M groups defined in the WiMAX network, or the subscriber of a WiMAX M2M Service.

8 Guidance and Recommendation to other WiMAX WGs

GR-[001] It is recommended the WiMAX Network has a single web API between the M2M server and the M2M User.

GR-[002] The M2M System NEED to support an efficient signaling architecture, which may change the existing signalling procedures designed for the use by the mass market.

Annex A Document History (*Informative)*

Date	Subject History	Version
2009-12-10	Initial template	A
2010-01-06	Revised template, contribution 10_00006 and 10_00005R1	B
2010-01-26	Incorporated contributions 10_00014R1, 10_00015R1, and 10_00016R1	C
2010-03-04	Incorporated contribution 10_00041R1	D
2010-03-24	Incorporated contribution 10_00068R1 and 10_00069R1	E
2010-04-14	Incorporated contribution 10_00080R1	F
2010-06-09	Incorporated contribution 10_00090R1	G

2010-06-24	Incorporated contribution 10_00099R1, 10_00100, 10_00101R1, 10_00102R2, 10_00108R2, 10_00109R1,	H
2010-08-12	Incorporated contribution 10_00125R2	I
2010-09-08	Incorporated contribution 10_00127R1, add acronyms	J
2010-09-20	Incorporated contribution 10_00129R1	K
2010-09-24	Incorporated modification of 10_00133	L
2010-11-02	Incorporated accepted ballot comments	M
2010-11-30	Incorporated TSC and SPWG plenary comments	N

1

2