White Paper

on

“Machine-to-Machine Communication (M2M)”

INDEX

Machine-to-Machine Communication (M2M)

1. Introduction

Machine-to-Machine (M2M) communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. M2M is also named as Machine Type Communication (MTC) in 3GPP. It is different from the current communication models in the ways that it involves:

- new or different market scenarios
- lower costs and effort
- a potentially very large number of communicating terminals
- little traffic per terminal, in general

M2M communication could be carried over mobile networks (e.g. GSM-GPRS, CDMA EVDO networks). In the M2M communication, the role of mobile network is largely confined to serve as a transport network.

With a potential market of probably 50 million connected devices, M2M offers tremendous opportunities as well as unique challenges. These devices vary from highly-mobile vehicles communicating in real-time, to immobile meter-reading appliances that send small amounts of data sporadically.

2. Applications of M2M

The applications of M2M cover many areas and the areas in which M2M is currently used are given below:

a. **Security :** Surveillances, Alarm systems, Access control, Car/driver security

b. **Tracking & Tracing :** Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering

c. **Payment :** Point of sales, Vending machines, Gaming machines

d. **Health :** Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics

e. **Remote Maintenance/Control :** Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics

f. **Metering :** Power, Gas, Water, Heating, Grid control, Industrial metering

g. **Manufacturing :** Production chain monitoring and automation

h. **Facility Management :** Home / building / campus automation

3. Key features of M2M

Some of the key features of M2M communication system are given below:

a. **Low Mobility** : M2M Devices do not move, move infrequently, or move only within a certain region

b. **Time Controlled** : Send or receive data only at certain pre-defined periods

c. **Time Tolerant** : Data transfer can be delayed

d. **Packet Switched** : Network operator to provide packet switched service with or without an MSISDN

e. **Online small Data Transmissions**: MTC Devices frequently send or receive small amounts of data.

f. **Monitoring**: Not intend to prevent theft or vandalism but provide functionality to detect the events

g. **Low Power Consumption** : To improve the ability of the system to efficiently service M2M applications

h. **Location Specific Trigger** : Intending to trigger M2M device in a particular area e.g. wake up the device

4. Architecture and components of M2M

Figure 1 shows a simple architecture of M2M systems with its components. The various components and elements of an M2M system are briefly described below:

a. **M2M Device**: Device capable of replying to request for data contained within those devices or capable of transmitting data autonomously.

Sensors and communication devices are the endpoints of M2M applications. Generally, devices can connect directly to an operator’s network, or they will probably interconnect using WPAN technologies such as ZigBee or Bluetooth. Backhaul to an operator’s network is than achieved via gateways that encapsulate and manage all devices. Consequently, addressing and identifying, *e.g.*, routing, of the devices relies heavily on the gateways. Devices that connect via gateways are normally outside the operator’s responsibility but belong to M2M applications that are provided by service or application providers.

Sensors and devices that connect directly into an operator’s network (via embedded SIM, TPM and radio stack or fixed line access) are endpoints of the network. Thus, the responsibility in terms of accountability, SLAs etc., lies within the network operator (or virtual network operator). This holds true especially with respect to TPM where it is necessary to ensure that the module is really that reliable and well protected.

b. **M2M Area Network (Device Domain)**: Provide connectivity between M2M Devices and M2M Gateways, e.g. personal area network.

c. **M2M Gateway**: Equipment that uses M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.

Gateways and routers are the endpoints of the operator's network in scenarios where sensors and M2M devices do not connect directly to the network. Thus, the task of gateways and routers are twofold. Firstly, they have to ensure that the devices of the capillary network may be reached from outside and vice versa. These functions are addressed by the access enablers, such as identification, addressing, accounting etc., from the operator's platform and have to be supported at the gateway's side as well.

Thus, platform and gateway form a distributed system, where generic and abstract capabilities are implemented on the gateway's side. Consequently, there will be a control flow between gateway and operator's platform that has to be distinguished from the data channel that is to transfer M2M application data. Secondly, there may be the need to map bulky internet protocols to their lightweight counterpart in low-power sensor networks. However, the latter application might lose its relevance since there are implementations of IPv6 for sensor networks available, that allow an all-IP approach.

d. **M2M Communication Networks (Network Domain)**: It covers the communications between the M2M Gateway(s) and M2M application(s), e.g. xDSL, LTE, WiMAX, and WLAN.

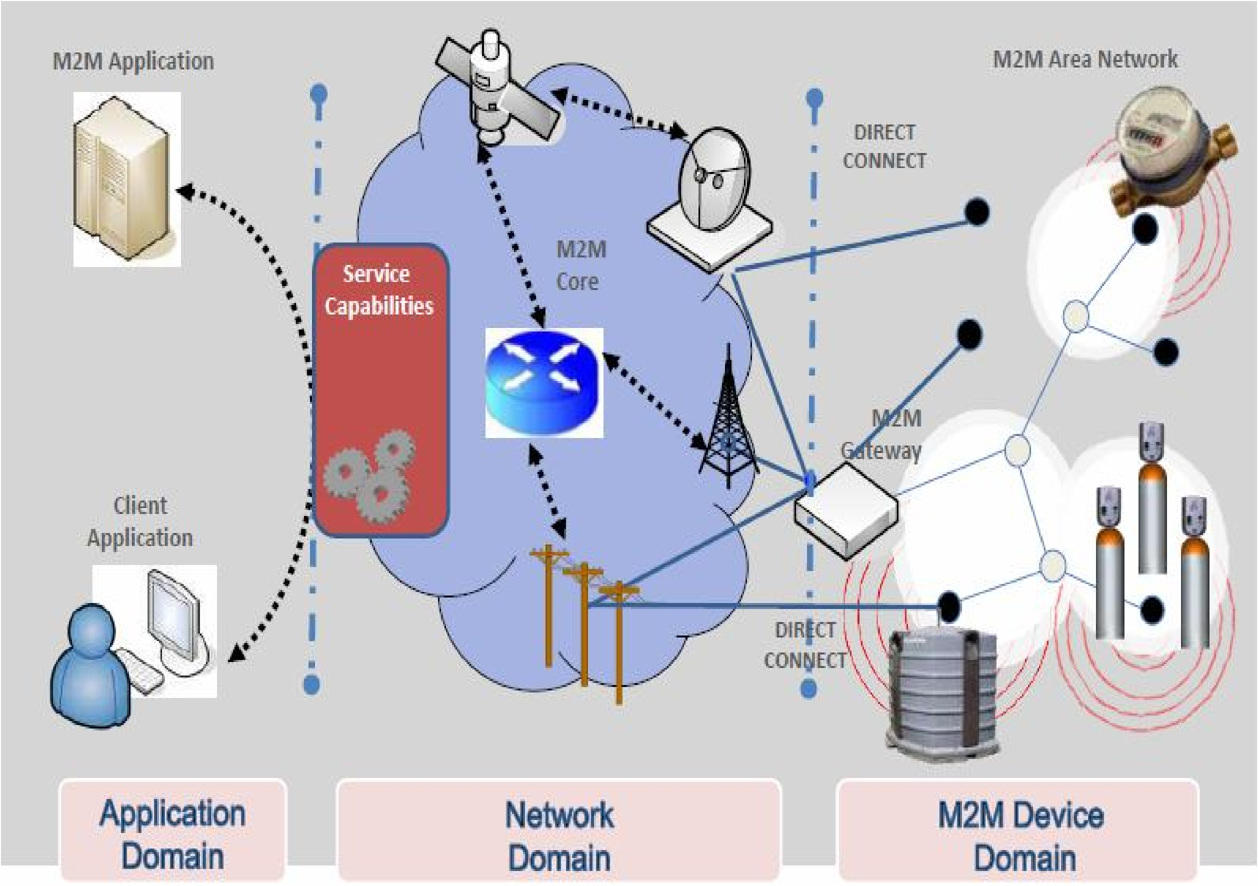

Figure 1: Architecture of M2M system

e. **M2M Applications**: It contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

M2M applications will be based on the infrastructural assets (*e.g.*, access enablers) that are provided by the operator. Applications may either target at end users, such as user of a specific M2M solution, or at other application providers to offer more refined building blocks by which they can build more sophisticated M2M solutions and services. e.g. customer care functionality, elaborate billing functions, etc. Those services, or service enablers, may be designed and offered by an application provider, but they might be offered by the operator via the operator platform itself.

Figure 2 shows the M2M system with examples of various components and applications.

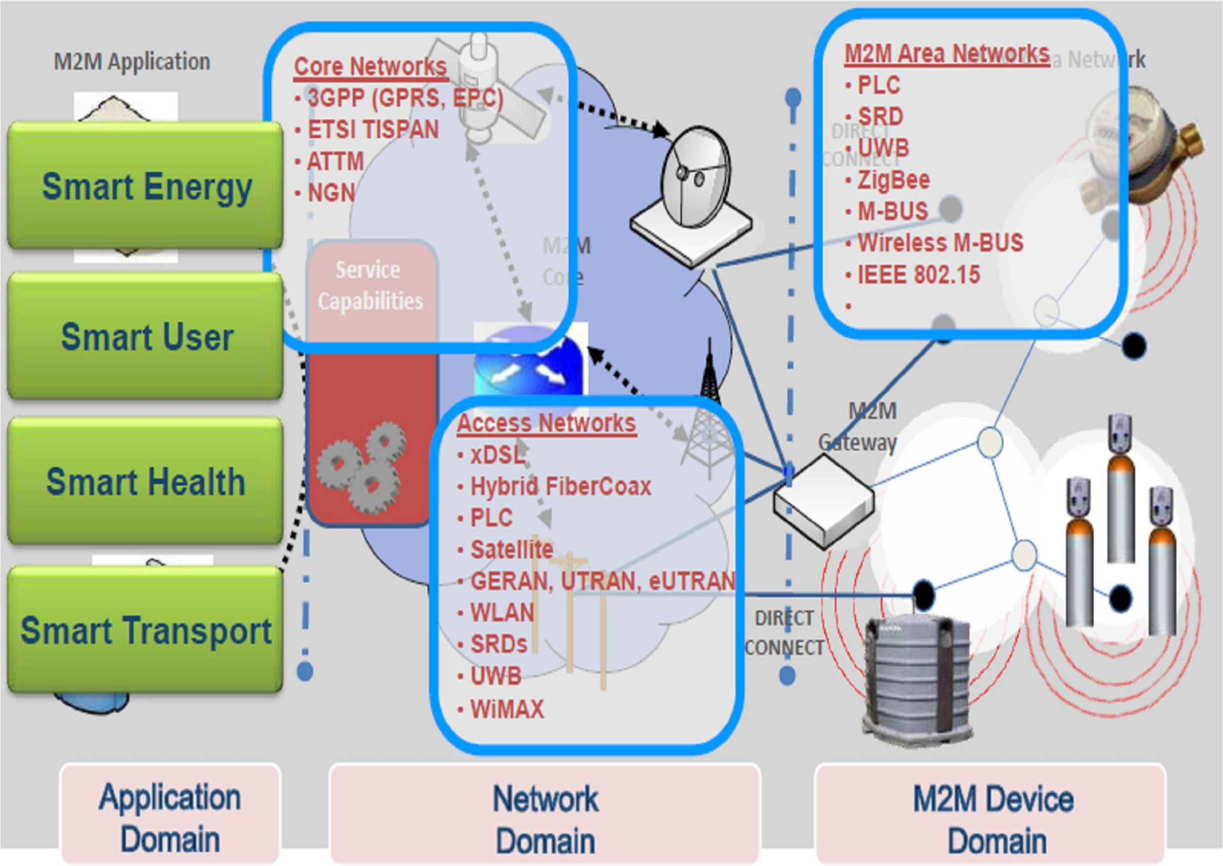

Figure 2: Examples of components of M2M system

5. Requirements for M2M

Some of the general requirements for the M2M System, as specified by ETSI, are given below.

a. **M2M Application communication principles:** The M2M system shall be able to allow communication between M2M Applications in the Network and Applications Domain, and the M2M Device or M2M Gateway, by using multiple communication means, e.g. SMS, GPRS and IP Access. Also a Connected Object may be able to communicate in a peer-to-peer manner with any other Connected Object. The M2M System should abstract the underlying network structure including any network addressing mechanism used, e.g. in case of an IP based network the session establishment shall be possible when IP static or dynamic addressing is used.

b. **Message Delivery for sleeping devices**: The M2M System shall be able to manage communication towards a sleeping device.

c. **Delivery modes** : The M2M System shall support anycast, unicast, multicast and broadcast communication modes. Whenever possible a global broadcast should be replaced by a multicast or anycast in order to minimize the load on the communication network.

d. **Message transmission scheduling**: The M2M System shall be able to manage the scheduling of network access and of messaging. It shall be aware of the scheduling delay tolerance of the M2M Application.

e. **Message communication path selection**: The M2M System shall be able to optimize communication paths, based on policies such as network cost, delays or transmission failures when other communication paths exist.

f. **Communication with devices behind a M2M gateway**: The M2M System should be able to communicate with Devices behind a M2M gateway.

g. **Communication failure notification**: M2M Applications, requesting reliable delivery of a message, shall be notified of any failures to deliver the message.

h. **Scalability:** The M2M System shall be scalable in terms of number of Connected Objects.

i. **Abstraction of technologies heterogeneity**: The M2M Gateway may be capable of interfacing to various M2M Area Network technologies.

j. **M2M Service Capabilities discovery and registration**: The M2M System shall support mechanisms to allow M2M Applications to discover M2M Service Capabilities offered to them. Additionally the M2M Device and M2M Gateway shall support mechanisms to allow the registration of its M2M Service Capabilities to the M2M system.

k. **M2M Trusted Application**: The M2M Core may handle service request responses for trusted M2M Applications by allowing streamlined authentication procedures for these applications. The M2M system may support trusted applications that are applications pre-validated by the M2M Core.

l. **Mobility:** If the underlying network supports seamless mobility and roaming, the M2M System shall be able to use such mechanisms.

m. **Communications integrity**: The M2M System shall be able to support mechanisms to assure communications integrity for M2M services.

n. **Device/Gateway integrity check**: The M2M System shall support M2M Device and M2M Gateway integrity check.

o. **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 Core.

p. **Confirm:** The M2M System shall support mechanisms to confirm messages. A message may be unconfirmed, confirmed or transaction controlled.

q. **Priority:** The M2M System shall support the management of priority levels of the services and communications services. Ongoing communications may be interrupted in order to serve a flow with higher priority (i.e. pre-emption).

r. **Logging:** Messaging and transactions requiring non-repudiation shall be capable of being logged. Important events (e.g. received information from the M2M Device or M2M Gateway is faulty, unsuccessful installation attempt from the M2M Device or M2M Gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.

s. **Anonymity:** The M2M System shall be able to support Anonymity. If anonymity is requested by an M2M Application from the M2M Device side and the request is accepted by the network, the network infrastructure will hide the identity and the location of the requestor, subject to regulatory requirements.

t. **Time Stamp**: The M2M System shall be able to support accurate and secure and trusted time stamping. M2M Devices and M2M Gateways may support accurate and secure and trusted time stamping.

u. **Device/Gateway failure robustness**: After a non-destructive failure, e.g. after a power supply outage, a M2M Device or Gateway should immediately return in a full operating state autonomously, after performing the appropriate initialization e.g. integrity check if supported.

v. **Radio transmission activity indication and control:** The radio transmitting parts (e.g. GSM/GPRS) of the M2M Device/Gateway should be able to provide (if required by particular applications e.g. eHealth) a real-time indication of radio transmission activity to the application on the M2M Device/Gateway, and may be instructed real-time by the application on the M2M Device/Gateway to suspend/resume the radio transmission activity.

6. Issues /concerns in M2M

The key concerns in M2M are related to addressing and security.

The M2M System should be flexible in supporting more than one naming scheme. Also it should support identification of connected objects or groups of connected objects by their names, temporary id, pseudonym (i.e. different names for the same entity), location or combination thereof (e.g. URIs or IMSI). It shall be possible to reuse names for certain classes of devices or for devices operating in certain (i.e. resource constrained) environments. The addressing schemes should include:

- IP address of connected objects.
- IP address of group of connected objects (including multicast address).
- E.164 addresses of connected objects (e.g. MSISDN).

It is expected that M2M devices would typically operate unmanned and unguarded by humans and thus are subject to increased levels of security threats, such as physical tampering, hacking, unauthorized monitoring, etc. Terminal devices may also get geographically dispersed over time. Such M2M devices should therefore provide adequate security to detect and resist attacks. Devices may also need to support remote management including firmware updates to correct faults or recover from malicious attacks. Some M2M Equipments (M2Mes) are typically required to be small, inexpensive, able to operate unattended by humans for extended periods of time, and to communicate over the wireless area network (WAN) or WLAN. M2Mes are typically deployed in the field for many years, and after deployment, tend to require remote management of their functionality. It is likely that M2Mes will be deployed in very large quantities, and many of them will also be mobile, making it unrealistic or impossible for operators or subscribers to send personnel to manage or service them. These requirements introduce a number of unique security vulnerabilities for the M2Mes and the wireless communication networks over which they communicate.

7. Standardization Efforts for M2M

Today's telecoms networks are designed mainly for human to human communication. At present for human to machine and machine to machine communication standardization are limited to standalone system not involving the mobile networks and other general transport models. In order to deliver effective M2M solutions and to allow the market to take off, efforts in the direction of standardizations to involve the existing technologies are taken up by various SDOs.

ETSI's has been established Machine-to-Machine Communications Technical Committee (TC M2M) to develop these necessary standards. TC M2M aims to bring disjointed component-level standards together, and to fill the standardisation gaps. It is developing an end-to-end architecture to support multiple machine-to-machine type applications.

The main gap currently being addressed is the development of a 'horizontal' platform which is application-agnostic but which, with its evolved functionality, is capable of supporting a very wide range of services, including smart metering, eHealth, city automation, consumer applications and car automation. An ETSI Technical Report (TR) outlining potential 'use cases' is being prepared for each of these five areas, which will eventually be used to verify the specification. The TR on smart metering was published in May 2010 and the work continues on the other four.

Significant progress on two technical specifications was made in 2010. The first includes the detailed specification of M2M functional architecture, covering all the new functionality (service capabilities) required to support M2M services, identification of the new interfaces required and the overall data model. In particular it also includes a security solution appropriate to M2M service needs. The second technical specification provides the first detailed specification of the necessary interfaces, in the form of a formal definition of the Application Programming Interface (API) and of the required parameters. The first full release of M2M specifications is expected to be completed by the end of 2011.

The standardization efforts in ITU are being addressed under various banners like ‘Internet of Things (IoT)’, ‘Machine to Machine (M2M) communication’, ‘Machine-oriented communication (MOC)’, ‘Smart ubiquitous networks (SUN)’, ‘Ubiquitous sensor networks (USN)’, etc.

Draft Recommendation ITU-T Y.IoT-overview “Overview of Internet of Things” covers the Introduction of IoT, Objectives of IoT, Characteristics of IoT, Ecosystem and business models for IoT, High level reference models of IoT, and Candidate study areas of IoT standardization.

Draft Recommendation Y.MOC-Reqts “Requirements for support of machine oriented communication applications in the NGN environment” covers extensions and additions to NGN capabilities in order to support machine oriented communication (MOC) applications in the NGN environment. The scope of this Recommendation includes:

- Service overview, description of MOC ecosystem and key supporting features of MOC applications
- Service requirements to support MOC applications
- Requirements of extended or new NGN capabilities based on the MOC service requirements
- Reference framework for MOC capabilities.

8. Conclusion

M2M as an application holds the promise of bringing benefit to both telecom operators and vendors. For service providers it is an opportunity as low-bandwidth M2M services can be readily overlaid onto the current user services network. Vendors are expected to profit from selling both M2M-capable devices, and from the network expansion brought about by increased throughput.

However, it comes with change in business model and value chain. There are questions regarding the role of operators in the value chain. Also, M2M services may have their own specific characteristics which might be different from services in which humans directly influence communication flow. The standardization in the direction of special handling or optimization of the network for M2M specific service will lead for better support of M2M communications.

Glossary

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
API	Application Programming Interface
ETSI	European Telecommunications Standards Institute
M2M	Machine to Machine Communication
MTC	Machine Type Communication
TC M2M	Machine-to-Machine Communications Technical Committee
TPM	Trusted Platform Module
TR	Technical Report