SOURCE : ETSI Input to TIA for the NNT on M2M for GSC-14

1. Introduction

ETSI TC M2M aims to build a first step towards the "Internet of Things," called "the Internet of Connected Machines."

2. Functional components of the framework

The high level illustration of M2M systems and of its components as given in the Figure 1:

A M2M service domain that is composed of the M2M core and M2M applications. M2M core provides a set of functionalities that will allow services to be developed in an efficient way for delivering the M2M services, *e.g.,* naming and addressing, mobility management, device management, service control and application interaction, charging, QoS control services and security aspects. Functionalities of the M2M core may be provided by the network operator. M2M applications utilize the capabilities provided by the M2M Core, to provide M2M services.

The functional components of the high level architecture may be isolated and abstracted as depicted in Figure 2. A M2M system comprises M2M devices, such as sensors or devices that may even encapsulate some application logic additional to sensor or actuator capabilities. It is common that these devices are encapsulated by gateways that offer different abstraction layers (SOA or protocol-based) to access the devices.

The operator platform should offer functionalities, *e.g*., services that allow M2M applications to access, manage and configure devices and gateways. These services act as enablers, since they enable third parties such as service providers, to offer services based on the functionality of the operator platform. These services will be referred to as access enablers.

Similarly, an operator may provide services that facilitate the creation of new services for services or application provider, *e.g.,* to facilitate the billing process.

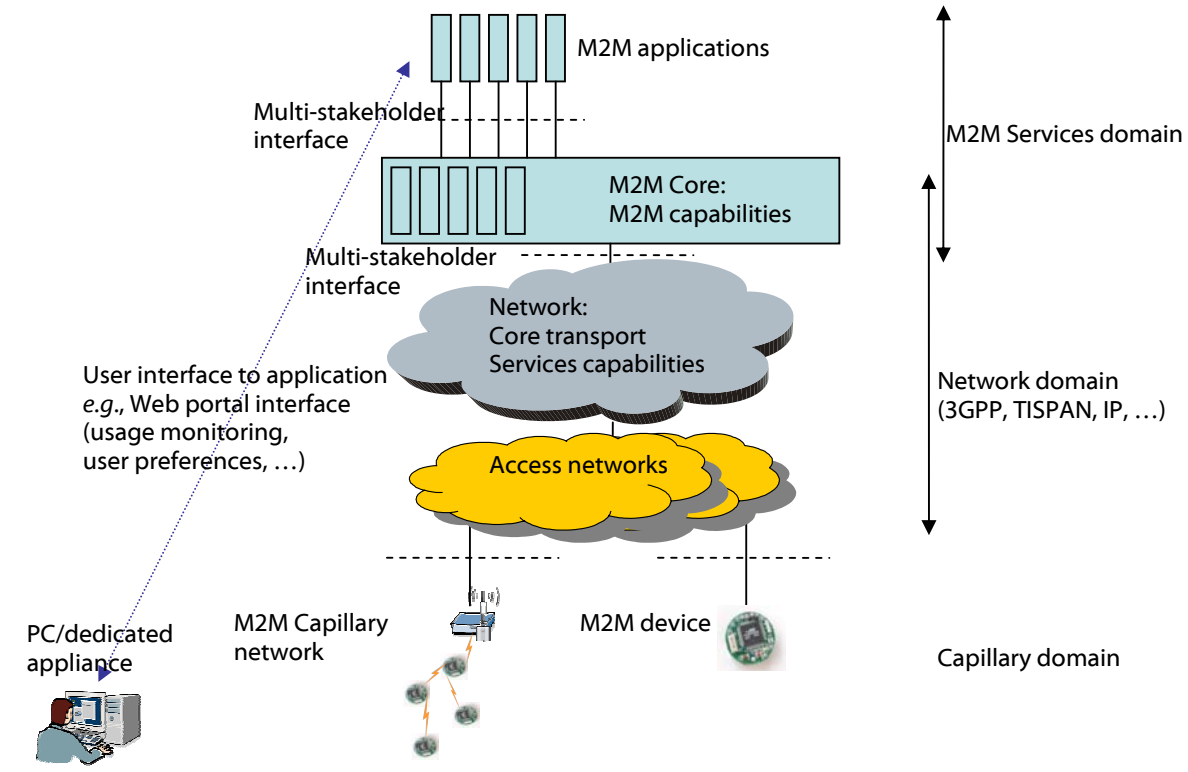

Figure 1: High level system architecture

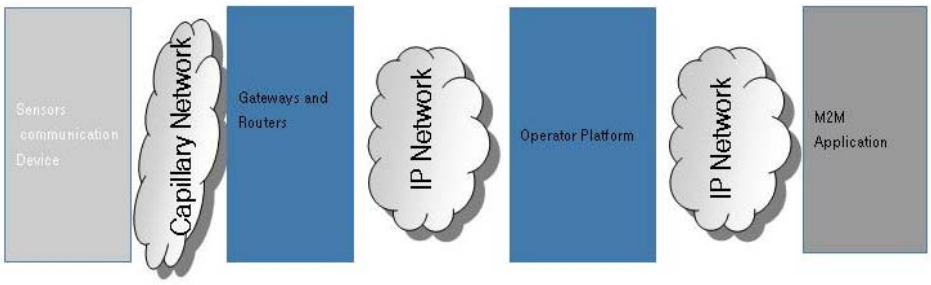

Figure 2: M2M System Abstraction

2.1. Sensors and communication devices

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. Thus, the compliance to specifications that allows mobility etc., has to be assured by those providers accordingly.

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.

2.2. Gateways and routers

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 form 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 loose its relevance since there are implementations of IPv6 for sensor networks available, that allow an all-IP approach.

2.3. M2M Applications

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. Examples might include customer care functionality or 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.

2.4. Operator Platform

An operator deploys platforms and networks as a base layer in their application stack. Platforms include service delivery platforms etc. The next layer would be the service enabling layer. In terms of the M2M platform this basically addresses the functionality to manage and configure access devices, *e.g.*, access enablers). In addition these offerings can be extended beyond those more horizontal oriented access enablers via vertical solution enablers like billing functionality, user (customer) management etc.

In competitive markets operators can offer different functionality with service enablers to support the business processes of their customers and thus may develop a sharp profile in M2M segments. However, it does make sense that basic access infrastructure is supported by all operators to provide some minimum M2M functionality for applications. This includes management of devices or basic messaging services as a replacement for SMS in packet switched networks.

As pointed out, the main limitation in the current approaches is the lack of security and reliability and the problem of addressing and identifying mobile devices. This could be solved by bringing some of the traditional operator's capabilities in the M2M domain. Thus, separation of addresses and identifications (such as IMEI and ISIM) on the one hand and offering managed and secure services (data handling, billing service) would be examples of such enabling services.