Challenges in Realizing Mobile M2M Global Services

July 2012

Connected Device Forum

Contents

1 Introduction

As the world becomes smaller and the “Internet of things” becomes larger, mobility and global services, i.e., provisioning, connection management, security, control and monitoring (roaming) of Machine to Machine (M2M) devices have become essential. For instance many modules purchased and provisioned in one location/country need to operate in other countries.

The deployment dynamics of M2M modules and applications differ from traditional, high-end consumer and business subscribers using smart phones and laptops; operators now have to consider low ARPUs, adapted data plans, and permanent roaming solutions to stay competitive in the M2M market.

The market opportunity for wirelessly connected machines is surrounded by speculation. Several estimates suggest the number of M2M and Connected Consumer Electronic (CCE) devices will be around 122 million by 2016. The number of connections that exist today on cellular networks includes an aggregation of various types of connected devices including gateways for smart meters and other sensors, e-readers, tablets and PCs with embedded wireless data modules and technologies, making the actual M2M opportunity even more unclear. In spite of this, many operators that are entering or becoming more aggressive in the M2M market remain optimistic that it is going to be worth their while.

1.1 Objective

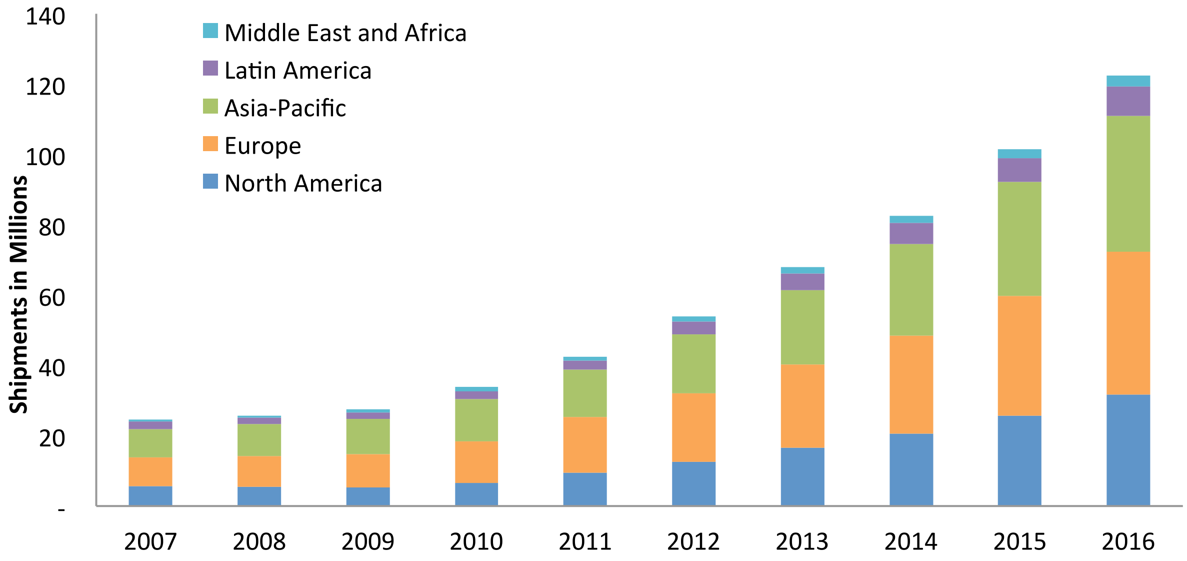
This paper identifies some of the potential roaming challenges for mobile M2M devices and applications along with the vertical industries and their potential market sizes. Using brief use cases, we will explore the practical uses for roaming and discuss the key challenges that operators may encounter in providing global services for M2M devices and applications.

The Connected Device Forum, (CDF), together with M2M network operators, their equipment providers and industry user, works to address these challenges.

2 Market Overview

While most operators are targeting similar verticals today including fleet management, automotive telematics, remote equipment/asset monitoring, eHealth monitoring, tablet and e-readers, the opportunities for M2M cellular connections are expected to grow from approximately 43 million in 2011 to 122 million by 2016, representing about 24% growth, worldwide. As chart 2.1 shows, the largest projected market growth is expected in Europe closely followed by Asia-Pacific. In Europe, the need for efficiency is fueling regulatory bodies to pass and enforce legislative regulation requiring the use of M2M devices and applications. However, in Asia-Pacific the size of the market, coupled with the lack of financial, healthcare, automatic meter reading, automotive, security, tracking, point of sale, emergency telephone systems, information displays and mass transit systems, make this an ideal market to enable M2M services.

Chart 2.1 Total Cellular M2M connections by Region, Forecast: 2007 - 2016

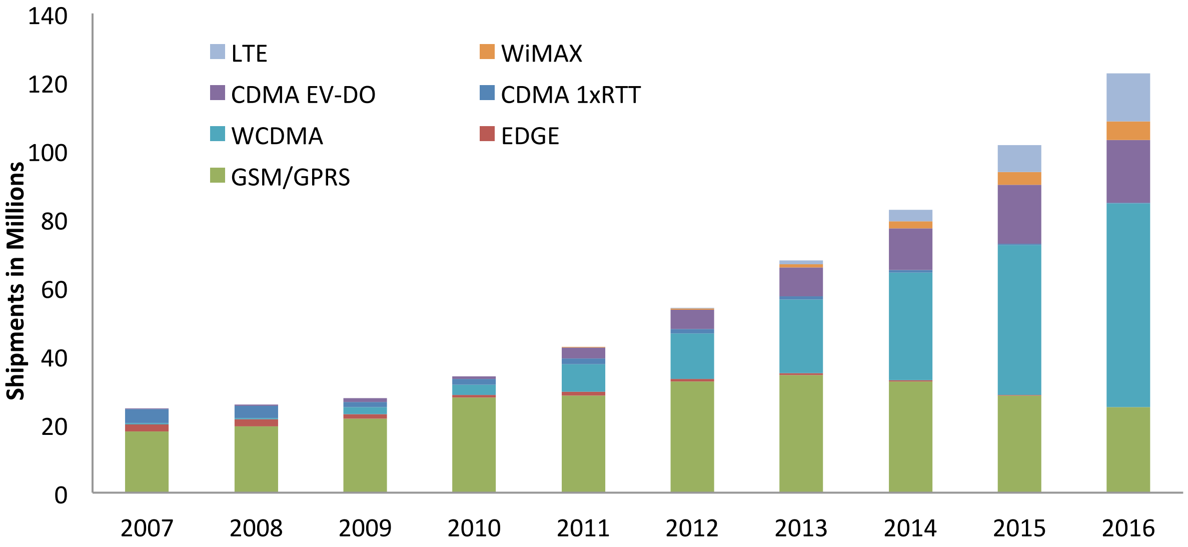


Source: ABI Research – M2M market data

2.1 3G and 4G for M2M Applications and Services

Today, cellular M2M applications are primarily deployed using CDMA2000 and GSM/GPRS technologies due to M2M's low bandwidth requirements. However, as more applications become available such as electronic billboards, real-time applications for monitoring medical devices, patient location and health status, telemedicine (which requires high-quality images for X-rays), CAT scans and MRIs for remote diagnostics, and video surveillance for enhanced security applications, more 3G and 4G network capabilities may become necessary. ABI Research indicates that by 2015 the lion share of the devices using M2M services will be moving from 2G to 3G technologies. While there has been significant discussion about the need for LTE to enable M2M, we find that 3G technology choices are ideal for future M2M deployments.

Chart 2.2 Total Cellular M2M connections by Air Interface, Forecast: 2007–2016



Source: ABI Research – M2M market data

As operators migrate from 2G to 3G, there is concern among some in the industry that 2G networks will be turned off at some point in the relatively near future. It is expected that the spectrum will be recycled for 3G use. With M2M device lifecycles lasting upwards of 10 years, the concern with M2M deployments on GSM is that an upgrade would change air interface standards, therefore requiring an expensive upgrade. Hence, device vendors and suppliers should consider building with 3G at a minimum.

It is clear that not one solution fits all. User experience, price, and the need for applications will vary depending on the degrees of connectivity for M2M applications. For example, polling a meter several times a day to upload a short burst of information on energy use to a remote server does not require a high-speed connection. This may yield a low ARPU compared to traditional wireless services. However, if we look at the cost model for M2M applications, we can suggest that offering data connectivity to and from devices can deliver a profitable business model using 3G systems.

2.2 Cost Model for M2M

Studies provided by Current Analysis Inc. describe the following costs for delivering service to M2M devices and applications:

- Customer acquisition such as marketing, advertising and promotion
- Implementation and management
  - Device certification costs
  - Subscriber provisioning costs
  - Customer “on-boarding” costs such as account creation, configuration and rate-plan association
  - Pricing and rating platform costs

    - ❒ Customer support such as tech support, billing and escalation calls
    - ❒ Bad debt from charge disputes
- ■ Network usage, depreciation, and amortization of assets

Assuming the same percentages and the same market scenarios apply, if we suggest customer acquisition costs make up roughly 40% of ARPU, implementation and management contribute to roughly 30% and the costs associated with the radio and core network usage make up the remaining 30% of revenues, then the below cost model results in a greater margin for M2M services over traditional wireless services.

Table 1: M2M and Wireless Service Margin Model

Metric	M2M	Traditional Wireless Service
Average Revenue Per Sub	$3.00	$50.00
Customer Acquisition Cost	$0.75	$13.00
Service Delivery and Customer Management	$0.15	$10.00
Network Usage per Sub	$0.60	$5.00
Total Cost per Sub	**$1.50**	**$28.00**
Profit/sub	$1.50	$24.00
Margin	**50%**	**44%**

Source: Best practices in M2M: The Operator Perspective, Current Analysis, 2009

In comparing M2M services directly to traditional wireless services, contributing factors that will increase this percentage include customer acquisition costs, device subsidies and network usage that will be marginalized resulting in an even greater operating margin for M2M services. While the average M2M application may result in low monthly ARPUs, the deltas between the numbers are expected to be so significant that the margins make this business model profitable. Once device certification and the length of time to certify devices diminish, this delta will be even greater.

2.3 M2M Vertical Markets

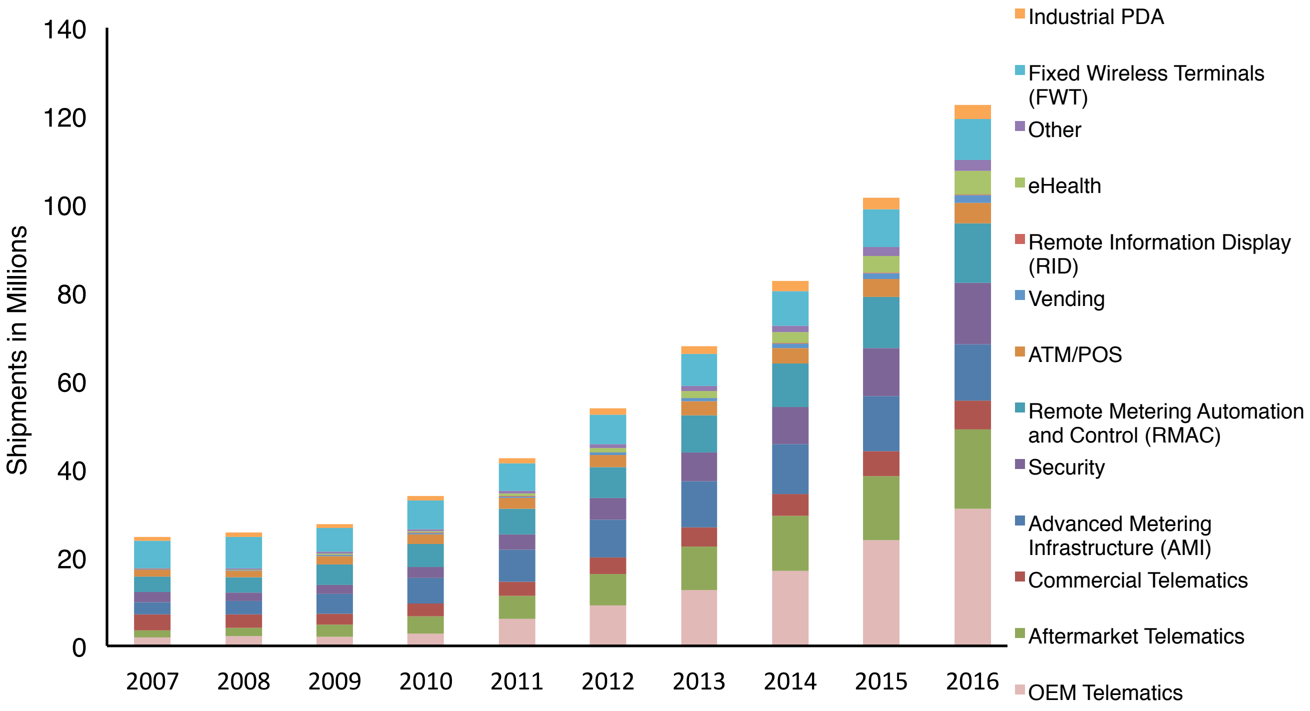
Operators differ in their approaches to the M2M market; those that have launched dedicated M2M business units have focused on verticals which stand to gain the most from wireless connectivity. These vertical markets include automotive (both for telematics and fleet management), eHealth solutions, consumer electronics, manufacturing/asset management, and smart grid deployments.

Of the mentioned vertical markets, ABI Research forecasts the telematics vertical (to include OEM, aftermarket and commercial markets) to be the largest with 37% of the market share and growing to 45% by 2016. Not only are more cars being shipped with diagnostic determination software but now they also include infotainment and connectivity via Wi-Fi.

Smart grid networks have largely been deployed due to regulatory requirements and mandates. While technology source is not specified in these requirements, utility companies have turned to proven wireless technologies to fulfill requirements. These networks make up roughly 16% of the market share with a projected decline down to 10% by 2016. This forecast is due to the market getting larger and at some point the number of connections becomes stagnant.

eHealth currently holds roughly 2% of the market share of devices being shipped. While there has been significant discussion, investment and development in this vertical, the total market share of eHealth applications is projected to be roughly 4% by 2016.

Chart 2.3: Total Cellular M2M Module Shipments by Application, Forecast 2007 – 2016



Source: ABI Research – M2M market data

We see the areas of telematics, asset tracking/monitoring and some classes of eHealth being the verticals that will be impacted by the need for global connectivity. Those verticals combined are expected to hold less than 50% of the market share of devices and applications that are being impacted.

2.3.1 Automotive Telematics

The connected car – All electric vehicles (EV) currently have a Telematics Control Unit which has M2M connectivity. Other cars have Internet access and/or infotainment access. For example, several car manufacturers are integrating connectivity into their cars for services such as Telenor's eCall (automatic call in case of accidents), remote diagnostics and infotainment. When the car is then shipped overseas, these systems send remote look up messages which require connectivity back to the home market. However, commercial fleets –-which make up a large portion of vehicles on the road – and insurance telematics platforms that provide emergency response systems are all in various stages of adoption. Juniper forecasts that new connected platforms in vehicles will exceed 100 million by 2016. It is expected that driver efficiencies in connected vehicles will increase, and reduce costs. Regulatory initiatives, such as the European Union's eCall, will also boost telematics adoption in vehicles.

Integrating the smartphone into consumer cars represents a new route for mobile Internet and infotainment as well. Vehicles manufactured in one country and operating across the globe are potential permanent roamers and will need to be capable of being monitored and reconfigured if necessary.

2.3.2 Asset and Fleet Tracking

The trucking and container industry needs global tracking which can significantly impact key factors of efficiency, prompt customer service, and hence revenue. The use of geofencing, over-speed alerts and other exception notification technologies can ensure that the assets are where they should be and safe even when the owner company is not directly managing them. Through a variety of intelligent M2M services, productivity and improvement of operations that control costs and generate revenue can be adopted.

With a Global Gateway services platform, one can monitor, measure, and manage assets via a single user interface using SMS or PD services worldwide with secure delivery of SMS messages to M2M devices, or alerts and notifications to an end-user's mobile terminals. Since these assets and fleet can be anywhere in the world, these are considered permanent roamers.

2.3.3 eHealth Applications

eHealth, monitoring fitness, wellbeing and urgent healthcare, increases the availability of remote healthcare while reducing the cost, and improves a physician's efficiency.

eHealth is a relatively recent healthcare model that engages the patient for self-monitoring their own wellbeing coupled with high-end healthcare through a media of specialized technology and communication systems. It involves the use of sensors to monitor patient data and software for remote diagnostics, transfer of images and scans via telecommunication and transactions within and between healthcare institutions. eHealth applications through M2M mobile devices make possible remote and wireless monitoring of health parameters, and diagnostics, etc.

Wireless health monitoring is one of the most common applications now being used. People can check their own blood pressure, glucose, and stress levels by using sensors with Bluetooth or Zigbee connections to smartphones with applications to monitor, manipulate and interpret data. They can then transmit that information to a physician securely whenever and from wherever potentially reducing costs and allowing older people to stay out of expensive nursing homes.

Another important trend through the use of M2M health applications is the ability for mobile health applications to collect community and clinical health data, deliver healthcare information to practitioners, researchers (immunology), and patients, real-time monitoring of patient vital signs, and direct provision of care via telemedicine. Given that integration of technology in hospitals has greatly increased, it is common practice for doctors to now use smartphones and tablets. The smartphones have helped improve communication with patients, and access to information is more efficient. eHealth applications have also improved urgent care handling of trauma situations by being able to provide needed monitoring when the patient is enroute to the hospital. The ambulance has the ability to send real-time information through properly equipped M2M devices.

While eHealth is a strategic vertical in the M2M space, there are challenges in providing end-to-end security when confidential patient information is involved. In some cases, information pertaining to a patient may belong to one healthcare program. Providing patient care in another healthcare program may require moving to other systems which could reside across operator domains. This change in systems could result in the device needing to roam in order for the patient's information to become available in the new healthcare program where treatment is being provided.

With the millions of patients projected to be implanted with M2M devices, the requirement of being able to provide connectivity globally becomes imperative, and this will represent a significant challenge in remote patient management.

However, the most important differentiator and impact of eHealth applications is the nature of data presentation from various devices, such as sensor data (as in pulse oximeter, blood glucose, etc.), in the required formats and sending that information via compliant application layer protocols like IEEE 11703 (under various device profiles). Currently this data is presented in individual healthcare formats based on service provider, type, and insurance agency. The need for mobile healthcare records to be in a standardized presentation, such as Hl7, is a critical component and the biggest challenge today in providing eHealth data across systems.

3 Global Connectivity for M2M

Many M2M applications are mission critical whether they support vehicle or fleet tracking, eHealth applications, or power delivery. Being able to access M2M devices, applications and services globally from gateways and control centers is imperative. The following is an overview of the requirements and challenges for providing M2M services globally.

3.1 All M2M Identifiers

Regarding M2M global services and roaming, the following identifiers need to be well defined.

3.1.1 Device and Smart Card Identifiers

The original HW identifier mentioned in the 3GPP2 standard was ESN (32 bits), but because of its exhaust, a new HW standard identifier has been used – MEID (56 bits/14 Hexa)

The smart card Identifiers are UIMID (32 bits) and SF_EUIMID (56 bits/14 Hexa) and LF_EUIMID (72 bits.18 Hexa) which is the ICCID when replaced by UIMID. Smart cards are identified during call processing via MIN/IMSI subscription identifier. There are several advantages of using card IDs over subscription IDs

- Cards for M2M are manufactured w/o MIN/IMSI being provisioned to allow activation by any MNO in any region.
- They are unchanged and useful for inventory and asset tracking.

3.1.2 Application Identifiers

A unique identifier that resides on the M2M Service device is the Application Identifier. The need for an Application Identifier to be globally unique needs further study. However, it should be transparent to the M2M transport operator and always owned by the M2M service provider. It may need to be changed when changing M2M service providers. In the case of CS, the application ID is represented as an identifier and it may be available to the transport CS core network in order to identify the intended specific application, e.g., SMS, USSD.

3.1.3 Subscription Identifiers

In 3GPP2, MIN and IMSI are used but again, because of MIN resource exhaust issues, true IMSI—especially for M2M devices which may roam (is provisioned along with MIN-based IMSI)—will be required.

3.1.3.1 Global Unique Identifier

Every M2M device that may need to access a network or roam must have access to a system that accepts incoming global roamers and should have a globally unique subscription identifier. At the time of writing, this is being debated, yet currently there are no new M2M requirements.

3.1.3.2 Multiple Subscriptions and Multiple Simultaneous Accesses

In some scenarios, M2M modules in CDMA2000 may require multiple subscription identifiers to minimize roaming requirements even though the module may support only one access technology at a time.

In case more than one simultaneous access is required, the module may use separate or multiple subscription accesses.

In case an M2M module supports more than one air interface (CDMA2000, WCDMA, LTE and WLAN), there could be two cases: 1) same subscription identifier used across all air interfaces/technologies, and 2) different subscription identifiers used across different technologies. This will depend on the access providers.

3.1.3.3 Packet Data Access Subscription Identifiers

This identifier is user@realm as defined by IETF (RFC 4282 NAI (Network Access Identifier)) although the actual length is limited to 72 bytes. The restriction comes about because of RADIUS protocol and required backward compatibility.

- The following mechanisms may be required to keep privacy on this identifier over the air and between the RAN elements and CN.
  - Use of Encryption
  - Use of Temporary Identifiers (vendor/carrier specific) in a specific occasion
  - Username privacy (omitting the user name part)

3.1.3.4 IP Identifiers

Deployment of a large number of M2M devices with IPv4 will increase the address exhaust problem and hence the use of IPv6 may address this problem, but several factors may impact this:

- M2M device/terminal IP capability
- Type of application (IPv4 only, dual stack and IPv6 only)
- Home network IP capabilities (IPv6)
- Roaming network IP capability (IPv6)

Suggested solutions to this include: 1) the use of private IPv4 addresses in conjunction with NAT, and 2) the use of IPv6 only for M2M devices.

3.1.3.5 MDN for SMS (CS Domain)

Many M2M devices use SMS for alert wake up to initiate network transactions, and the addressing is either MIN based or MDN (conforming to the ITE-T E164 numbering scheme). ANSI-41 systems route SMS using MDN instead of MIN, and MCs and other CN entities use MDN only. For SMS requirements, M2M devices may need to be addressed using MDNs as well as for inter technology SMS (between CDMA2000 and GSM); the use of an MDN becomes essential.

In addition, some M2M applications which use VOIP will require the use of an MDN in order to interconnect with the PSTN.

3.1.3.6 Network Access Identifiers (NAI)

NAIs are designed by the IETF to accommodate certain use cases as the syntax of user identifier used when roaming (RFC 4282).

- Optionally carry only user identifier
- Optionally carry only an authoritative domain – the Home operator
- Optionally specify routing – routing decoration
- Other decoration (not in RFCs but commonly used)
- Used by many of the IETF protocols and other SDOs
- In AAA, it is used to help the AAA client and proxy route AAA messages to the home network.

To use NAI's for roaming purposes, determine what the identifier is identifying and how big it should be while taking into consideration that size constraints may exist.

- In the case where the identifier is sent, then the maximum size over RADIUS is 253 octets, which includes everything you put in the NAI.
    - Is it globally unique or is it unique in the context of a home realm? If it is globally unique, which registry is controlling it?
- The need to convey the NAI outside the home realm is dependent on M2M devices' roaming capability.
    - Identity is really only required by the home realm.
    - There may be privacy concerns of revealing the true identity.
- There may be a need to know in the RAN or PDSN whether the entity is an M2M device. Device type or group(s) to which it belongs can be revealed during the authentication process; that information can be conveyed after the authentication.

3.1.3.7 PLMN ID Selection

An MTC/M2M device normally operates on its home PLMN (HPLMN) or equivalent home PLMN (EHPLMN). However, when it is away from a home PLMN for any reason, a visited PLMN (VPLMN) may be selected. There are two modes for PLMN selection:

1. Automatic mode utilizes a list of PLMNs in priority order. The highest priority PLMN which is available and allowable is selected.
2. Manual mode may not be relevant or provided in M2M where the terminal indicates to the user which PLMNs are available. Only when the user makes a manual selection does the terminal try to obtain normal service on the VPLMN.

There are two cases:

- International roaming: This is where the M2M device receives service on a PLMN of a different country than that of the HPLMN.

- National roaming: This is where the terminal receives service from a PLMN of the same country as that of the HPLMN, either anywhere or on a regional basis. The terminal can make a periodic search for the best HPLMN while roaming nationally.

If service is not allowed in any PLMN, a message is received by the terminal in response to attach, UMTS detach, or routing area update request from a VPLMN. That VPLMN is added to a list of "forbidden PLMNs for UMTS service" which is stored in the terminal, and thereafter that VPLMN will not be accessed

The terminal maintains a list of allowed PLMN types. The allowed PLMN type can be GSM-MAP only, ANSI-41 only, or both. During PLMN selection, based on the list of allowed, PLMN types, and a list of PLMN identities in priority order, the particular PLMN may be selected either automatically or manually. Each PLMN in the list of PLMN identities can be identified by either 'PLMN identity' (GSM-MAP) or 'SID'. In the system information on the broadcast channel, the device can receive a 'PLMN identity' (GSM-MAP), or a 'SID' or a 'PLMN identity' (GSM-MAP), and a 'SID', in a given cell. For a given cell, the device might receive several 'PLMN identities' from the system information on the broadcast channel. The result of the PLMN selection is an identifier of the selected PLMN, the choice being based on the allowed PLMN types, device capability, or other factors. This identifier is one of either 'PLMN identity' for GSM-MAP type of PLMNs or 'SID' for ANSI-41 type of PLMNs.

3.1.3.8 International Roaming MIN (IRMs)

MINs are numbers that uniquely identify mobile M2M devices working under the TIA standards for Cellular and PCS technologies (e.g., EIA/TIA–553 analog, IS–136 TDMA, or IS–95 CDMA).

IRM (International Roaming MIN) are MINs with the following format: 0-XXX+6D or 1-XXX+6D. The 4-digit prefix of an IRM is allocated by IFAST (International Forum on ANSI-41 Standards Technology) that attempts to facilitate international roaming by minimizing conflicts with North American MIN. The last 6 digits of an IRM are allocated by the carrier.

3.1.4 MTC Subscriptions

The equivalent term for an M2M device in 3GPP is called an MTC device and will henceforth also be used. Based on stage1 requirements, the MTC features are controlled by subscription. Any usage of the subscribed MTC features is activated by default at the time of feature subscription. The simplified assumption here is that the M2M server platform resides with the operator.

It should be possible to allow MTC subscribers to activate the unsubscribed MTC features or deactivate the subscribed MTC features based on the operator’s policy. The mechanisms used for activation/deactivation are outside the scope of 3GPP. The MTC solution shall make it possible to provision the home PLMN with MTC subscriptions and allow one or more MTC devices to share this subscription. This key issue aims at specifying the architectural requirements related to MTC subscriptions as well as the relationship between MTC subscriptions, MTC devices, and MTC architecture enhancements.

MTC features are controlled by subscription in HSS. The capability to subscribe/unsubscribe MTC features is left to the provided MTC subscriber. The subscription information of the MTC feature shall be stored in the relevant 3GPP CN entities.

It is also possible for a network operator to restrict incompatible MTC feature subscriptions (according to network operator policy). During the activation/deactivation, if the MTC subscriber requests results in a set of incompatible MTC features (according to network operator policy), it shall be possible for the operator to reject the request.

Upon attachment or subscription update, it shall be possible for the SGSN/MME to support only a subset of the subscribed MTC features based on network capability and/or MTC device capability.

It may be possible for the network operator to inform the MTC device's enabled/disabled status of the MTC features.

The following requirements are relevant to MTC subscriptions:

- It shall be possible to provision the Home PLMN with MTC subscriptions, each one shared by one or more MTC Devices.
- From a roaming point of view, it may be required to provision or change the MTC subscription from outside the Home PLMN.
- Each MTC device shall be associated to one MTC subscription and shall have a device subscription including the security credentials used to authenticate the device.
- As mentioned earlier, an MTC subscription shall indicate MTC features that are subscribed by the MTC devices sharing this subscription.
- It shall be possible for all MTC devices sharing the same MTC subscription to use all subscribed MTC features belonging to this subscription.

3.1.4.1 MTC Device Triggers

For many M2M applications a poll model for communications between MTC devices and the MTC server may be required. This may be because the MTC user wants to be in control of communication from MTC devices, and does not allow MTC devices to randomly access the MTC server (possibly creating an access/traffic overload situation on the network). For applications where normally the MTC devices initiate the communication, there may occasionally be a need for the MTC server to poll data from all MTC devices.

For MTC devices that are not continuously attached to the network or that have no always-on PDP/PDN connection, it is beneficial to trigger MTC devices to attach and/or establish a PDP/PDN connection based on a trigger indication from the MTC server.

The following functionality is required to trigger MTC devices:

- PLMN shall be able to trigger MTC devices to initiate communication with the MTC server based on a trigger indication from the MTC server.
- MTC device shall be able to receive trigger indications from the network and establish communication with the MTC server when receiving the trigger indication. Possible options are:
  - Receiving trigger indication in detached state and establish communication.
  - Receiving trigger indication in attached state and the MTC device has no PDP/PDN connection.
  - Receiving trigger indication in attached state and the MTC device has a PDP/PDN connection.

> (There are currently available solutions to trigger MTC devices (e.g., unanswered CS call attempts, sending an SMS). However, these have disadvantages when used on a large scale (e.g., they are based on MSISDNs) and will work only for attached MTC devices. Future enhancements will require possible improvements over the currently available means for triggering).

3.2 Key Technical Challenges in M2M Roaming

Providing global services or roaming to M2M devices can be challenging, since these devices rely on partner networks for communication back to the home network. The challenges include identity management and security, configuration management, service layer, and connection management for M2M roamers.

3.2.1 Some Roaming examples

The following section will deal with a specific M2M roaming scenario and possible implementation.

3.2.2 Future EV requirements including access to charge points in different geographies.

An Electric Vehicle (EV) needs access to a charge point. Many of the charging stations laid out on national freeways are serviced by specific service providers. These service providers may need to access different operators which will need access to different PLMNs based on coverage. EV roaming across multiple charge point operators / energy utilities (smart grid operators) need to have roaming agreements just like cellular operators. The following scenario can be assumed:

1. Authorization and Energy policy exchange between Home Utility and a visited Utility (smart grid operator)
2. Completion of charge with time stamps for each charge occasion
3. Energy settlement notification to Home Utility and HPLMN for each charge instance
4. Start and end of communication with time stamps to HPLMN for each charge occasion

It is also assumed that a different third party clearing house (similar to the settlement process in today's data roaming service) may also be required.

3.2.3 Identity Management and Security for M2M Healthcare Roamers

The healthcare industry depends on accurate identification and authentication of patient-involved data coupled with past medical data, accurately linking patients with their personal information for hospitals, other healthcare providers, and healthcare players, including the government. This is particularly challenging when the patient (client M2M device) is in a visited network, and access to an M2M application server is located in the home network. The case may also be that the healthcare provider is different and may or may not recognize the application ID.

An end-to-end identity and authentication solution based on USIM application/smart card provides the best solution in a secure, private, sensitive way. The application ID in this case will not rely on lower layers' security or transport but instead, on application protocols that can accomplish this. For example, the smartphone, which acts like a gateway collecting sensor information, can still transmit health parameters over the WWAN to a healthcare provider back in the home network over a VPN or using TLS/SSL.

A USIM with an application and with suitable encryption software can provide a high level of security and privacy, making the technology ideal for complying with HIPAA [10] and preventing fraud. Smart cards can be readily used online and across networks and deliver very high levels of security over the Internet. Smart cards are also very convenient and easy for people to use over multiple wireless operators across regions.

While this seems like a viable solution, this method has not been accepted globally; therefore, these types of services are still not available today to M2M roamers.

3.2.4 Remote Configuration Management for M2M Roamers

M2M devices may have a need in the life cycle of the device to change provisioning/credentials of the device and/or to change the configuration when the device is in a visited network or is roaming. This requires a trusted environment. One way is to have a secure tunnel to access the device from the Control Center in the home network or a third-party server in a different location. The need to change the credentials on the USIM could arise because the IMSI of the local service provider needs to be populated along with a new APN from the remote server.

Typically, the third party who manages Remote Subscriptions (USIM) may have access to different operators globally, along with a block of IMSIs for each of those operators which could be a solution for M2M roamers. However, M2M devices that appear as incoming roamers to a visited network need to be able to get packet data services at local rates or near local rates instead of at high roaming rates. This is because M2M devices provide frequent bursts of data traffic. A third party for global USIM management could become a common practice in the industry, since traditional roaming models involve several bilateral roaming agreements which include lengthy negotiations, timelines, and resources, who can then manage the large traffic volumes and small marginal gains of M2M roamers. A large number of M2M roaming devices requiring local IMSIs and their monitoring and control could be challenging in visited networks.

An alternative proposal is to provide a single agreement with a third party who also provides remote USIM services.

3.2.5 Service Layer and Connection Management for M2M Roamers

The requirements for an M2M service layer have been identified, and general stage 1 requirements are specified in 3GPP TS 22.368 by SA1, 3GPP Rel.10. The standard service layer addresses:

- M2M fragmentation avoidance
- Provides M2M applications on networks, gateways, or devices with standardized access to commonly needed functionality
- Standardized interfaces (protocols & APIs) – simplifies application development
- M2M application developers do not need a deep understanding of underlying access
- Same service layer for different verticals – simplifies deployment and operation
- Enables underlying networks to use M2M optimizations (but does not force them to)

Also, ETSI TC M2M defines the following service layer functions:

- Registers apps on devices/network
- Establishes secure connections
- Reads/writes connected objects
- Allows messaging and other higher-level functions
- Possibly allows store-and-forward
- Keeps track of reachability
- Enables macroscopic scheduling
- Manages events (subscribe/notify)

There will be service layer implementations on both the network and device, but if the service layer (and interface) implementation at the visited network side is not in conformity with what is implemented in the home network, the M2M device would not be able to obtain the complete suite of services in that vertical.

It could even happen that the connection manager may not be compatible in the visited network and may require connection manager adjustments which could pose problems. Currently, the standard service layer implementations are not firmed up because of lack of agreements on open APIs or a minimum set of APIs required for implementation. These are ongoing discussions both in GSMA as well as in different standards bodies. M2M roaming requirements and other issues have not been significantly discussed.

3.2.5.1 Network Enhancements for M2M

There is a need for many enhancements in both 3GPP2 and 3GPP (access as well as CN) if millions of M2M devices are to be accommodated. The details of these enhancements are outside the scope of this paper, but it must be mentioned that overload control in order for the MTC to work is important. The following details need to be discussed in order for efficient use of current network implementations:

- Overload control for low priority (MTC) UEs
- The case of “single MTC application per device”
- Overload control for PS domain

This could become an issue if there is a large number of incoming M2M roamers to be accommodated and the visited network does not implement any access barring or overload control.

4 Summary and Key Challenges of M2M Roaming Devices

Presently, M2M device penetration (by whatever measure these are counted) in the cellular network is rather low; these numbers are forecasted to exponentially grow in the near term. While it is generally agreed that not all M2M devices would need to address roaming requirements, there are certain verticals/segments that are deemed as roamers and in some cases permanent roamers. The definition of M2M roaming is somewhat different than in traditional wireless communication. In the case of these M2M devices, the services over their lifetime are truly global which means:

- The SIMs/devices can be sold without configuration/provisioning
- The SIMs will be embedded modules in many instances and will be provisioned in the home network where the devices are manufactured
- The SIMs/devices will move globally or work in a remote location in a different network
  - Arising from the need to either reconfigure/reprovision during their life cycle
  - The need to monitor and control the devices from the home network
  - The SIM provider could be a third-party to securely access and change credentials in a trusted environment
  - This need may arise because the M2M devices, like tablets and PCs, may need to get data services at local or near local rates

Coupled with these aspects, there are currently no standard implementations of service layer with interfaces on the network side which can manage and provide a similar suite of services as in the home network. Multimode M2M devices will present other challenges as well such as:

- No agreement of provisioning a global unique user ID or an M2M application ID
- Device reachability without IP connection
- Special requirements of Electric Vehicles on universal charging and rates
- Location and battery life of containers/fleet management tasks
- Healthcare M2M devices needing standard application protocols like Hl7 and IEEE 1703
- M2M remote batch deployments with high chance for roaming
- Many different M2M third parties to manage
  - SIM management
  - M2M services
  - Connectivity services
- No entity can manage all aspects of M2M devices over the life cycle

4.1 Conclusions

There is an urgent need to recognize the challenges and find solutions for M2M device roaming capabilities and global services which could be brought under the IR bodies to address them. The key point is to solve and agree to solve the cost of operating the service in a roaming environment, since the ARPUs, even in home networks, are too low to sustain efficient management and control. This is a call to action for an industry group to be created to focus on these challenges, aligning efforts with the standards organization and other contributing industry organizations and to provide global M2M roaming to all verticals and air interfaces.

Acronym List

3GPP	3G Partnership Project
3GPP2	3G Partnership Project 2
AAA	Authentication, Authorization and Accounting - said "triple A"
ANSI-41	American National Standards Institute – 41
CN	Complimentary Network
ESN	Electronic Serial Number
GSM-MAP	Global System for Mobile Communications Mobile Application Part
HSS	High Speed Solutions
HW	Hardware
ICCID	Integrated Circuit Card Identifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFAST	International Forum for ANSI-41 Standards
IMSI	International Mobile Subscriber Identity
LF_EUMID	Long Form Extended User Identity Module Identifier
MDN	Mobile Directory Number
MEID	Mobile Equipment Identifier
MIN	Mobile Identification Number
MME	Mobility Management Entity
PD	Packet Data
PDP	Power Distribution Panel
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Service
RAN	Return Authorization Number
SDO	Standards Development Organization
SF_EUMID	Short Form Extended User Identity Module Identifier
SGSN	Serving GPRS Support Node
SMS	Short Message Service
UE	User Equipment
UMID	Unified Multi-Purpose ID
VOIP	Voice Over Internet Protocol