|  |  |  |
| --- | --- | --- |
| APTlogogreen3 | ASIA-PACIFIC TELECOMMUNITY |  |
| **SOUTH ASIAN TELECOMMUNICATIONS REGULATOR’S COUNCIL** **(SATRC)** |  |
|  |  |

**SATRC REPORT ON**

**ICT REGULATORY FRAMEWORK FOR M2M COMMUNICATIONS AND IOT FOR THE SATRC COUNTRIES**

**Prepared by**

**SATRC Working Group on Policy, Regulation and Services**

Adopted by

**19th Meeting of the South Asian Telecommunications Regulator’s Council**

13 – 15 December 2018, Islamabad, Pakistan

Table of Contents

[EXECUTIVE SUMMARY 3](#_Toc531850669)

[Chapter 1 4](#_Toc531850670)

[Introduction and Background 4](#_Toc531850671)

[1.1 Methodology used for the study 5](#_Toc531850672)

[1.2 Definition and Meaning 5](#_Toc531850673)

[1.3 IoT vs M2M 6](#_Toc531850674)

[1.4 Forecast/Projections: 7](#_Toc531850675)

[1.5 Use Cases of Machine-to-Machine Communications 7](#_Toc531850676)

[1.6 M2M Ecosystem 8](#_Toc531850677)

[Chapter 2 10](#_Toc531850678)

[Global Regulatory Practices and Challenges 10](#_Toc531850679)

[2.1 Global M2M Policy issues and regulations 10](#_Toc531850680)

[2.2 Regulatory Framework for M2M 11](#_Toc531850681)

[2.3 Numbering and Addressing : 14](#_Toc531850682)

[2.4 Regulatory practices for permanent roaming of M2M 21](#_Toc531850683)

[2.5 Quality of Service 23](#_Toc531850684)

[2.6 Security, Privacy and Data Protection 24](#_Toc531850685)

[Chapter 3 25](#_Toc531850686)

[Regulatory framework in SATRC member countries 25](#_Toc531850687)

[Chapter 4 27](#_Toc531850688)

[Conclusion/Recommendations 27](#_Toc531850689)

[Annexure-I: Questionnaire 30](#_Toc531850690)

[Annexure-II: Response to the questionnaire by SATRC working group experts 31](#_Toc531850691)

#

# EXECUTIVE SUMMARY

In recent years a rapid development of a variety of services that make use of Machine-to-Machine (M2M) communication has taken place. M2M is a communication technology where data can be transferred in an automated way with little or no human interaction between devices and applications.

In this report, M2M/IoT communications are understood as a fully or largely automated communication (data transfer) between two or more information and communications (ICT) entities, that may be part of a predetermined group. A goal of this report is to help SATRC members to come out with effective policies to promote the proliferation of M2M services and devices. The spectrum requirement for M2M services is not deliberated in this report because it is a subject matter of another working group.

The potential amount of M2M/IoT devices could be large and some applications may need several numbers (e.g. E.164 numbers) or addresses (e.g. IPv6 addresses), and therefore there is a potential need for a large amount of identifiers. It is recognized that some national numbering plans may not be prepared for such big demand for numbers. Thus a numbering strategy is required for both short and long term to meet requirements for M2M services.

It is expected that the development of M2M/IoT applications will have an impact on national numbering plans because machines need to be uniquely addressed in order to communicate with them, or rather to enable them to communicate with each other. The natural intention by operators and M2M service providers is to use E.164 numbers from the existing numbering plan for M2M services because of the relatively simple implementation in already existing network infrastructure. In the long run IPv6 addressing will become very important as an alternative numbering resource for most of the M2M/IoT applications. However, there is much uncertainty what period is involved so that numbering policy for M2M should be flexible enough to be also a solution for the longer term

SATRC member countries need to come out with effective registration/licensing mechanism for M2M services. They should also strive for efficient numbering and addressing solutions for Machine to Machine (M2M) applications and to avoid possible exhaustion of existing numbering ranges. The information in this report might be useful as policies on M2M numbering in most countries are still in an early stage of development and information on best practices may not be available. Permanent roaming is also an important requirement for the success of services using M2M/IoT. The quality of service, security, and privacy aspects of M2M /IoT services are also deliberated upon in this report.

#

#

# Chapter 1

# Introduction and Background

In recent years a rapid development of a variety of services that make use of Machine-to-Machine (M2M) communication has taken place. M2M is a communication technology where data can be transferred in an automated way with little or no human interaction between devices and applications. The advantages of M2M are great for both business and consumer purposes. For business use, M2M technology may lead to more effective and efficient operations (e.g. fleet control). For consumers, as an example, applications used for home security and smart metering can be facilitated by M2M.

Machine to Machine (M2M) communication is the next evolution on the technology front and lot of development activities in this field are taking place across the world. M2M communication along with Information and Communication Technology (ICT) will play a critical role in collection of information from the field, collation and analysis of this information and activating desirable outcomes, by reducing the human machine interface. M2M is applicable in various sectors like Agriculture, health, security, electricity, water management etc to name a few. By linking large number of previously unconnected ‘things’ and sharing their data, M2M is unleashing a new age of innovation.

Apart from M2M, other terms are also being used to describe such communication - Internet of Things (IoT), Embedded Wireless, Smart systems (Homes, Cities, Meters, Grids etc.) with slightly different attributes to each term. IoT is connected network of embedded devices capable of having M2M communication without human intervention. M2M Communication when combined with logic of cloud services and remote operation becomes “Smart”. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of connected “things” to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

It is expected that the development of M2M applications will have an impact on national numbering plans because machines need to be uniquely identified and addressed in order to communicate with them, or rather to enable them to communicate with each other. The natural intention by operators and M2M SPs is to use E.164 numbers from the existing numbering plan for M2M services because of the relatively simple implementation in already existing network infrastructure.

The potential amount of M2M devices could be large and some applications may need several numbers (e.g. E.164 numbers) or addresses (e.g. IPv6 addresses), and therefore there is a potential need for a large amount of identifiers. It is recognized that some national numbering plans may not be prepared for such big demand for numbers. Thus a numbering strategy is required for both short and long term to meet requirements for M2M services.

In this domain, the policy and regulatory challenges are enormous and involve reshaping regulations and opening up avenues for imaginative new policies. The numbering resources for M2M and IoT devices, Quality of Service (QoS), Roaming aspects, security etc. are some of the actionable areas which need to be deliberated, to further the M2M ecosystem growth.

This report will help SATRC countries to prepare a uniform and timely regulatory framework on M2M communication and IoT in the region and there by proliferating the growth of M2M and IoT ecosystem and to bring tangible social and economic benefits to consumers, businesses, citizens and government.

## 1.1 Methodology used for the study

During the first meeting of the Working Group on Policy, Regulation and Services held in Dhaka, Bangladesh from 18 to 19 April, 2017, it was agreed that the lead expert will carry out the study based on:

1. Questionnaire: The lead expert had developed questionnaire and was circulated to all the nominated experts from the member countries. The responses of this questionnaire have been used to review and analyse the current practices or regulatory framework for M2M and IoT.
2. Secondary research: In order to supplement the questionnaire, the lead expert used secondary research to review and to understand best practices on regulatory framework for M2M and IoT. Numerous reports on best practices by the international organizations such as International Telecommunication Union (ITU), European Telecommunications Standards Institute(ETSI), Organization for Economic Co-operation and Development(OECD), Body of European Regulators for Electronic Communications (BEREC), GSM Association (GSMA), European Conference of Postal and Telecommunications Administrations (CEPT), Electronic Communications Committee (ECC) in the CEPT, etc have been reviewed to get the insight various aspects of regulatory framework for M2M and IoT services. The reports published by different national telecom regulatory authorities have also been reviewd.
3. Consultation and peer review by experts: The issues and concerns associated with the subject have been discussed and deliberated thoroughly during the meetings of the experts as well as workshop conducted by Asia Pacific Telecommunity (APT) for the SATRC Working Group.

Besides consultations, the draft report has been circulated to the members of the working group for their review and feed-back. Based on the feed-backs /comments, the report has been finalized for submission to the Council during its 19th Meeting to be held in Islamabad, Pakistan.

## 1.2 Definition and Meaning

There are various definitions given by Global Standardization organizations for M2M. European Telecommunications Standards Institute (ETSI) has defined M2M as

 *‘Physical telecommunication based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure.’*

According to OECD’s report, the term M2M describes

*‘Devices that are connected to the Internet, using a variety of fixed and wireless networks and communicate with each other and the wider world. They are active communication devices. The term is slightly erroneous though as it seems to assume there is no human in the equation, which quite often there is in one way or another.’*

The International Telecommunication Union (ITU-T) has defined Internet of things (IoT) as

*“Global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.”*

The term M2M, also commonly known as ubiquitous or pervasive computing refers to what is essentially a four-step process: data is generated, data is transmitted, data is analysed, and data acted upon. Other names that define M2M or its subsets include the ‘internet of things’, ‘connected devices’, ‘remote monitoring and diagnostics’, ‘smart computing’, ‘smart metering’ and ‘extended internet’. M2M (machine to machine) leverages innovations in micro computing and wireless technology that allow embedded devices to collect and distribute real-time data and has the potential to connect millions of machines today, and even more in the near future. In simple terms, M2M is defined as a technology that enables electronic and mechanical devices to communicate with each other seamlessly and perform actions without human intervention.

According to BEREC, the term Machine to Machine (M2M) generally refers to the process of the transfer of information on the part of devices which do not necessarily require human interaction. Since this process perforce involves elements of both connectivity (access terminals and technologies) and of the supply of the service (contents and platforms), the term M2M covers many aspects and can regard many sectors of use.

With regard to connectivity, although M2M was originally developed on wired network (typically for industrial automation), the scope of M2M has recently increased and it is considerably extended to wireless networks, both for the spread of low cost and low energy consuming "intelligent" terminals, and for the increased capacities of the radio networks. For that matter, the possibility of using the radio-mobile networks has allowed for the development of certain applications such as logistics (e.g. goods monitoring) and the management of transport vehicles (e.g. fleet management).

## 1.3 IoT vs M2M

This report mainly concentrates on the M2M devices which require interconnection with the public network, since the other cases can be understood as private installations and therefore they are not of particular interest for the purposes of the regulatory analysis. In M2M process, automatic interconnection of the devices takes place by connection to the Internet network. For this reason, M2M is often associated with the Internet of Things (IoT): in fact, M2M and IoT are partially overlapping concepts and, in much of the literature of the sector (especially that of Anglo-Saxon and United States origin), both terms are used as synonyms. On the other hand, on the technical level, a partial distinction between the two is possible: there are many applications (industrial automation, management of alarms, etc.) which are based on M2M communication services but which are extraneous to IoT. Although the above considerations may not be shared (e.g. because they tend to confine M2M to intermediate services for the supply of connectivity and to separate it from the performance rendered to the end user), the relative arguments show that it is worth distinguishing between the two concepts of M2M and IoT.

One question that often arises when discussing IoT is the difference between IoT and M2M communication. While the distinction is not universally agreed, the GSMA’s view is that M2M typically refers to the connection between machines or devices, while IoT refers to the whole ecosystem, which includes the application, backend and connectivity. So, using the example of a connected car, M2M would typically cover the elements where machines communicate with each other with little or no human intervention. Diagnostics, telematics and software updates typically only involve machines or devices making connections to each other. Conversely, infotainment services or remote services, such as using a wireless device to find a car’s location in a car park, typically involve a whole ecosystem of different services, including GPS and payments, as well as human interaction with the solution. We would therefore class these as IoT solutions.

## 1.4 Forecast/Projections:

The importance of the M2M debate figures prominently in the views of many market futurists, for example:

1. The GSMA forecasts a connected universe of upto 50 billion connected devices by 2020 and GSMA reiterated the important role M2M will play in the future of communications as its annual GSMA mobile world congress[[1]](#footnote-1)
2. Analysys Mason predicts that the global market for M2M device connections will grow from 62 million devices in 2010 to 2.1 billion devices in 2020. With an estimated year on year growth rate of 36%-52%, M2M seeks to be one of the fastest growing connectivity sectors in the next decade.[[2]](#footnote-2)
3. GE (General Electric) estimates that the industrial internet has the potential to add $10-15 trillion to global GDP by 2030 and reduce billions of dollars of waste across major industries such as healthcare, energy and transportation. While this recent report is primarily focused on the impacts on heavy industries (aviation, energy, etc) it does also cover a range of other sectors.[[3]](#footnote-3)

## 1.5 Use Cases of Machine-to-Machine Communications

M2M communications is applicable in various sectors like Automative/Transportation, Utilities/energy, Healthcare, Safety and surveillance, Public Safety, Smart city, Agriculture etc. to name a few. The most popular use cases of M2M communications is summarized below.

**Table1.1: Use Cases of M2M/IoT**

|  |  |
| --- | --- |
| Industry/ Vertical | M2M applications |
| Automotive Transportation | Vehicle tracking, e-call, V2V and V2I applications, traffic control, Navigation, Infotainment, Fleet management, asset tracking, manufacturing and logistics,Intelligent traffic management systems that control the flow of traffic, reducing congestion, bottlenecks and delays. And cars that communicate with each other, making the flow of traffic smoother and safer. |
| Utilities / Energy  | Smart metering, smart grid, Electric line monitoring, gas / oil / water pipeline monitoring,A smart energy grid that intelligently manages the power being generated from renewable or local energy sources with consumer demand for electricity. This could reduce reliance on large power stations to meet dips in supply and peaks in demand. |
| Health care | Remote monitoring of patient after surgery (ehealth), remote diagnostics, medication reminders, Tele-medicine, wearable health devices,Intelligent pill boxes and wearable sensors that monitor the health of patients and automatically trigger an alert if a problem arises. This will help patients leave hospital earlier and reduce the frequency of routine follow up appointments – improving quality of life and reducing costs. |
| Safety & Surveillance | Women Safety Bands, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police / medical alert Financial /Retail Point of sale (POS), ATM, Kiosk, Vending machines, digital signage and handheld terminals. |
| Public Safety | Highway, bridge, traffic management, homeland security, police, fire and emergency services. |
| Smart City | Intelligent transport System, Waste management, Street Light control system, Water distribution, Smart Parking |
| Agriculture | Remotely controlled irrigation pump, Remote Monitoring of Soil Data,Fertilizer, fodder and water distributed across the farm in the right quantities, in the right places, and at the right time |

## 1.6 M2M Ecosystem

M2M ecosystem is very complex and is entirely different from the standard telecom ecosystem. It is more diverse and involves multiple stakeholders. Connectivity provider forms an important part of this complex ecosystem. In order to derive a regulatory framework which adequately address and foster each of the incumbent players in the M2M ecosystem, it is necessary to understand all the layers involved and their interplay and interdependence.

 The M2M/IoT ecosystem typically consist of –

1. Device Manufacturer/Provider: The device provider is responsible for devices providing raw data to the network provider and application provider according to the business model. This category will encompass the M2M chip-set manufacturer, the M2M module manufacturer and the end device manufacturer (for e.g. a car manufacturer or an air conditioning manufacturer) who integrates the M2M module in his device).
2. Connectivity/Network provider: The network provider/ operators are the connectivity providers who own the underlying network to provide connectivity and related services for M2M Service provider. In particular, the network provider can perform the following main functions:
* access and integration of resources provided by other providers; support and control of the M2M/IoT capabilities infrastructure;
* Offering of M2M/IoT capabilities, including network capabilities and resource exposure to other providers.
1. M2M service provider (MSP): It is an entity that provides M2M Common Services (registration, discovery, security, group management, data management & repository, subscription & notification, device management, application & service management, communication management, network service exposure, location, service charging & accounting) to Application provider.
2. M2M Application provider: It is an entity that realizes the service logic of an M2M Application and utilizes capabilities/resources provided by the network provider, device provider and M2M service provider, in order to provide M2M applications to end users.
3. End user: Individual or company who uses an M2M solution. 

**Fig 1.1 M2M ecosystem**

Connectivity provider plays a central and critical role in the M2M ecosystem. In general, the M2M ecosystem has two networking landscapes; connectivity using licensed spectrum which are mainly provided by Mobile Network Operators (MNOs) or Mobile Virtual Network Operators (MVNOs) and connectivity through unlicensed spectrum. Various wired and wireless technologies can be leveraged for M2M communication. Some of the wireless technologies are mentioned in the following Table Generally, the technologies in WPAN, WLAN, HAN, LPWAN, use unlicensed spectrum whereas in WAN, licensed spectrum is used.

**Table 1.2: Wireless technologies**

|  |  |
| --- | --- |
| **TYPE OF NETWORK** | **TECHNOLOGIES** |
| Wireless-Personal AreaNetwork (WPAN)/ Wireless-Local Area Network (WLAN) | INSTEON, IrDA, Bluetooth, BLE,Z-Wave, Zigbee, Body AreaNetwork RFID, WiSUN, Wi-Fi |
| Wide Area Network (WAN) | GSM, CDMA, WCDMA, LTE,Satellite communication, LTE-A |
| Low Power Wide Area Network(LPWAN), *specifically designed**for Machine- type**communication (MTC)* | Sigfox, LoRa, Weightless,Ingenu, SilverSpring’s Starfish,Cyan’s Cynet, Accellus, Telensa,Waviot |

 Globally both licensed and unlicensed spectrum is used for offering M2M services. M2M deployments using unlicensed spectrum is substantial. The large scale adoption of Bluetooth for wearable devices is one such example, where, network is not based on licensed spectrum. Many new approaches , for example, LPWAN technologies viz. LoRa, SigFox, Weightless-N; WPAN/WLAN technologies viz. INSTEON, IrDA, Bluetooth, BLE, Z-Wave, Zigbee, WiSUN and other proprietary mesh networks, which are specifically designed for machine-type communication (MTC) and that use unlicensed spectrum, are being experimented and adopted.

The deployment of M2M and IoT systems in multiple sectors, and their potential impact on individuals and businesses, raises regulatory issues such as licensing, numbering and addressing, spectrum management, network standards, QoS, data protection, privacy and security etc. Moreover, as the roll out of M2M proliferates and the pace picks up, one can expect a large number of unforeseen issues getting thrown up. Such issues can be sector specific or cross-sector in nature.

Government/policy makers have a major role to play in shaping market rules that affect M2M/IoT adoption such as appropriate licensing/registration, regulations etc. They have to create a robust and enabling regulatory framework to create sustainable M2M/IoT development and deployments. Moreover, it is incumbent on their part to set out guidelines for data collection, data sharing, use of IoT data, data privacy, data security etc. In addition, they must establish rules about liability and ownership.

#

# Chapter 2

# Global Regulatory Practices and Challenges

M2M communication is in its evolving stage world over with certain countries having implemented it in a modest way. The benefits this revolutionary technology can have in the way we live and its cross sector impact has been well understood by international organizations and telecom sector regulators world over. It is expected that in the next 10-15 years, M2M communication will percolate to all facets of human life and will be a game changer for the industry and the economy at large. It is vital to have a policy framework in place, well in time, to foster the M2M communication so that complete benefits of this innovation can be passed on to the citizens. The orderly growth of this sector will demand cross sector policies and regulatory framework.

## 2.1 Global M2M Policy issues and regulations

By linking large numbers of previously unconnected ‘things’ and sharing their data, M2M is unleashing a new age of innovation. The policy and regulatory challenges are enormous and involve reshaping regulations and opening up avenues for imaginative new policies. Telecom Service Providers (TSP’s) and Internet Service Providers (ISP’s), as connectivity providers, are familiar in dealing with telecom regulators. But when it comes to IoT/ M2M they are out of their comfort zone, as there are multiple regulators and data authorities for health, energy, road & transportation services and so on. Further muddying the waters, many market segments, such as the automobile industry, are global in scope. As vehicles cross frontiers via exports, travel and cargo transportation, regulatory loopholes emerge such as ‘permanent roaming’ SIMs. While regulations have proved to be a constraint to IoT/ M2M growth, ironically they also can be a major driver for expansion. In long run, globally, following issues have to be dealt by regulators:

1. Regulatory framework
2. Numbering plan
3. Permanent roaming
4. Spectrum licensing and management
5. Quality of service:
6. Security, Privacy, Data protection

This suggested scope of study of this report includes licensing, numbering, and other related issues like quality of service, roaming requirements and security.

## 2.2 Regulatory Framework for M2M

Regulatory frameworks for M2M services are in their early stages worldwide, with very few countries formalizing any specific roadmap. Increasingly, regulators in many countries are focusing on M2M as a key priority and looking at it in a comprehensive way. Challenges arise in terms of identifying the feasibility of the framework, as the scope of M2M is diverse that involves different sectors, multitude of players and wide ranging technologies. The primary objective of any framework should be to safeguard the interests of consumers and end users. A brief overview of Regulatory Practices followed by different countries and Regulatory bodies are as follows:

**Table 2.1 Regulatory Practices for M2M**

|  |  |
| --- | --- |
| **Countries/Regulatory bodies** |  **Position** |
| BEREC (The Body of European Regulators for Electronic Communications). | No special treatment is necessary or appropriate for M2M communication, except for the following areas:* Roaming
* Switching
* Number portability
 |
| Europe | Some countries have issued Mobile Virtual Network Operator (MVNO) licenses for M2M players. |
| United Kingdom | Ofcom observed that the industry is best placed to drive the development, standardization and commercialization of new technologies such as M2M. Ofcom has launched Business Radio licences for M2M communication, covering the use of radio for mostly short range localised radio networks for factories, shopping centres. Other licences cover communication requirements for courier firms, bus companies, taxis and utility firms. There is also a radio supplier’s licence covering demonstration and short term hire of equipment. The current telecomlicensees would continue to operate under the existing framework; however, specific changes to particular licenses on a case-by ­case basis would be made. |
| Singapore | Operators are required to have a license to offer M2M services under the framework of the regulator, Info-communications Media Development Authority (IMDA).Licensees have to ensure that SIM cards used for M2M services are only used for automated communication. Licensees shall list out the following:1. The range of International Mobile Subscriber Identity (IMSI) numbers and Mobile Station International Subscriber Directory Number (MSISDN) to be used
2. Working with any local operator partner in relation to the provision of M2M services
3. Identification of M2M equipment importer
4. Registration of all SIM cards used to provide M2M services in Singapore
5. The records to be maintained in Singapore for a minimum of 12 months from the date of termination of the service

The M2M license enables the licensee to provide M2M services using equipment with embedded SIM cards. |
| Brazil | The M2M players are registered in the MVNO category and brought under the regulatory framework |
| USA | In January 2017, the US Department of Commerce published guiding principles and outlined an approach to support the advancement of M2M. The key highlights are as follows:* Enabling infrastructure availability and access: Physical and spectrum related assets; IPv6 adoption
* Crafting balanced policy and building coalitions: Cyber security, privacy, intellectual property and free flow of cross-border data
* Promoting standards and technology advancement
* Encouraging markets: Public private partnerships, Government procurement and workforce issues (education, training and civil liberties)
 |

Source: “BEREC Report on Enabling the Internet of Things,” BEREC IoT Workshop, 1 February 2017; “Fostering the advancement of the IoT,” The Department of Commerce Internet Policy Task Force & Digital Economy Leadership team January 2017; “Guidelines for submission of application for services based operations license,” IMDA, December 2016; VHF radio spectrum for the Internet of Things,” Ofcom, March 2016; ,” Ofcom, July 2014. around: “VHF radio spectrum for the Internet of Things,” Ofcom, March 2016 and “Promoting investment and innovation in the Internet of Things,” Ofcom, July 2014.

## 2.3 Numbering and Addressing:

The international trends/practices/on addressing or numbering resource allocation for M2M services are listed below:

**2.3.1 Electronic Communications Committee (ECC) Reports**

ECC has carried out comprehensive analysis of numbering requirement and various solutions which are available in its various reports which are detailed in the following sections.

**Important points of ECC report 153, November, 2010[[4]](#footnote-4)**

1. The number length of network external numbers should be as long as possible (max 15 digits according to ITU-T Rec. E.164).
2. As a long term solution IPv6 addresses, or numbers/addresses other than E.164 numbers should preferably be used for device based communication applications. These numbering/addressing schemes or switching from E.164 numbering plan to a new plan should not prohibit market development or competition.
3. There are possible situations where a new number range should be opened. For example, the number range in question may require different regulatory treatment, e.g. relating access to emergency services, or the services to be provided have certain characteristics (e.g. M2M applications in fixed networks) where existing mobile number ranges may not be adequate.

 **Options suggested by ECC**

For planning MSISDN (ITU Rec E.164) numbering resources for M2M devices/Gateways, ECC documents have suggested the following four options:

***Option A****:*

Existing mobile number ranges, including possible expansion of them (E.164 numbers)

***Option B:***

A new number range for M2M or similar applications (E.164 numbers) (for example longer numbers than normally, however max 15 digits according to E.164)

***Option C:***

An international numbering solution (E.164 numbers)

***Option D:***

Network internal numbers

 **Analysis of these options is as follows:**

***Option A: Existing mobile number ranges***

Complies with ITU-T Rec. E.164 (interconnection and international traffic is possible; max. 15 digits),

* Number portability is directly applicable (flexibility to change operator)
* May not allow separate back-office solutions for M2M applications
* A risk of exhausting the existing ranges
* Less new capacity than the network internal number option D
* In the case of non-geographic and existing Premium Rate service(PRS) numbers, limitations on access from overseas;
* Inter-operator billing difficulties and a risk of incurring unnecessary expense

***Option B: New number range***

* Must comply with ITU-T Rec. E.164 (interconnection and international traffic is possible; max 15 digits)
* Number portability is applicable (flexibility to change operator)
* Enough capacity available if full number length is used
* A fresh start for number analysis
* Different regulatory requirements possible if needed
* May allow easier back-office solutions, such as charging and billing

***Option C: international number range***

* Comply with ITU-T Rec. E.164 (interconnection and international traffic is possible; max 15 digits)
* Number portability is applicable (flexibility to change operator)
* Full capacity of numbers is available
* Number range needs to be assigned by the ITU and the applicant needs to be qualified
* International number, i.e. international prefix has to be always used
* Challenges in number analysis and effective routing
* New interconnection agreements might be negotiated
* May need to be treated in the same way as other international Traffic

 ***Option D: Network internal numbers***

* Not regulated in many countries; decisions and management by operators
* Same numbers can be used in every network allowing multiplied capacity
* Allows long numbers with much capacity – even longer than 15 digits numbers are possible if technical feasible
* No need for determining number length
* Allows use of hexadecimal digits if technical feasible
* Number portability is in practice not possible
* M2M SP is locked with one operator => possible competition issues
* Difficult or impossible to evolve to ‘network external’ mode if required for some reason
* Didn’t comply with ITU-T Rec. E.164

**Significant points of ECC/REC/ (11)03, May 2011**

a) The number length in the new number range(s) accommodating future mass M2M applications should be as long as possible (in case of E.164 numbers maximum of 15 digits according to ITU-T Rec. E.164).

b) The NRA should ensure that the new number range(s) are not used as an alternative to existing number ranges to escape regulatory requirements.

c) As some existing regulatory requirements (e.g. access to emergency services) may not be relevant or useful for M2M applications, exceptions regarding existing regulatory requirements could be applied to new numbering range(s) accommodating these applications.

**ECC report on M2M, Brussels, November, 2013**

ECC had published a report in November, 2013 in Brussels, ensuring the availability of numbering and addressing resource. The conclusions are as given below:

a) The potential number of M2M applications/connections may have a big impact on National Numbering Plans;

b) Reports help regulators to develop efficient numbering solutions and to avoid numbering exhaustion (existing and new national numbering ranges);

c) Meet the needs of operators and M2M SP and to avoid possible lock-in of M2M users

d) The IP addresses might be a long term solution;

e) The E.164 number length for new M2M numbering range should be as long as possible (maximum of 15 digits including Country Code);

 **ECC recommendations (15)02, April, 2015**

ECC vide their recommendations (15)02, issued guidelines for major changes to National numbering and dialing plans concerning E. 164 numbers which was approved in April, 2015. The important recommendations of this report are as given below:

*Sufficient capacity is always made available for the growing demand for numbers for mobile services, and also for M2M services in accordance with* ***ECC/REC/(11)03 of May 5, 2011.***

**2.3.2** **Allocation of MNC (Mobile Network Code) for M2M**

 The ITU held a consultation on the "Possibility of parallel usage of 2 and 3 digit E.212 Mobile Network Codes (MNCs) under one geographic Mobile Country Code (MCC)" in 2013, However, its formal position is yet to be finalized. Opening up access to MNC’s for M2M service providers could stimulate competition by enabling balanced negotiations that promote the growth of M2M. A large M2M SP holding its own MNC could have more leverage when entering negotiations with a potential partner MNO over its roaming (and other) rates. As it would no longer be dependent on the specific package that a mobile operator is prepared to offer, but could change SIM and other settings over the air, competition in the marketplace for M2M would be enhanced. Furthermore, switching to a new MNO at any stage would be much simpler and less costly for an M2M SP because the SIM cards themselves that are installed in the M2M devices would not need replacing. If the ITU recommend the issuing of MNCs to such M2M organizations and change the criteria as currently stipulated in Annex B of the ITU-T Rec. E.212, some countries may directly allocate MNC to big M2M SPs.

**2.3.3 AT&T comments on Ofcom consultation document**

AT&T had commented on the Office of Communications, U.K. (Ofcom) consultation document, promoting investment and innovation in IoT, during October 2014.[[5]](#footnote-5) The important points related to Numbering and addressing taken from the paper are as given below:

Machines are required to be uniquely identified and addressed in order to communicate; therefore, it is likely that E.164 numbers will be necessary for a long term with the M2M / IoT devices. For many devices and applications developed today, E.164 numbers are used and will continue to be used throughout the lifecycle of the product. With many consumer and industrial products having lifetimes of 10 to 20 years, an ongoing supply of E.164 numbers will be needed.

For the highly integrated nature of high-volume, low-cost, electronic modules, a retrofit or upgrade to an alternate numbering resource would be uneconomical. For instance, after expending substantial effort and incurring considerable expense, IPv6 use has seen considerable growth over the last few years. However, there may be a substantial overlap period where both IPv6 and E.164 numbers are in use. It is estimated that it will take 5 to 10 years for IPv6 to become widely available. If the field lifecycle of a device is 20 years, E.164 numbers could be needed for the next 30 years. However, issuance of new E.164 numbers could only begin to be phased out when IPv6 becomes widely available and then only for those devices that do not need to rely on PSTN-based addressing.

AT&T had advised Ofcom to consider the approach of several European countries (For example, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Netherlands, Norway, Portugal, Spain, and Sweden), which have introduced a special range of numbers for M2M communication. These special ranges typically have number blocks which use a longer number sequence (up to the full 15 digits) in E.164 format. The length of E.164 numbers for mobile users was selected to balance the needs of the efficient use of numbering with the human factors of communicating and dialing a convenient length. To achieve that balance, in Europe (including the UK) the average length of E.164 number ranges typically does not exceed 12 digits, which includes trunk code. Machines, however, have no such need for convenience and so for M2M communications a full 15-digit number allocation, as described in ITU E.164, could be considered.

 **2.3.4 Singapore Public Consultation**

There was a public Consultation on Proposed M2M Access Code Allocation Framework, by Infocomm Development Authority (iDA) Singapore.[[6]](#footnote-6) Important points on M2M Numbering, described in this paper are:

1. In developing the pilot M2M framework in 2010, IDA assessed that it would not be appropriate to open up existing telephone number levels for M2M services as these number levels are established primarily for persons-to-persons telecommunication. For instance, the NNP provided the 8-digit number levels for fixed-line telephone services (starting with prefix “6”) and mobile telephone services (starting with prefixes “8” and “9”), took into consideration the total capacity to cater for the long-term growth of these services and the ease of dialing by users. Allowing M2M services to use these number levels may exhaust the numbering capacity much sooner than expected.
2. To ensure that there is sufficient numbering capacity for all M2M devices and machines in the future, and to differentiate M2M services from other services, IDA has reserved a block of 4-digit M2M Access Code (i.e. “144X”) for M2M services. IDA also took the view that a maximum digit length should be adopted. Based on the International Telecommunication Union (“ITU”) E.164 numbering format, Singapore would allow numbers of up to 13-digit length, using the designated 4-digit Access Code (excluding the country code), based on current network routing technology and arrangements.

 **National Numbering Plan, IDA Singapore[[7]](#footnote-7)**

Important points on M2M Numbering plan in Singapore:

a) Service-based Operator (SBO) (Individual) licensees providing M2M services areeligible for ‘144XX’ access code.

b) The M2M access code allocated may be used with international connectivity andinternational roaming services.

c) Licensees providing M2M services using the M2M access codes, i.e. ‘144XX’ areencouraged to maximize the allowable numbering capacity with a 13-digit numberingformat (excluding country code) for each M2M access code.

In Singapore, mobile as well as fixed line numbers are of 8 digits. Without using theexisting numbering resource, they have planned a new 13 digits numbering scheme forM2M services.

**2.3.5 Hong Kong**

**Code of Practice Relating to the Use of Numbers and Codes**

Hong Kong is having 8 digit numbering scheme in fixed and mobile service, excludingcountry code. The code of practice relating to the use of numbers and codes in the HongKong Numbering Plan was revised in April 2015. Important points related to M2Mnumbering proposed in Hong Kong are as given below[[8]](#footnote-8):

a) In differentiating the “4500X” M2M numbers from the ordinary subscriber numbers,following guidelines were issued to the operators while assigning “4500X” numbers:

* 1. The numbers should be of 12 digits in length.
	2. The numbers shall not be required to support number portability.
	3. No mandatory requirement of inter-network routing is imposed on the numbers. Operators may freely enter into commercial arrangements with their interconnecting partners for routing of 12-digit “4500X” M2M numbers across networks based on their own business decisions.
	4. The numbers should not be used for voice and SMS communications. In case any M2M application would require communications via SMS, operators should assign ordinary 8-digit subscriber numbers for the application. Mobile network operators, MVNOs, fixed network operators, services-based operators in providing Class 1 or Class 2 services, and paging operators who provide M2M communications through the public telecommunications network using E.164 numbers may apply for the allocation of “4500X” M2M numbers.

 **2.3.6 MSISDN less Numbering plan**

In 3GPP Release-12/13, M2M HLR has a feature “MSISDN-less subscription”. This feature makes it possible to define MSISDN-less M2M subscriptions in R12/13 HLR, meaning that thistype of subscription may not have a valid MSISDN assigned to it. This feature may potentiallyreduce the pressure on MSISDN number series assigned to the PLMN operators and to someextent the risk of running into shortage of MSISDN numbers during large scale deployment ofM2M services. The MSISDN sent to the network for a MSISDN-less M2M subscription is theNetwork Application specific dummy MSISDN stored in M2M profile.However, MSISDN less M2M subscription cannot be examined at this stage because of lack of information about use cases and probable lack of any regulatory policy.

 **2.3.7 Summary of M2M numbering policy**

The summary of M2M numbering policy in various countries is as follows

 **Table 2.2: Summary of M2M Numbering Policy**

|  |  |
| --- | --- |
| **Country** | **M2M Numbering Policy** |
| Belgium | Non-geographic, fixed mobile agnostic network code, dedicated to M2M; |
| Denmark | IMSI only identifier to be used for M2M. No dedicated number range specified. |
| Finland | fixed length of 11 digits of national (significant) numbers for mobile numbers beginning with 049. The purpose is to use numbers beginning with 049 primarily for machine-to-machine communication (M2M) or similar purposes where the number's user friendliness is not on a top priority. |
| United Kingdom | Ofcom believes the limits on the availability of telephone numbers will not be a barrier to the development of the IoT as a range of alternative identifiers, such as Internet Routing Codes, SIM or equipment identifiers and IP addresses could be used. It also considers that migration to IPv6 in the longer term is likely. |
| Netherlands | Dedicated M2M number ranges for mobile |
| Norway | Dedicated M2M number ranges for mobile |
| Spain | Dedicated M2M number ranges for mobile |
| Sweden | Separate dedicated M2M number ranges for fixed and for mobile |
| Hongkong | allocate “4500X” numbers in 12-digit length for M2M services;450(1-9)X” numbers with digit length of 12 will be reserved to meet the future demand for M2M services;For M2M services. Numbers shall be assigned to machines but not subscribers. Numbers shall not be portable across networks and not be mandated to route |
| Brazil | M2M service providers are MVNO with separate IMSI block of their own. |
| Australia | In responding to the expected demand for new mobile numbers, in 2012 the ACMA made available a new mobile number range (05 range) to supplement the existing (04) mobile number range. The ACMA will continue to monitor changes in demand for mobile numbers used in M2M communications. |
| Singapore | Licensees providing M2M services using the M2M access codes, i.e. ‘144XX’ are encouraged to maximise the allowable numbering capacity with a 13-digit numbering format (excluding country code) for each M2M access code |
| Saudi Arabia | 13 digits with 12 digits National Significant Number (NSN)- 3 digits service indication code and 9 digits subscriber number.  0 83Z YY XX XXXXX, Z=0, Y=0-9, YY indicates licensee.M2M numbers may be allocated to fixed and mobile licensees in 100 sequential blocks (‘XX’) of 100K numbers (‘XXXXX’). Once an initial allocation has been made within a particular value of range ‘083ZYY’ (10M total numbers), CITC will generally designate all numbers within that range for the same licensee but, at its sole and reasonable discretion, may allocate within that range to another licensee for sequential allocation in blocks of 100K. The utilization ratio is 75% before the licensee may apply for a new block. |

Source: Consultation on ‘Numbering for Machine-to-Machine Communications’, Commission for Communications Regulation, Ireland(Comreg13/33, 28th March 2013), “M2M number resource requirements and options” published by Telecom Engineering Centre, India, Nov 2015, National numbering Plan, Saudi Arabia; National numbering Plan(Issue 1 – 1 October 2016)Info-communications Media Development Authority, Singapore; National Numbering Plan, Hong Kong

Report by Machina Research

 According to the report released by Machina Research in 2015

1. A number of regulators have opted to implement a dedicated E.164 mobile number range for M2M
2. Ultimately addressing of all connected devices will be handled by IPv6
3. CEPT has sought to encourage adoption of dedicated numbering –most EU countries have adopted

The distribution of countries with no M2M numbering and dedicated M2M numbering can be seen in the following diagram



From the above discussion, it can be concluded that the E.164 numbering resources (i.e. numbers in the national numbering plan) are the most viable solution for addressing M2M applications at least in the short and medium run. It is expected that most M2M applications will be based on mobile networks, and therefore within E.164 numbers the present mobile number ranges seem to be most suitable for M2M solutions. It is possible that IP-based solutions with IPv6 addressing will become more important in the long run.

## 2.4 Regulatory practices for permanent roaming of M2M

One of the critical aspects of M2M is the ability to offer services on a global scale. Lack of specific regulations on permanent roaming in most countries has benefitted the M2M market so far. However, M2M roaming is growing exponentially. Permanent roaming offers key benefits, ranging from supply chain simplicity to wider coverage. For instance, many multinational companies like to avail services from a single M2M player. The cost of M2M services increases significantly on account of switching M2M players. The absence of permanent roaming feature in M2M device acts as a significant barrier to businesses. The following table summarizes the regulatory practices for permanent roaming.

**Table 2.3: Regulatory Practices for Permanent Roaming**

|  |  |
| --- | --- |
| **Country/Regulatory body** | **Position** |
| BEREC/European commission | The European roaming regulatory framework applies in general to mobile connectivity in M2M services. However, certain exemptions have been made for M2M roaming services that are applicable to retail data roaming:Roaming providers need not send any automatic messages to M2M devices to inform the customer that roaming is ongoing, and provide information about prices.There is no obligation to provide M2M customers accumulated consumption of data or any maximum financial limits for specified periods of use.The EC roaming regulation do not obligate operators to offer permanent roaming |
| Germany | The telecom regulator, German Regulatory Authority for Industries: Telecommunications, Postal Services, Railways, Electricity (BNetzA), introduced new numbering rules in June 2016 to facilitate M2M services and to enable exterritorial use of numbers. The regulator has allowed the use of German IMSIs for M2M services in other countries. In addition, use of extraterritorial IMSIs is allowed in Germany. |
| Belgium | In August 2015, the Belgium telecom regulator, Belgian Institute for Postal Services and Telecommunication (BIPT), recommended that there should be more flexibility in the general extraterritorial use of Belgian numbering resources.For M2M services in particular, it recommended that permanent roaming be allowed for Belgian numbers abroad as well as for foreign numbers roaming in Belgium. |
| Ofcom, UK | has not taken any position on permanent roaming for M2M |
| Italy | The Italian regulator advocates adopting a global SIM approach |
| France | Telecom regulator, Regulatory Authority for Electronic Communications and Posts (ARCEP), favors leaving prices to commercial negotiation for M2M roaming. |
| Australia  | Currently, there are no restrictions on permanent roaming. |
| Brazil | Permanent roaming is prohibited |
| Singapore  | Permanent roaming is prohibited. In January 2016, IMDA embarked on a trial to see how an open GSMA standard (over-the-air subscription management) can enable embedded SIM (eSIM) chips to switch between different MNOs. The interoperable standards are expected to lead to a more competitive environment for the deployment of M2M devices, by reducing costs and increasing adoption.. |

Source : Source: “BEREC Report on Enabling the Internet of Things,” BEREC IoT Workshop, 1 February 2017; “Fostering the advancement of the IoT,” The Department of Commerce Internet Policy Task Force & Digital Economy Leadership team, January 2017; “Guidelines for submission of application for services based operations license,” IMDA, December 2016; VHF radio spectrum for the Internet of Things,” Ofcom, March 2016; ,” Ofcom, July 2014. around: “VHF radio spectrum for the Internet of Things,” Ofcom, March 2016 and “Promoting investment and innovation in the Internet of Things,” Ofcom, July 2014.Regulating Permanent Roaming for M2M and IoT devices by Ovum

Report on Permanent Roaming by Machina Research

 Permanent roaming: uncertainty persists around the world. “Extra-territorial use of E.164 numbering” is probably the thorniest issue in M2M regulation today. Supporting overseas connections is critical and there is an existing large installed base of permanent roaming SIMs. The Regulatory situation is unclear, and changing. The following diagram shows the regulatory practices for permanent roaming.



From the above discussion, it can be concluded that very few countries have explicitly banned permanent roaming for M2M devices and most of the countries follow the same regulations which are applicable for P2P SIMs.

## 2.5 Quality of Service

Different machines (e.g., sensors, meters) in an M2M system capture “events” (e.g., temperature, inventory level), which are transmitted through a network (e.g., wireless, wired or hybrid) to an application that translates them into meaningful information (e.g., items need to be restocked) . From the QoS perspective, in the service provisioning process, networks of different characteristics can be used. According to that, the challenge is how to provide end-to-end QoS guarantees despite the limitations of different means of communication. Namely, when providing services in M2M systems, service providers have to be very careful when agreeing on certain QoS parameters.

Although some initial efforts in the area of M2M standardization have been made, notably within the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP) . QoS in M2M has not yet been considered. However, the problem of QoS in M2M systems has been identified.

Some standards for M2M systems were proposed by the 3GPP where each M2M device attaches to the existing mobile cellular infrastructure. In that way, their solution is not applicable in every M2M system, because some M2M solutions may not be based on the cellular mobile network.

Any regulation that has a significant bearing on service providers’ handling of network traffic is not desirable. Operators should have the flexibility to manage end-to-end QoS for consumers. Typically, in a competitive environment, consumers choose service providers on the basis of various performance measures such as pricing, coverage and network quality. This ensures that consumers get the best of services in a transparent manner. Only if there is evidence of market failures can regulators possibly intervene.

QoS needs vary widely between usage, devices, applications and industries in M2M. The vast array of connected devices makes it difficult to prescribe and monitor QoS measures. There are a number of communication technologies for the deployment of M2M services and each one has specific nuances and protocols. A combination of different technologies is used for end service provisioning. In addition, various industries have separate regulators, each with its distinct set of requirements. For M2M services, it would be difficult to adhere to individual guidelines, which may significantly differ from each other.

## 2.6 Security, Privacy and Data Protection

The growth in the number of connected devices is increasing security concerns for organizations and M2M players alike. Connected devices offer more avenues for attacks. Identification of security breaches in a M2M context becomes very challenging. The large-scale deployment of identical devices increases vulnerability. Moreover, due to the hyper-connectivity of the M2M ecosystem, any security breach has the potential to affect other systems globally. Typically, in M2M, devices that are deployed in remote and hazardous areas have a long shelf life and are difficult to upgrade with new security patches. As a result, these devices/sensors are potential targets for cyber-attacks.

When switching M2M players, managing the life cycle of security credentials stored with the service providers as well as on the M2M devices is a key challenge. Without the ability to remotely change security credentials, it would be a challenge to upgrade each device/sensor physically. At times, an M2M device is manufactured at a certain location and used in a different location. In this case, the initial security provisioning process has to be robust and compatible with the requirements of different M2M players. Most of the security parameters have to be embedded in the M2M device, which increases vulnerability to attacks.

In the M2M context, individual KYC (Know Your customer) guidelines for subscriber registration are not relevant and practical from an implementation perspective. There are significant challenges in authenticating M2M SIMs. Typically, M2M SIMs are sold by service providers on a business-to-business (B2B) operating model. Any intermediary or system integrator (SI) would in turn offer M2M solutions to end customers such as utilities and automobile companies. It is a cumbersome task to gather information on the device/machine and the user of that hardware. Further to comply with KYC norms, service providers need to impose contractual conditions on intermediaries, which adds to the complexities. KYC is relevant if a connected device is associated with a single user or if a single user has full control over it. However, in case of M2M solutions, which are pure B2B applications and a SIM cannot be referred to a specific user, KYC and SIM registration rules are not relevant.

Organizations are struggling with the large number of devices that will become part of their networks in a very short period of time. Well tried, existing measures and provisions, as mandated under the licensing and policy regime, should be used to ensure security of networks and data.

The GSMA IoT Security Guidelines, which explain how an entity providing a cellular M2M service can secure its service end-to-end from most cyber-attacks, can be used as a reference set for security and privacy best practice guidelines. NIST Cyber-security Framework also acts as a reference point for security measures.

The very benefits that M2M provides like monitoring, collecting, analyzing and transforming data into meaningful information, are giving rise to privacy concerns. In M2M, where most of the communication happens without human intervention, intrusion of privacy is a tricky aspect. There are challenges in determining whether specific information is personal in nature or not. This distinction gets blurred when more stakeholders are involved, increasing data sharing interfaces. With M2M, the reach and feasibility of surveillance and tracking mechanisms are enhanced.

In many countries, there are strict rules and regulations around securing and storing personal data of customers. However, there are no consistent norms for data privacy across geographies. Multi-party real-time information flows may be hampered if privacy issues are not addressed at the outset. In the current scenario, there are patchworks of geographically bound laws that do not apply in the same manner to different technologies and sectors. Information collected in one country may be termed as personal data in a different jurisdiction. Increasingly, various stakeholders are resorting to using aggregated and anonymized data through which no individuals can be identified. There is growing debate on how to balance individual rights on the one hand and ensure law enforcement and maintain surveillance on the other. However, the regulatory position for private data collected by M2M devices is similar to that used for that collected by other means.

**Table 2.4: Regulatory Practices for personal data collected by M2M devices**

|  |  |
| --- | --- |
| **Country/Regulatory body** |  **Position** |
| BEREC | Personal data may be collected by a number of connected devices.**•** There is no need for special treatment with regard to EU Data Protection Principles (e.g., consent-based data collection and processing also apply in M2M context).**•** Careful adaptation or evolution is required in the M2M context (e.g., user-friendly information and consent procedures for smart homes). |
| Singapore | Governed by the Personal Data Protection Act (PDPA 2012) that comprises various rules governing the collection, use, disclosure and care of personal data. |

Source: Legislation and guidelines,” PDPC Singapore.

#

# Chapter 3

# Regulatory framework in SATRC member countries

A questionnaire was circulated to the experts in the SATRC working group from all the member countries to ascertain the status of Regulatory framework in these countries. Responses were received from Afghanistan, Bangladesh, Bhutan, Maldives, Nepal and Pakistan.

In most of the countries there is no licensing or registration mechanism for M2M and IoT service providers. However, it is possible that M2M and ioT services are being provided using the services of licensed telecom services. Most of these countries are studying the impact of these services and thinking over the need for the appropriate framework.

In Bangladesh there is no specific regulatory framework on M2M communication and IoT services. MNOs have recently launched some industry based M2M communication solution to enable users to have better control over his/her all devices in more efficient and easy way. M2M and IoT services are delivered as a part of licensed telecommunication services using the existing licensed spectrum band. Mobile Network operators provide these services by taking prior approval from the regulator or intimating them. Only for vehicle tracking service there is a requirement of license particularly for non-MNO whereas MNOs need to go through a simple registration process.

In June 2016, the Department of telecommunications (DoT), Govt. of India; released draft guidelines for M2M service provider registration for stakeholder consultation. As part of general conditions, registration can be granted to any company following certain guidelines. Also, M2M service providers shall not infringe upon the jurisdiction of any authorized telecom licensee/other service provider (OSP) and they shall provide only those services for which this registration is granted to them. As part of technical conditions, M2M service providers can take telecom resources only from authorized telecom licensee, should adhere to the KYC (Know your customer) norms and traceability guidelines, and ensure QoS stipulations. However, the final guidelines for M2M service provider registration are still awaited.

In most of the member countries M2M and IoT devices are being used extensively particularly in Power metering, Traffic and Fleet management, Agriculture and Industrial applications. In India also there is a very rapid deployment of M2M and IoT devices in various sectors of the economy. In May 2015, the Department of Telecommunications, Govt. of India released a national road map for M2M that focused on the communication aspects of M2M with the aim to have interoperable standards, policies and regulations suited for Indian conditions across sectors. In June 2015, the Govt. of India launched the Smart Cities Mission. A total of 100 Smart Cities have been selected among the various states and union territories (UTs) of India for this mission. In India M2M devices are being used extensively in almost all the sectors of economy viz. transport, manufacturing, agriculture, energy, and healthcare.

In Pakistan, International & national ICT firms are in early stages of developing innovative services using M2M technology, IoT and green solutions in Pakistan. Examples include advanced metering infrastructure with automated meter reading with real-time or near-time two way communication, Smart city solutions, smart devices/sensors/ actuators, smart farming, health care solutions, smart grids and connected agriculture.

Bangladesh Government has visionary plan to expand digital services to all people which is well defined in plan of Digital Bangladesh by 2021 and relevant policies of Bangladesh. Under PT&ICT ministry through training initiatives government is creating a large base of qualified human resources. Government is also providing innovation fund from where interested IT professionals can get fund to explore their interest on ventures related to M2M and IoT. Bangladesh government has already created platform for IoT expansion by established many IT parks where entrepreneurs will be able to involve themselves from starting to produce sensors, devices related to M2M and IoT services. Vehicle tracking services has got some popularity in Bangladesh Different govt. electricity power supply companies has started to provide smart metering based on M2M communication. Mobile network operators have launched M2M based smart factory, personal devices management etc. M2M and IoT industry is growing and with the time being it will expand in a great speed. So, interested parties have already started their work regarding M2M and IoT services.

In almost all of these countries no separate numbering series has been allocated for use for M2M and IoT devices which are are using the existing cellular network. India has however recently allocated a 13 digit numbering series for M2M services which consists of 3 digit M2M identifier, 4 digit telecom licensee identifier, and 6 digit device number. So, gradually all the M2M devices which were using the 10 digit numbering series used for P2P services are getting migrated to the new 13 digit series.In July 2016, the DoT had issued 3-digit M2M identifier codes: 559, 575, 576, 579 and 597.

In India, the power to issue telecom licenses is vested with the Department of Telecommunication. TRAI has recommended that suitable amendments in licensing conditions should be made for provisioning of M2M services. Connectivity providers using LPWAN technologies should also be put under the licensing through a new authorisation under Unified licence. It has further recommended that Devices with pre-fitted eUICC should be allowed to be imported only if they have the ability to get reconfigured “over the air” (OTA) with local subscription. Devices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian and mandatorily converted/ reconfigured into an Indian TSP’s SIM within the stipulated period or on change of ownership of the device. Country-specific relaxation on permanent roaming of foreign SIMs, if any, can be considered based on the strategic importance, bi-lateral or multi-lateral trade agreements and principle of reciprocity by the Government. International roaming in M2M shall be allowed under the well-recognized framework of GSMA ‘“M2M Annex.”

Department of Telecom in India is still deliberating upon the recommendations made by TRAI. However, DoT has laid down some guidelines for use of embedded SIMs and the KYC (know you customer) norms to be followed to fill up the Customer Acquisition Form for SIMs to be used for M2M devices. It has also issued the guidelines for bulk connections to be provided to M2M service providers. These SIMs will have some restrictive features in comparison to P2P SIMs. These SIMs are issued subject to the condition that such SIMs will have restrictive features compared to traditional SIMs for voice/data communications used for person to person (P2P) communication. The ownership of all such M2M SIMs shall be with entity/organization providing M2M Services. The details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, should be maintained by entity/organization providing M2M Services. Up-dated information regarding (a) Details of M2M end device i.e. IMEI, ESN etc, (b) Make, Model, Registration no. etc of the machines (i.e. Cars, Utility Meters. POS etc and (c) Corresponding physical custodian's name and address should be made available online through some web interface to Licensee by entity/organization providing M2M Services. Regarding maintenance of database/records of the end users of the SIM cards by the Licensee, the procedure as prescribed for bulk connection shall be followed.

The DoT guidelines also contain the procedure for transfer of these M2M SIMs from one entity to another and also compliance requirements for the telecom licensees. DoT has also decided to permit the use of "Embedded-Subscriber Identity Module (e-SIM)" with both Single and Multiple profile configurations with Over the Air (OTA) subscription update facility, as the case may be, as per the prevailing global specifications and standards (GSMA).The Licensees profiling e-SIMs shall take all reasonable steps to ensure that the device manufacturer embedding such SIM do not tamper the e-SIM at manufacturing stage. In order to facilitate Mobile Number Portability (MNP) and to avoid Telco Lock-in for all use case scenarios of e-SIM, the Licensees shall be permitted for Profile updation via Over the Air (OTA) feature, as per the prevailing global specifications and standards.

DoT is in the process of taking a final decision to formulate the registration/licensing mechanism for M2M service provider based on the recommendations of TRAI. The final decision on the International roaming requirements for SIMs used for M2M devices is also awaited.

# Chapter 4

# Conclusion/Recommendations

On the basis of the responses received from some of the SATRC member countries it can be concluded that the complete regulatory framework is yet to evolve although the M2M services are already working in the member countries and this sector is growing at a rapid pace.

It is imperative that the SATRC countries should come up with a light touch regulatory regime for M2M services. It is also important for the telecom regulator to work in unison with the sector regulator also for various types of M2M services in different sectors of the economy.

The decision on prescribing the numbering series to be used for M2M devices is very important because a huge number E.164 based numbering resources will be utilized for providing these services until IPV6 based addressing is used for this type of services. So, all the countries should come up with their policy on numbering resources for M2M devices. In case the existing numbering series is not enough for large scale deployment of M2M and IoT, they should use a separate numbering series for M2M devices which is being followed by most of the countries globally including India. The countries should also strive for rapid rollout of IPV6 based addressing for Internet services which will be used extensively for M2M services.

The aspects of international roaming and the security requirements are also the area of concern for the SATRC member countries. All the member nations are following the same international norms as being followed for P2P devices. They should come up specific guildelines for international roaming for M2M devices and also explore the option of over the air provisioning of SIM for M2M devices. Member States are encouraged to collaborate to ensure that charging of M2M roaming and permanent roaming are affordable thorough regional and bilateral initiatives. In market segments such as the automobile industry and consumer electronics that are global in scope it is important to have a clear policy on permanent roaming.

The quality of service aspects may be left to the market forces for the time being. However the services being provided using the licensed spectrum band are already being regulated by the telecom regulators. Service providers should have maximum flexibility to design their networks instead of defining SLAs at various points through regulatory mandates. Mandating any uniform QoS for M2M is not recommended. QoS is best left to a mutual agreement between stakeholders.

It is also necessary to have clear registration norms for SIMs used for M2M devices which may not owned by a specific person. The norms for transfer of ownership should also be defined. The Security and Privacy concerns for M2M/IoT should be addressed by the member countries in harmony with the existing laws of the respective countries.

#

# Annexure-I: Questionnaire

**SATRC Working Group on Policy, Regulation and Services**

**Questionnaire on work item “ICT Regulatory framework for M2M communications and IOT for the SATRC countries”**

1. **Background and Purpose**

Machine to Machine (M2M) communication is the next evolution on the technology front and lot of development activities in this field are taking place across the world. M2M communication along with Information and Communication Technology (ICT) will play a critical role in collection of information from the field, collation and analysis of this information and activating desirable outcomes, by reducing the human machine interface. M2M is applicable in various sectors like Agriculture, Health, Security, Electricity, Water resource management etc to name a few. By linking large number of previously unconnected ‘things’ and sharing their data, M2M is unleashing a new age of innovation.

Apart from M2M, other terms are also being used to describe such communication - Internet of Things (IoT), Embedded Wireless, Smart systems (Homes, Cities, Meters, Grids etc.) with slightly different attributes to each term. IoT is connected network of embedded devices capable of having M2M communication without human intervention. M2M Communication when combined with logic of cloud services and remote operation becomes “Smart”. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of connected “things” to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

In this domain, the policy and regulatory challenges are enormous and involve reshaping regulations and opening up avenues for imaginative new policies. The numbering resources for M2M and IoT devices, Quality of Service (QoS), Roaming aspects etc. are some of the actionable areas which need to be deliberated, to further the M2M ecosystem growth.

This report will help SATRC countries to prepare a uniform and timely regulatory framework on M2M communication and IoT in the region and thereby proliferating the growth of M2M and IoT ecosystem and to bring tangible social and economic benefits to consumers, businesses, citizens and government.

1. **Scope of the study**

The suggested scope of study is to explore the possible regulatory framework including licensing, numbering and other aspects:

* Quality of Service in M2M Services and IoT
* M2M Roaming Requirements
* Other issues related to M2M and IoT
1. **Methodology for carrying out the study**

As agreed during the last meeting of the Working group on Policy, Regulation and services in Dhaka, Bangladesh from 18-19th April 2017, the study will be carried out by the Lead Expert in consultation with the other experts from the member countries.

Therefore, in order to pursue the study further, the following questionnaire has been prepared to obtain inputs from the experts from the member countries. Based on the inputs provided, the lead expert will compile and generate a report based on the best practices for the SATRC region.

1. **Questionnaire:**
2. Please provide the details of existing regulatory framework for M2M communications and IoT in your country. Whether any licensing or registration mechanism exists for M2M and IoT services in your country?
3. What is the status/plan of deployment of M2M and IoT in your country?
4. Whether separate E.164 numbering series is being used for cellular/fixed network based M2M services and IoT devices in your country?
5. Whether separate MNC (Mobile Network Code) has been allocated for SIM used for cellular network based M2M devices? (MNC is a part of IMSI which is used for unique identification of SIM)
6. How is the Quality of service of M2M and IoT services being monitored and/or regulated in your country?
7. How the International roaming related issues of cellular network based imported M2M devices are being dealt with in your country?
8. Please provide your views on effective regulatory interventions to promote M2M and IoT related services in your country.

#

# Annexure-II: Response to the questionnaire by SATRC working group experts

1. **Response received from Afghanistan**

1. Still there is no regulatory framework in our country. IoT license is under work, which will be ready to the sector soon

2. There is no particular from government side yet, It might be planed in near future.

 3. Not applicable

4. Not applicable

5. Not applicable

 6. Not applicable

 7. License issue should be resulted.

 Spectrum should be studied and be allowed for IoT.

 IPV6 and addressing ( IPV6 policy and implementation in the county)

1. **Response received from Bangladesh**
2. At present there is no specific regulatory framework on M2M communication and IoT services. IoT and M2M services are yet to get attraction in Bangladesh. MNOs have recently launched some industry based M2M communication solution to enable users to have better control over his/her all devices in more efficient and easy way.

M2M and IoT services are delivered as a part of licensed telecommunication services using the existing licensed spectrum band.Mobile Network operators provides these services by taking prior approval from the regulator or intimating them. Only for vehicle tracking service there is a requirement of license particularly for non-MNO whereas MNOs need to go through a simple registration process.

1. Bangladesh Government has visionary plan to expand digital services to all people which is well defined in plan of Digital Bangladesh by 2021 and relevant policies of Bangladesh. Under PT&ICT ministry through training initiatives government is creating a large base of qualified human resources. Government is also providing innovation fund from where interested IT professionals can get fund to explore their interest on ventures related to M2M and IoT. Bangladesh government has already created platform for IoT expansion by established many IT parks where entrepreneurs will be able to involve themselves from starting to produce sensors, devices related to M2M and IoT services. Vehicle tracking services has got some popularity in Bangladesh. To provide VTS intended companies have to take license from BTRC. Different govt. electricity power supply companies has started to provide smart metering based on M2M communication. Mobile network operators have launched M2M based smart factory, personal devices management etc. M2M and IoT industry is growing and with the time being it will expand in a great speed. So, interested parties have already started their work regarding M2M and IoT services. Thus government will facilitate market better regulatory framework for the expansion of M2M and IoT services.
2. Currently no separate E.164 numbering series is being allocated for cellular/fixed network based M2M services and IoT devices in Bangladesh. As an identifier, already allocated E.164 number series is used for M2M services.
3. No separate MNC allocated for SIM used cellular network based M2M devices. Presently M2M services are being deployed with the MNC already allocated in favor of mobile operators.
4. As specific regulation is yet to be formulated, currently no monitoring of quality of service is present there and it is yet to be regulated. For VTS, licensed operators has to submit periodic reports.
5. We are yet to fix our position on permanent roaming issue. However, we will consult with industry and refer the GSMA and ITU recommendations in this regard.
6. Bangladesh is a country where M2M and IoT services are yet to be popular and adopted widely. We are in favor of taking an approach that facilitates market to grow. To facilitate the growth of IoT, we are in process to formulate a guideline on this.
7. **Response received from Bhutan**
8. Right now, we (Bhutan) have not done anything on M2M communications and IoT. A study will soon be carried out to see how licensing mechanism for M2M and IoT can be adopted including the allocation of frequencies.
9. Right now, there is no deployment of M2M and IoT services in Bhutan, except that the Power Company is exploring the introduction of smart-meter reading.
10. We still have not looked into this issue. However the study on M2M and IOT service will look into the numbering plan for such services. We might explore the possibility of E.NUM as an option for issuance of number for such services.
11. We have not issued such code.
12. We have not defined the QoS for M2M and IoT services.
13. Till date, we have not faced such issues. But we are aware of the issues concerning the roaming of M2M and IoT devices.
14. Since these are new concept in Bhutan, we are in the process of carrying out a comprehensive study on the effective regulatory interventions to promote such services.
15. **Response received from Maldives**
16. *Currently no specific registration/licensing mechanism. But can be generally provided under existing Telecom licenses.*
17. *Some trials and pilot projects by telecom service providers. Commercial deployment planned for 2019*
18. *Being discussed.*
19. *Operators considering using same MNC.*
20. *N/A yet*
21. *N/A yet. But service providers will involve their roaming partners in dealing with the issues once M2M services commercially launched.*
22. *Establishing national regulatory framework for IOT services across the country*
* *Enforce all mobile operators to follow regulatory framework for M2M communications and IoT strategy*
1. **Response received from Nepal**
	1. There is no specific regulatory framework for M2M communications and IoT in Nepal.
	2. Nepal Telecommunications Authority (NTA) has started study to prepare regulatory framework for standardization of M2M communication and IoT in Nepal. After received and approval of regulatory framework, NTA will deploy the licensing or registration mechanism of M2M communication and IoT in Nepal.
	3. Currently there is no regulation for M2M services and IoT devices. That’s why same National Numbering plan is applicable for for cellular/fixed network based M2M services and IoT devices using E.164 numbering scheme.
	4. No.
	5. The Quality of service of M2M and IoT services is being monitored and/or regulated similar to voice and data service of Telecommunications in Nepal.
	6. The International roaming related issues of cellular network based imported M2M devices are being dealt with in Nepal similar to the International roaming related issues of mobile communication (Voice and Data) services.
	7. For effective regulatory interventions to promote M2M and IoT related services in the SATRC countries, following regulatory issues to be addressed by the regulatory authority or government:
* Licensing and spectrum management: Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands.
* Switching and roaming: Encourage development of SIMs and mobile network accounts suitable for large M2M users, roaming mobile devices, and fixed devices in areas of poor reception.
* Addressing and numbering: Large address space needed for globally addressable things (although many IoT devices only need local connectivity) with Deployment of IPv6 by ISPs, public and private sector organizations and use of IMSI for M2M applications.
* Competition: Avoid IoT user lock-in and new barriers to entry, ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions and provide institutional mechanism for ongoing review of laws and regulations for impact on IoT competitiveness.
* Security and privacy: Significantly reduce security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles, encourage security and vulnerability patching of devices, smart city vulnerabilities can be hard to fix but present significant safety issues (e.g. in traffic lights), ensure individual control of profiles, which can be used to infer sensitive personal information, such as medical disorders and reduce potential for discrimination in employment, financial and healthcare services.
1. **Response received from Pakistan**
2. No specific framework for M2M and IoT

1. International & national ICT firms are in early stages of developing innovative services using M2M technology, IoT and green solutions in Pakistan. Examples include advanced metering infrastructure with automated meter reading with real-time or near-time two way communication, Smart city solutions, smart devices/sensors/ actuators, smart farming, health care solutions, smart grids and connected agriculture
2. Same numbering plan being used for cellular and fixed networks

1. As above; No
2. As per QoS of transmission modes, for example, broadband QoS for cellular networks

 6 and 7: Under the Telecom Policy 2015, licensing framework will be reviewed. In this regard, provisions of spectrum, licensing, roaming, security, privacy and related regulations for M2M and IoT will be assessed considering international best practices.

1. http://www.gsma.com/newsroom/gsma-the-rise-of-connected-devices-will-drive-mobile-operator-data-revenues-past-voice-revenues-globally-by-2018#.UTnALM1bduI.email [↑](#footnote-ref-1)
2. http://www.analysysmason.com/Research/Content/Reports/RRE02\_M2M\_devices\_forecast/ [↑](#footnote-ref-2)
3. GE report, published 26 November 2012, http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf [↑](#footnote-ref-3)
4. ECC REPORT 153, NUMBERING AND ADDRESSING IN MACHINE-TO-MACHINE (M2M) COMMUNICATIONS, Luxembourg, November 2010 [↑](#footnote-ref-4)
5. AT&T Comments on Ofcom Consultation Document, Promoting Investment and Innovation in

the Internet of Things, 1 October 2014. [↑](#footnote-ref-5)
6. Public Consultation on Proposed M2M Access Code Allocation Framework, iDA Singapore.Proposed Machine -To- Machine (“M2M”) Access Code Allocation Framework ,11 April 2013 [↑](#footnote-ref-6)
7. National numbering Plan( Issue 1 – 1 October 2016) Info-communications Media Development Authority,Singapore [↑](#footnote-ref-7)
8. https://www.coms-auth.hk/filemanager/statement/en/upload/385/cop-numbering\_e.pdf [↑](#footnote-ref-8)