Consultation Paper No. 21/2016

Telecom Regulatory Authority of India

Consultation Paper

on

'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications'

18th October, 2016

Mahanagar Doorsanchar Bhawan

Jawahar Lal Nehru Marg

New Delhi-110002

Written comments on the Consultation Paper are invited from the stakeholders by 15th November, 2016 and counter-comments by 29th November, 2016. The comments and counter-comments may be sent, preferably in electronic form, to Shri Sanjeev Banzal, Advisor (Networks, Spectrum and Licensing), TRAI on the Email-Id advmn@trai.gov.in Comments and counter-comments will be posted on TRAI's website www.trai.gov.in.

For any clarification/ information, Shri Sanjeev Banzal, Advisor (Networks, Spectrum and Licensing), TRAI, may be contacted at Telephone No. +91-11-23210481

CONTENTS

CHAPTER – I: INTRODUCTION

1.1 The digital space has witnessed exponential evolution in the last couple of years and would continue to evolve rapidly. The latest entrant to the digital space is the Machine-to-Machine (M2M) communications. Expansion and evolution of networks, falling costs of hardware like sensors and actuators, increasing battery life, new business models etc are the major factors leading to the emergence of services like remote monitoring of patients, automatic security systems, connected cars, smart grid etc. The connected devices deliver innovative services by utilizing the M2M communication technologies.

1.2 M2M communication has potential to bring substantial social and economic benefits to governments, citizens, end-users and businesses through increase in productivity and competitiveness, improvements in service delivery, optimal use of scarce resources as well as creation of new jobs.

1.3 Although forecasts indicate a significant opportunity in this field, this industry is still in a nascent stage. The M2M ecosystem is composed of a large number of diverse players, deploying innovative services across different networks, technologies and devices. Providing clarity and consistency of regulation for equivalent services, as well as policies that enable growth, will play a significant role in fully capturing its opportunity to stimulate this market.

1.4 Government of India has recognized the potential of M2M communication and emphasized the same in the National Telecom Policy (NTP) 2012. Accordingly, in May, 2015, the Government has come out with 'National Telecom M2M roadmap' with the purpose of boosting development of M2M based products and to provide efficient citizen centric services in India.

A. Machine to Machine: Definitions

1.5 Broadly, Machine to machine (M2M), which is the acronym for Machine-to-Machine communication, refers[1] to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information.

1.6 M2M is also being inter-changeably used with various other terms - Internet of Things (IoT), Internet of Everything (IoE), Smart systems (Homes, Cities, Meters, Grids etc.). IoT refers to addition of communications and sensing capabilities to a wide range of physical objects. In the coming decade it is expected that millions of IoT devices will be deployed in electric meters, parking meters, thermostats, car components, roads etc. IoT devices will send data directly using protocols such as Wi-Fi and Bluetooth and via mobile networks, specialized networks and over the global network.

1.7 There are various definitions given by Global Standardization organizations for M2M. European Telecommunications Standards Institute (ETSI) has defined M2M[2] 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.'*

---

[1] http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[2] TR 102 725 V1.1.1 (2013-06)

1.8 The International Telecommunication Union (ITU-T)[3] 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.*".

1.9 M2M/ IoT devices will have very big societal impact once they are put together in larger, interconnected, systems. Their biggest market will be smart cities wherein cities are expected to perform smartly in order to efficiently utilize the available infrastructure to improve efficiency and sustainability of a whole range of urban activities. Therefore, many Government and private organizations are funding research on IoT in the areas of modularity, reliability, flexibility, robustness and scalability etc. There are certain characteristics which are broadly shared by M2M/IoT devices.

1.10 According to a Body of European Regulators for Electronic Communications (BEREC)'s report, current M2M services broadly share some of the following characteristics:

- Fully automatic communication of data from remote devices (or with limited human intervention).
- Relatively simple devices that can either be static (e.g. smart meters) or mobile (e.g. M2M devices integrated in connected cars).
- Low volume traffic, often with sporadic or irregular patterns. However, M2M applications have already emerged and/or might emerge in the future that transmits data in greater volumes, especially if demand for video-based services increases (e.g. automatic analysis of surveillance video streams, alarm systems).

[3] ITU recommendations, ITU-T Y.2060 (06/2012)

- M2M services require connectivity though connectivity accounts for a relatively low proportion of the overall revenue opportunity in the M2M value chain.
- Many M2M services are provided via devices designed and produced for the world market and for usage based on global mobility.
- Many M2M devices are designed to have a lifetime of many years and may be installed within equipment or infrastructure that itself has a long lifetime. Therefore, the cost of replacement may be relatively high.
- In most cases, the business model is B2B, even if devices may be aimed at consumers (B2B2C). The business model is usually not B2C[4].

There are different ways in which M2M services could be implemented:

- Different connectivity technologies may be used and, in the case of wireless services, different spectrum bands may be used.
- M2M services may use different protocols to deliver their data. They may be based on the IP protocol but could also use SMS, USSD and/or automatic calls.
- An M2M device is addressed via an identifier (e.g. number(s), IP-address). However, not all M2M devices need global identifiers (e.g. those that are not connected to public networks).

B. M2M applications

1.11 There may be a various types of M2M applications in different verticals. Some verticals and related M2M applications as per industry are given in the table below:

[4] M2M services are changing the relationship between connectivity providers and end-users: the connectivity providers are losing the direct relationship with the end-user (typical B2C model), which becomes, instead, in many cases the prerogative of the "M2M user".

Table 1.1: M2M applications

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
Utilities / Energy	Smart metering, smart grid, Electric line monitoring, gas / oil / water pipeline monitoring.
Health care	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, Tele-medicine, wearable health devices
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

C. Projections

1.12 Industry analysts estimate the number of connected devices could be anywhere from 20 billion to 100 billion by 2020 (shown in the figure

1.1)[5]. Mobile access to the Internet, coupled with the rapid growth of the smartphone market and declining costs of semiconductors has begun to create consumer demand for the IoTs.

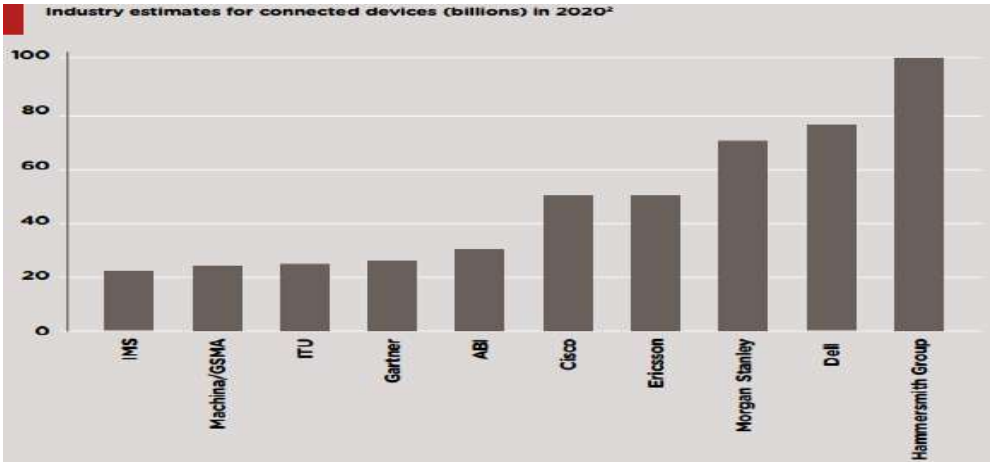


Figure 1.1: Industry estimates for connected devices by 2020

1.13 Telecommunication Engineering Center (TEC) in its technical report[6] while quoting the study by Machina Research 2012, has projected approximately 275 million connected devices in India by 2020 (shown in the figure 1.2).

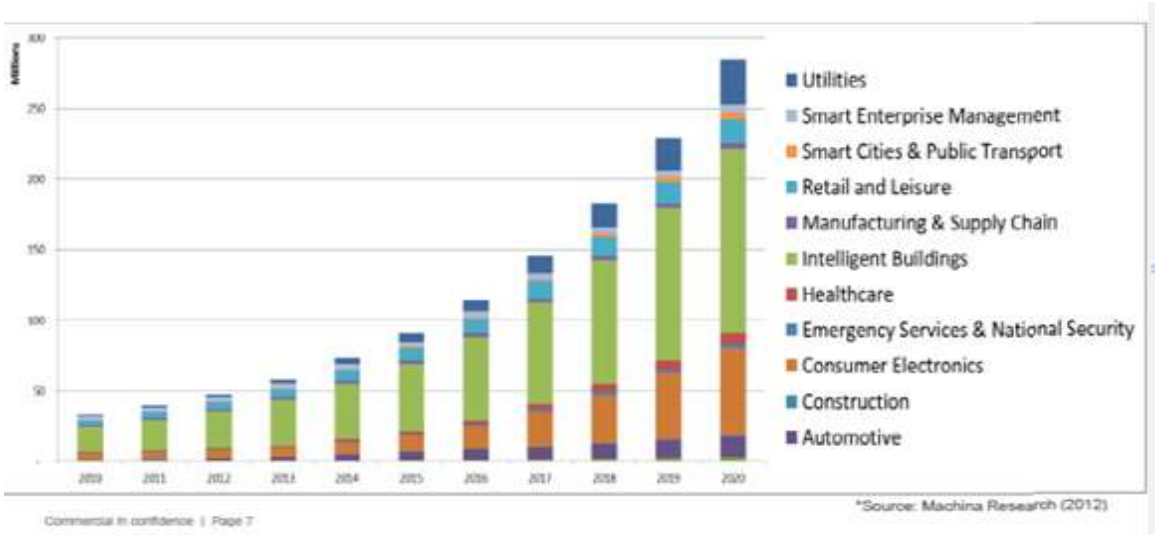


Figure 1.2: Connected devices in India by 2020

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[6] http://tec.gov.in/pdf/M2M/M2M%20Number%20resource%20requirement%20&%20options.pdf

D. Architecture of M2M communication network

1.14 There are a number of verticals/industries that utilize M2M communication network for delivery of services; therefore, it is necessary to have a collaborative approach of having a common Service Layer Architecture. This will not only allow a uniform framework but also achieve economies of scale and interoperability standards across different domains. There are M2M architectures proposed by organisations like, oneM2M, 3GPP, ETSI, Telecommunications Industry Association (TIA) etc. In all these architectures requirements for connectivity, addressing, security, data handling remain the same.

E. Global scenario of M2M standardization

1.15 With standards, it is more likely that a managed service infrastructure could be developed for M2M and shared across diverse independent applications. A new, open infrastructure, object-oriented approach could ultimately lead to services and features common to many applications, thereby reducing complexity, development effort and maintenance costs. There would also be significant operating cost savings since the resulting service infrastructure could be pooled across many independent applications. However, the biggest benefits would come from the ability to allow sensor information to be shared in a secure manner across any application and to allow any device to connect to any application. Due to the need of having a global Partnership in developing standards for M2M communications and the Internet-of-Things (IoT) "oneM2M partnership" was formed to play a vital role to ensure that various industries can benefit fully from the economic growth and innovation opportunities that M2M communications presents.

OneM2M Partnership:

1.16 World's eight leading Standards Development Organizations (SDOs) have formed a partnership to develop specifications to ensure the global

functionality of M2M, allowing a range of industries to effectively utilize the M2M technology. oneM2M is the partnership of the following major ICT SDOs:

i. Association of Radio Industries and Businesses (ARIB)
ii. Telecommunication Technology Committee (TTC) of Japan
iii. Alliance for Telecommunications Industry Solutions (ATIS)
iv. Telecommunications Industry Association (TIA) of the USA
v. China Communications Standards Association (CCSA)
vi. European Telecommunications Standards Institute (ETSI)
vii. Telecommunications Technology Association (TTA) of Korea
viii. Telecom Standards Development Society – India (TSDSI)

1.17 The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect myriad of devices in the field with M2M application servers worldwide. With an "access independent" view of end-to-end services, oneM2M will develop globally agreed M2M end-to-end specifications using common use cases and architecture across multiple M2M applications.

1.18 Besides oneM2M, various other Standards Development Organizations (SDOs) - ETSI M2M, 3GPP, IETF ROLL, ITU, TSDSI etc. are also engaged in standardization activities.

1.19 International Telecommunication Union (ITU) has established various Focus Groups with the objective of developing recommendations relevant to M2M from telecom/ ICT perspective. Some of them are Focus Group on Smart Sustainable Cities (FG SSC); Focus Group on Smart Water Management (FGSWM); Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR & NRR); Focus Group on Smart Cable Television (FG Smart Cable); Focus Group on M2M Service Layer (FG M2M); Focus Group "From/In/To Cars Communication" (FG CarCom);Focus Group on Smart Grid (FG Smart); Focus Group on Cloud

Computing (FG Cloud).

1.20 In June 2015, Telecommunication Standardization Advisory Group (TSAG) also approved the creation of ITU-T Study Group-20 on IoT and its applications including smart cities and communities (SC&C). It will be responsible for international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. The group will develop standards that leverage IoT technologies to address urban-development challenges. A key part of this study will be the standardization of end-to-end architectures for IoT and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.

1.21 TSDSI, in India is the government recognized body working on ICT including M2M standards. It is an industry led, legal entity with participation from all stakeholders including Government, service providers, equipment vendors, equipment manufacturers, academic institutes and research labs etc. It aims at developing and promoting research based India-specific requirements, standardizing solutions for meeting these requirements, contributing to global standardization in the field of telecommunications, maintaining the technical standards and other deliverables of the organization and safe-guarding the related IPR. It is responsible for ensuring the Indian requirements are considered by the global M2M Standards.

F. Global scenario of M2M guidelines and policy framework

1.22 GSMA (Groupe Speciale Mobile Association) has issued *'IoT Device Connection Efficiency Guidelines,'* that outline how devices and applications should communicate via mobile networks in the most intelligent and efficient way. The guidelines include a number of best practice areas such as data aggregation within devices, non-synchronous network access, application scalability and guidance on how to manage

signaling traffic from de-activated or out-of-subscription SIMs. These will help IoT/ M2M device and application developers to expand the number of devices connecting to mobile networks, whilst preventing service outages and ensuring optimal performance that will ultimately enable the market to scale across a diverse range of sectors including automotive, transportation, utilities and health.

1.23 Though presently M2M is a nascent industry, regulators across the globe are realizing the enormous regulatory challenges that need to be tackled for fostering a suitable environment for M2M services. Therefore, various countries have also released consultation papers and surveys to gain an insight on these new developments in order to gather facts and to get an understanding of the issues raised. The details of the same are given in the Chapter-III titled International Practices.

1.24 Interoperability is a key to manage systems and to open markets to competitive solutions. The existence of standards guarantees that components of different suppliers and technologies can interact seamlessly. Internationally, the rules and standards on interoperability of ICT elements in M2M scenario are still evolving. There are enormous challenges while making rules in a multiservice-multi-operator network scenario. Thus there is no clarity on the issues involved. In India, C-DoT (Centre for Development of Telematics) has recently demonstrated open standards-based machine to machine (M2M) communications platform in association with oneM2M.

G. Government of India's policy and initiatives

1.25 Recognizing the potential of IoT/ M2M, emphasis is laid in NTP–2012 as:

"To facilitate the role of new technologies in furthering public welfare and enhanced customer choices through affordable access and efficient service delivery. The emergence of new service formats such as Machine-to-Machine (M2M) communications (e.g. remotely operated irrigation pumps, smart grid etc.) represent tremendous opportunities, especially as their roll-out becomes more widespread."

1.26 Launch of various government programs such as “Digital India”, “Make in India” and “Startup India” will also help immensely in driving the growth of the M2M/IoT industry in the country.

1.27 In addition, many mega projects have been undertaken by the Government of India, which will help in the effective and sustainable utilization of resources by the application of M2M/IoT technology. Some of the major projects are as follows:

a) Development of 100 Smart cities proposed by Ministry of Urban development
b) Setting up of 14 Smart Grid pilots by Ministry of Power
c) Mandating the commercial passenger vehicles of more than 22 seating capacity, to be equipped with GPS, emergency calls etc. by Ministry of Road transport.

1.28 Department of Electronics and Information Technology (DeitY) has released a 'Draft Policy on Internet of Things – 2015'. The objectives of this draft policy are as follows:

i. To create an IoT industry in India of USD 15 billion by 2020. This will also lead to increase in the connected devices from around 200 million to over 2.7 billion by 2020. As per Gartner Report, the total revenue generated from IoT industry would be of USD 300 billion and the connected devices would be 27 billion by 2020 globally. It has been assumed that India would have a share of 5-6% of global IoT industry.
ii. To undertake capacity development (Human & Technology) for IoT specific skill sets for domestic and international markets.
iii. To undertake Research & development for all the assisting technologies.
iv. To develop IoT products specific to Indian needs in the domains of agriculture, health, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, automated metering and monitoring of utilities, waste management,

Oil & Gas) etc.

1.29 As mentioned earlier, in May 2015, Department of Telecom (DoT) published the "National Telecom M2M Roadmap" after seeking inputs from selected stakeholders from the industry. The Roadmap focuses on communication aspects of M2M with the aim to have interoperable standards, policies and regulations suited for Indian conditions across sectors in the country. In addition, Telecom Engineering Centre (TEC) of DoT has also come out with 9 technical reports on M2M detailing sector specific requirements/use cases to carry out gap analysis and future action plans with possible models of service delivery.

1.30 In view of the above background, the DoT through its letter dated 5th January, 2016 **(Annexure)**, has sought the recommendations of TRAI on three aspects related to M2M communications:

a) Quality of Service in M2M Services
b) M2M Roaming Requirements
c) M2M Spectrum Requirements

1.31 While formulating this consultation paper (CP) on M2M issues, the Authority realised that certain other regulatory aspects including licensing framework for M2M service providers, Know Your Customer (KYC) norms for M2M devices, numbering scheme, inter-operability of devices between different sectors, various technical challenges in implementation, allocation and utilization of various network codes, data protection, and privacy issues also need to be deliberated for preparing comprehensive recommendations on the framework of M2M communication for the country. However, it is noted that DoT/TEC is already working on KYC norms, inter-operability and numbering of M2M devices in consultation with the industry. Therefore, the Authority is not raising these issues for consultation. However, in case stakeholders desire to submit their views on these issues too, the same may be submitted alongwith the responses to the issues raised in the CP.

1.32 In India the facility of Mobile Number Portability (MNP) is available to the consumers since January, 2011. It facilitates porting of a mobile number from one mobile service provider to another mobile service provider without changing the mobile number of the consumer. In present telecom market the number is required to be used by humans mainly for voice communication and thus required to be remembered and retained (by a subscriber) due to various compelling reasons viz. banking transactions, business transactions and to access online applications. The same principle does not apply to Number Portability for M2M since in M2M scenario it is expected that there will be different numbering scheme. As no human intervention or voice communication is envisaged, the necessity of porting the number is not anticipated at this stage. In case of change of service provider by a subscriber, the SIM/eUICC provisioning techniques like Over-The-Air (OTA) are being adopted by many operators across the world. In some markets, however, number portability is available in M2M segment also. The Authority feels that in view of the facts mentioned above, there is no apparent requirement of number portability in M2M segment as of now. However, in future, if needed, the Authority would form necessary regulations.

1.33 For drafting this consultation paper, various documents available in the public domain, published by government agencies/departments, telecom regulators in many countries, research agencies/institutions, academic institutions, telecom vendors, operators and international agencies/forums etc were referred with the purpose to make the consultation paper balanced and comprehensive. Excerpts from certain documents, which had domain relevance, are also included in this CP.

1.34 Accordingly, in this consultation paper, Chapter-II deals with the Policy and Technical aspects of M2M communications. In chapter-III international practices in regulating the M2M communication services are covered and the Chapter-IV provides the summary of issues for consultation.

CHAPTER –II: POLICY AND TECHNICAL ASPECTS OF M2M COMMUNICATIONS

2.1 M2M is in its infant stage world over with certain European and western 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.

A. M2M Service provider framework

2.2 Globally M2M connections have increased @ 37.6% CAGR annually for the last five years[7]. As per estimates by Machina Research[8], there will be 29 billion M2M connections by 2024, up from 4.5 billion in 2014. In Indian context, Government's vision of setting up 100 smart cities will give a boost to the proliferation of M2M communication/services market. It can be visualized that once M2M activities are operationalised in Indian smart cities, the demand will percolate into other conventional cities and also to rural areas. TSPs will be able to support only a portion of these connections thus leaving a huge market potential for entry of more operators who will be exclusively dealing with M2M services called the M2M service providers (MSP).

2.3 To design the regulatory framework for M2M Services, there has to be a clear understanding about the M2M ecosystem and its typical

[7] http://www.gsma.com/connectedliving/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

[8] http://www.teoco.com/wp-content/uploads/Machina-Research-White-Paper-M2M-growth-necessitates-a-new-approach-to-network-planning-and-optimisation.pdf

architecture. TEC in its technical report on "M2M Gateway & Architecture"[9], has depicted a generic M2M Network architecture model as shown below:

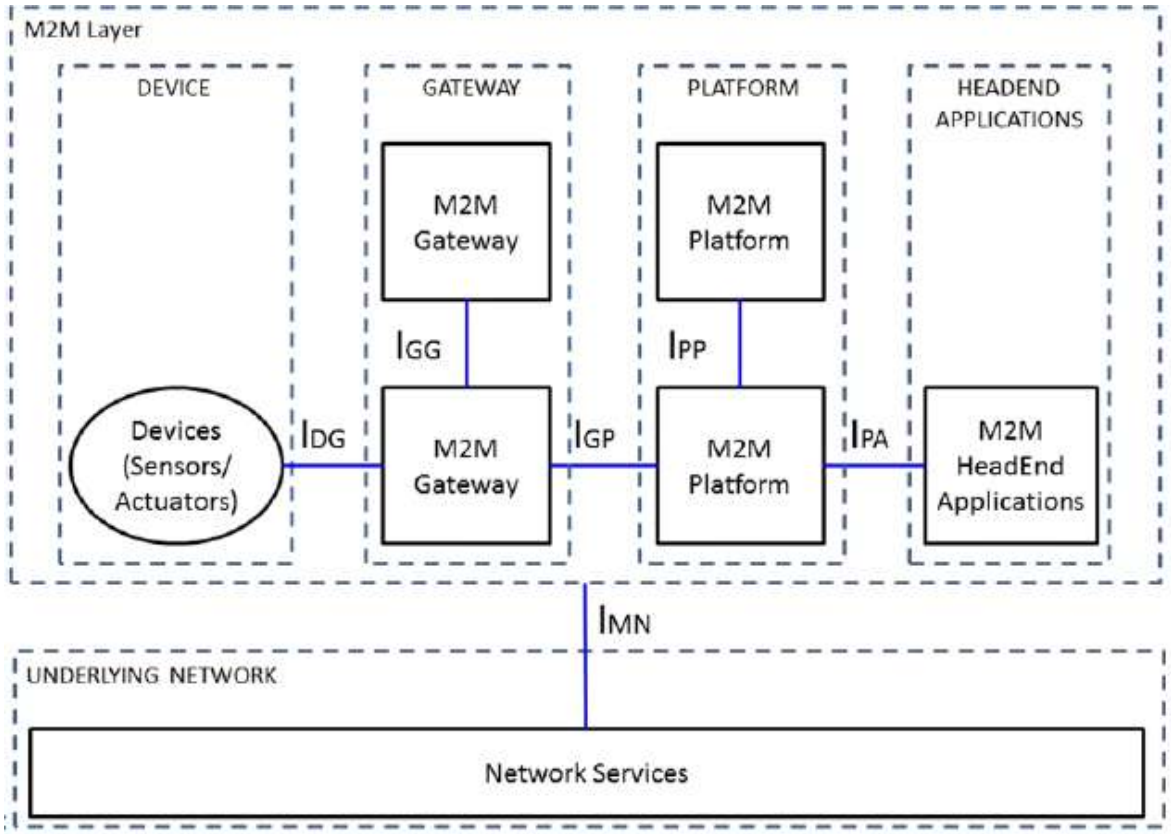


Figure 2.1: A generic M2M Network architecture model

2.4 The key components of this generic M2M Network architecture model are Device, Gateway, Platform, Head-End applications and underlying network. Based on the possible fragmentation and combination of various segments of the model, shown in the figure, there can be various service delivery models. Depending on the model that is selected, the role of the M2M Service Provider can be one or more of the following:

- Provision of platform only
- Provision of platform and applications
- Provision of gateway and platform
- Provision of gateway, platform and applications

[9] http://tec.gov.in/pdf/M2M/M2M%20Gateway%20&%20Architecture.pdf

- Provision of devices, gateway and platform
- Provision of devices, gateway, platform and applications
- Provision of devices, gateway, platform, applications and underlying network

Different verticals and applications may require deployment of particular service model(s) based on its specific requirements.

2.5 There are number of verticals/ industry segments as mentioned at Para 1.11 above where there is immense potential for proliferation of M2M/IoT. Also according to the estimations by various agencies as mentioned at Fig 1.1 the number of M2M/IoT devices are going to be in the range of 20 billion to 100 billion by 2020. These figures indicate that the role of MSP will not only to provide M2M services, but may also include integration of different parts of a city infrastructure which usually fall under the purview of different bodies, from utilities to public works bodies, with no central body controlling the cyber-security standards across these organizations. As more systems are connected, the task of preserving their security posture becomes exponentially more complex. For example- a hacker might be able to tinker with electronic road signs and bring a city to a standstill. Further in the larger context, a hacker may be able to penetrate into important establishments and pose a threat to national security triggered due to online systems. Thus for areas activated with M2M services, there is a strong case for use of dedicated network infrastructures and services that are reliable and secure. Thus role of the M2M service providers should not be treated in isolation. Further, it is necessary that such an entity (MSP) could either be a licensed entity with certain obligations cast upon it or be a registered agency with DoT.

2.6 The proliferation of M2M/IoT is definitely to touch various aspects of the life of a common citizen. Thus mass adoption of M2M/IoT warrants for a robust framework to safeguard the interest of consumers, inter operator

operational aspects and certain regulatory obligations with regard to maintaining QoS, tariffs and roaming etc. Without proper robust framework, the M2M market will mushroom into an unorganized sector and enforcement to regulating guidelines may become difficult. The regulations and norms can be obviously lightweight but should be effective enough at ground level. Mushrooming of Cable operators in the country in an unregulated way is a perfect example where subsequent digitalization of Cable networks became a tedious task. Hence, a long term vision is required to maintain a fine balance between proliferations, orderly growth and enforcement of monitoring mechanism and regulatory interventions for M2M/IoT market.

2.7 'National Telecom M2M roadmap'[10] May, 2015 has discussed this issue and it has favoured to have lightweight regulations towards M2M service providers. The 'National Telecom M2M roadmap' envisages to have lightweight regulation towards M2M services and addressing concerns like interface issues with Telecom Service Provider, KYC, security and encryption (for the purpose of lawful interception at TSP level), all M2M service providers utilizing telecom facilities from authorized TSPs should have MSP (M2M service Provider) registration as in case of OSP registration.

2.8 The above roadmap envisages registration of M2M service providers (MSPs) similar to that of Other Service Providers (OSP) category. As per New Telecom Policy (NTP) 1999, agencies catering to tele-banking, tele-medicine, tele-trading, e-commerce etc were allowed to operate by using infrastructure provided by various access providers for non-telecom services under OSP category. In this category Call Centers, both International and Domestic, in the country and services like Network Operation Centers and Vehicle Tracking Systems, were also included. As per the OSP registration terms and conditions, Application Service Providers could take telecom resources from authorized TSPs only and

[10] http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

may not infringe upon the jurisdiction of other authorized TSPs and they cannot provide switched telephony.

2.9 Unlike MSPs, there are no issues of mobility, numbering, roaming and interoperability with the OSPs. Also many M2M services are supposed to be mission critical in nature in city operations. Therefore the issue for consultation is whether MSP could be a licensed entity with moderately lightweight licensing/regulatory requirement or it could be a registered agency with DoT.

2.10 Internationally, MSPs are Mobile network Operators (MNOs) and Virtual Network Operators (VNOs) or Mobile Virtual Network Operators (MVNOs). Currently, the most popular vertical M2M segment among service providers is automotive/transport/logistics. The largest international M2M service providers based on M2M cellular connections are AT&T, China Mobile, China Unicom, Deutsche Telekom, Orange, Sprint, Telefonica, Telenor, Verizon and Vodafone. MSPs are placed under regulated regime in most of the countries, eg; In Singapore M2M Services provider has to apply for SBO (Individual) Licence. Similarly in many countries MSPs are registered with telecom regulator or licensor to provide the services. Mostly a light-handed licensing regime is adopted worldwide for provision of M2M services by interested services providers.

2.11 Like other countries the existing TSPs would also like to provide M2M services in India as they have their own supporting ICT infrastructure. In the recent past some TSPs have launched 4G/LTE services and some are using unlicensed spectrum band for providing Wi-Fi based broadband services using Wi-Fi hotspots. A few TSPs are in the process of building M2M/IoT based network in India. In context of M2M services, Wi-Fi hotspots will play major role as a part of ICT infrastructure. For TSPs having access service/ISP license and wanting to provide M2M services as separate service, one alternative could be to amend their license to facilitate M2M services or add a chapter of authorisation in the Unified License for the new licensees.

2.12 The NTP-2012 envisages facilitating entry of Virtual Network Operators (VNOs) in Indian telecom sector for introducing competition in the area of service delivery. The Authority in its recommendations dated 1st May, 2015 recommended for introduction of VNOs in Indian telecom sector. Further, it recommended various licensing provisions for VNO operators. The Government has accepted Authority's recommendations and has issued guidelines and UL(VNO) license document on 31st May,2016. For provision of M2M services one option could be adding one chapter in VNO license so that MSP can obtain authorization for M2M services using backend infrastructure of the existing TSPs.

2.13 In view of the foregoing, following issues are raised for the consultation of stakeholders.

Q1. What should be the framework for introduction of M2M Service providers in the sector? Should it be through amendment in the existing licenses of access service/ISP license and/or Licensing authorization in the existing Unified License and UL (VNO) license or it should be kept under OSP Category registration? Please provide rationale to your response.

Q2. In case a licensing framework for MSP is proposed, what should be the Entry Fee, Performance Bank Guarantee (if any) or Financial Bank Guarantee etc? Please provide detailed justification.

Q3. Do you propose any other regulatory framework for M2M other than the options mentioned above? If yes, provide detailed input on your proposal.

B. Identification of spectrum bands suitable for M2M communications

2.14 In the case of the use of radio technologies, M2M is based on the use of both the licensed and the unlicensed spectrum. Before one gets into the actual spectrum requirement or the frequency bands that are to be made

available, it is important to understand the type of networks where M2M technologies are used.

Networks used for M2M Communication

2.15 There are several communication technologies in prevalence today. These can broadly be classified based on communication networks i.e. Personal Area Network (PAN), Local Area Network (LAN) and Wide Area Network (WAN) etc. In these technologies both wireless and wired connections are possible.

2.16 Various technologies that can be leveraged for M2M communication are depicted in the figure below:

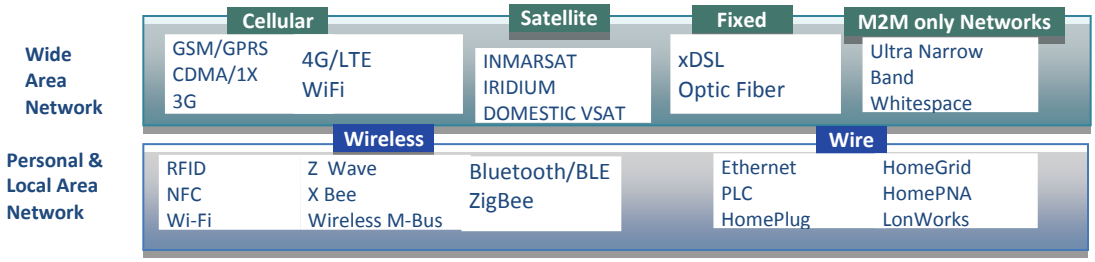


Figure 2.2: Technologies for M2M communications

i. WPAN:

A Personal Area Network (PAN) is a network used for data transmission among personal devices such as computers, phones, personal digital assistants, wearables, etc. Wireless PAN or WPANs can be used for communication among the personal devices (intra-personal communication), or for connecting to a higher level network and the Internet (an uplink). Technologies used in PAN are INSTEON, IrDA, Wireless USB, Bluetooth, BLE, Z-Wave, ZigBee, Body Area Network RFID etc. Among these Zigbee and Z-Wave are considered to be a Low Rate WPAN (LRWPAN).

ii. WHAN/WLAN:

A Local Area Network (LAN) is a network that interconnects computers, phones and other devices within a limited area such as a residence, school, laboratory, or office building. An example of a Wireless LAN is

Wi-Fi. A home network or home area network (HAN) is a type of LAN with the purpose to facilitate communication among digital devices present inside or within the close vicinity of a home. BLE, Zigbee and Z-Wave are technologies that fall in this domain. Z-Wave, a standard built on 802.15.4 was developed specifically with the needs of home automation device makers in mind.

iii. WAN:

A wide area network (WAN) is a telecommunications network that extends over a large geographical distance. Wide area networks are often established with leased telecommunication circuits. In wireless this includes cellular technologies like GSM, CDMA, LTE as well as Satellite technologies and IoT technologies.

iv. LPWAN

Low Power Wide Area Networks (LPWAN) is a new type of WAN that is suited for M2M communication because of characteristics that render themselves more compatible. Outside the cellular world, LPWAN solutions such as Sigfox, LoRa, Weightless and Ingenu are the current front runners. There are other technologies also in the LPWAN market supporting several million devices such as SilverSpring's Starfish, Cyan's Cynet, Accellus, Telensa, Waviot etc.

2.17 Today majority of M2M/IoT applications are in narrow band, generally consuming few kbps data and can operate over second generation mobile networks (2G) or use low cost narrow band short range devices. A number of new M2M/IoT oriented technologies are also emerging typically geared towards narrower band applications with potentially large volumes of data transactions, using short/long range technologies and minimum/very low power consumption to preserve battery life.

2.18 There could be three key differentiating elements to categorise these devices viz. range, bandwidth and QoS. This differentiation helps in grouping and choosing particular M2M devices.

- **Range:** Location (e.g. indoor, outdoor), coverage, distribution, degree of mobility: stationary, nomadic or continuously moving.
- **Bandwidth:** Bit rate, data volume, transmission duty cycle, software update requirements
- **QoS:** Security, criticality, sensitivity to delay, jitter or error.

Therefore, the grouping of application for M2M can be done based on range, bandwidth and QoS, reflecting the predominantly narrow band nature of most M2M applications. The groupings are shown below along with examples of typical applications in each case.

Table 2.1: Grouping M2M applications based on range, bandwidth and QoS

Band	QoS	Area	Range
Narrow Band	**Low**	**Local** Consumer white goods, fitness/training	1
		Wide Fitness/training, street lighting, vending match	2
	Medium	**Local** Security alarms, controlled devices, road tolls	3
		Wide Smart meters, residential HVAC[11]	4
	High	**Local** EPOS[12], process monitoring, fire alarms	5
		Wide Area EPOS, fire alarms, heart monitors	6
Wide Band CCTV, consumer video glasses, advertising displays			7
Satellite Deepwater fishing, air transport, pipelines			8

2.19 In addition, a number of secondary characteristics like extent of deployment internationally, application lifecycle, power requirements,

[11] HVAC(heating, ventilating, and air conditioning)

[12] EPOS (Electronic Point of Sale)

accessibility, size and cost etc also influence the choice of technology or frequency band.

Estimation of Spectrum for M2M communication:

2.20 Spectrum management is an important issue for ensuring availability and capacity for M2M/IoT communications. IoT devices communicate using a range of different protocols, based on their connectivity requirements and resource constraints. These include short-range radio protocols such as ZigBee, Bluetooth and Wi-Fi; mobile phone data networks; and in more specialised applications such as traffic infrastructure, longer-range radio protocols such as Ultra-Narrow Band (UNB). To communicate to remote networks, IoT devices may send data via a gateway with a wired (PSTN, Ethernet, power line or DSL) or wireless (2G, 3G, 4G/LTE or UNB) connection to the global Internet or telephony network or directly over one of these mediums. For consumers, the gateway will often be a smartphone or home wireless router. Businesses will make use of their existing corporate data networks. Devices communicating over kilometres need access to the 300 MHz to 3GHz spectrum area, while centimetre or millimetre contactless transactions may use near field communications. Some IoT applications may also make use of AM/FM bands in the VHF range.

2.21 Various spectrum bands which can be optimally used for M2M communication could be in unlicensed frequency range and/or in the licensed frequency range. Sub GHz spectrum bands are also very useful from the point of propagation characteristics and the ecosystem development. The main advantages of sub-GHz band are long range, deep penetration, low interference, low power consumption, low Total Cost of Ownership (TCO). These bands are suitable for sensors, devices which are placed in deep pockets, underwater or normally inaccessible areas.

2.22 The International Telecommunication Union's Radio communication sector (ITU-R) has reserved several frequency bands for Industrial, Scientific and Medical (ISM) applications. These ISM bands are unlicensed, and vary slightly from country to country. Popular ISM bands are 433 MHz, 868 MHz, 915 MHz and 2.4 GHz, which are used by wireless communication systems such as remote controls, cordless phones and Wi-Fi etc. Worldwide the 2.4 GHz band became very popular because it is allowed for unlicensed use in all regions. The ubiquity of the 2.4 GHz band makes development and distribution of 2.4 GHz-based products across nations easier. Wi-Fi can also operate in the 5.8-GHz band. However, since the range of 5.8-GHz radios inside buildings is shorter compared to 2.4 GHz, 5 GHz is mainly used in enterprise applications to ensure good Wi-Fi coverage. These existing license-exempt bands are widely used worldwide for M2M communication.

2.23 Internationally, studies by the European Commission have suggested that a licence exempt model is most effective for IoT development, since it avoids the need for contractual negotiations before devices are manufactured and used, allowing the production of large numbers of cheap devices. Further, there is no roaming requirement within the country in such bands. Generic Bluetooth, ZigBee and Wi-Fi standards also work in unlicensed spectrum. In Europe system, SIGFOX, uses the most popular European ISM band (the ETSI and CEPT defined 868MHz) and 902MHz band is used in the USA. A review by the Korean government, found an increasing demand for unlicensed, low-power, long distance communications to connect devices in remote areas.

2.24 In India too, two bands 2.4GHz (2.400-2.4835 GHz) and 5.8GHz (5.825-5.875GHz) have been defined as License-exempt bands for indoor and outdoor applications. In addition, 5.15-5.25GHz and 5.725-5.825GHz are also available for indoor uses in unlicensed bands. In addition, TRAI has recommended to the Government for delicensing the V-band (57-64GHz)

which can also be considered for M2M communication if devices are manufactured in this band too.

2.25 There are other bands in Sub-GHz band which are also made license exempt for Indoor applications. The specifications of these bands are given in table 2.2:

Table 2.2: Delicensed bands in Sub GHz band in India

S.No.	Frequency Band	Power Requirements	Use of this frequency band
1	433-434 MHz	Maximum Effective Radiated Power: 10mW Maximum Channel Bandwidth: 10KHz	Indoor applications
2	865-867 MHz	Maximum Transmitted power: 1W Maximum Effective Radiated Power: 4W Maximum Channel Bandwidth: 200KHz	Any low power device or equipment

2.26 With the development in IoT field, 400 MHz band and 800 MHz band have become preferred candidate bands for IoT worldwide. In the future, 5G is expected to accommodate a wide range of IoT use cases with advanced requirements, especially in terms of latency, resilience, coverage, and bandwidth to fulfill vertical-specific requirements. European administrations in CEPT, which is studying IoT and M2M spectrum needs, offer a view that most M2M applications existing today or foreseen can be carried over Short Range Devices (SRD), RLAN, Private Mobile Radio (PMR) or MFCN (Mobile/Fixed Communication Networks).

2.27 In licensed band approach M2M can be deployed in any harmonised mobile networks band, including 700MHz, 800MHz and 900MHz. Conference of European Postal and Telecommunications Administrations

(CEPT) Electronic Communication Committee (ECC) Europe Decision (15)01 considers Machine to Machine (M2M) as a national option in the 733-736MHz and 788-791MHz ranges.

2.28 700 MHz band is a sought after band for LTE deployment around the world due to its efficiency and propagation characteristics. In this band, the APT700 FDD plan, designated as B28, is being adopted as a prime band for Long Term Evolution (LTE) technology by a number of countries in the Asia-Pacific (APAC), Middle East, Europe and Latin American region. The APT700 band plan offers 2x45 MHz contiguous spectrum.

2.29 In India too 700MHz is being put to auction in the upcoming auction under 700MHz APT band plan in band-28 configuration. The 3GPP Band Plan-28 comprises of 703-748 MHz (45 MHz) as uplink frequency and 758-803 MHz (45 MHz) as downlink frequency with 10 MHz center gap between both uplink and downlink. The center spacing of 10 MHz has been kept to provide sufficient isolation between uplink and downlink to prevent signal pilferage and mitigate self-band interference from uplink to downlink. Since M2M devices work in low power environment in comparison to commercial cellular networks, the bandwidth requirement of M2M devices are also low. In order to ensure optimum and efficient utilization of the center gap of 10 MHz (748-758 MHz), one option could be to explore technical feasibility of utilizing a portion of center gap spacing for say 3 MHz (751-754 MHz) for M2M operations as a long term perspective as unlicensed band for M2M/IoT usages. However this will require technical feasibility and interference study.

2.30 The table 2.3 consists of possible candidate bands, in sub GHz bands, with their usage as per National Frequency Allocation Plan (NFAP) that can be put in the consideration zone for their use for M2M/IoT.

Table 2.3: Possible candidate bands for M2M communication

S.No.	Frequency Bands/Spots	Usage as per NFAP 2011
1	380-389.9 MHz, 390-399.9 MHz, 410-430 MHz	May be considered for digital radio trunked systems on a case-by-case basis.
2	402-405 MHz	Very low power remote cardiac monitoring RF wireless medical devices, medical implant communication/telemetry systems and other such medical RF wireless devices.
3	406.1-450 MHz	May be considered for digital seismic telemetry on a case by-case basis.
4	410-420 MHz	Fixed mobile (except aeronautical mobile) and space research.
5	420-430 MHz	Fixed mobile (except aeronautical mobile) and radiolocation.
6	430-432 MHz	Radiolocation, fixed mobile (except aeronautical mobile) and amateur services.
7	432-438 MHz	Radiolocation, fixed mobile (except aeronautical mobile), amateur and Earth exploration-satellite (active).
8	433-434 MHz	Low power short range devices for indoor applications on a non-interference, non-protection and non-exclusive basis.
9	434-438 MHz	Amateur service.
10	436.525 MHz	Earmarked for demonstration of equipment on non-interference, non-protection and non-exclusive basis.
11	438-440 MHz	Radiolocation, fixed mobile (except aeronautical mobile) and amateur services.
12	440-450 MHz	Fixed mobile (except aeronautical mobile) and radiolocation.

S.No.	Frequency Bands/Spots	Usage as per NFAP 2011
13	441.6 MHz	May be considered for anti-collision device applications on a case-by-case basis.
14	450-460 MHz	Fixed mobile.
15	450.5-457.5 MHz and 460.5-467.5 MHz	May be considered for IMT applications on a case-by-case basis.
16	460-470 MHz	Fixed mobile, meteorological satellite (Space to Earth)
17	466.8 MHz	May be considered for anti-collision device applications on a case-by-case basis.
18	470-520 MHz and 520-585 MHz	Will be considered for fixed and mobile services on a case-by-case basis.
19	806-890 MHz	Broadcasting and mobile satellite services except aeronautical mobile satellite service may be considered
20	806-811 MHz	Earmarked for mobile trunked radio system to be used predominantly for captive networks. May be considered for requirements for Public Mobile Radio Trunked Systems which cannot be met in any other bands.
21	811-814 MHz	Earmarked for spectrum efficient digital Public Mobile Radio Trunked Systems (PMRTS) and Captive Mobile Radio Trunked Systems (CMRTS).
22	814-819 MHz	Earmarked for mobile radio trunked systems to be used predominantly for PMRTS.
23	819-824 MHz	May be considered for PMRTS and CMRTS.
24	849.0125-849.1250 MHz	SCADA applications except for a few locations

S.No.	Frequency Bands/Spots	Usage as per NFAP 2011
25	851-856 MHz	Earmarked for mobile trunked radio system to be used predominantly for captive networks. May be considered for requirements for PMRTS which cannot be met in any other bands.
26	856-859 MHz	Earmarked for spectrum efficient digital PMRTS and captive mobile radio trunked systems.
27	859-864 MHz	Earmarked for mobile radio trunked systems to be used predominantly for PMRTS.
28	864-869 MHz	May be considered for PMRTS and CMRTS.
29	865-867 MHz	Low power devices or equipment for any application.
30	869-889 MHz	Earmarked for cellular telecommunication systems, including WLL.
31	890-902.5 MHz and 935-947.5 MHz	Earmarked for cellular telecom systems.
32	902.5-915 MHz and 947.5-960 MHz	May be considered for cellular telecom systems on a case-by-case basis.

2.31 There is a need to clearly identify the bands as well as the quantum of spectrum for M2M communication at this stage itself so as to promote ecosystem development in those bands. In view of the above, the following questions are put for consultation:

Q4. In your opinion what should be the quantum of spectrum required to meet the M2M communications requirement, keeping a horizon of 10-15 years? Please justify your answer.

Q5. Which spectrum bands are more suitable for M2M communication in India including those from the table 2.3 above? Which of these bands can be made delicensed?

Q6. Can a portion of 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) be used for M2M communications as delicensed band for short range applications with some defined parameters? If so, what quantum? Justify your answer with technical feasibility, keeping in mind the interference issues.

C. National/ International roaming: Technical and interconnection issues

2.32 Presently, global level M2M device penetration in the cellular network is growing at a slow pace. However, it is forecasted that the numbers will increase at exponential rate in the near term. While it can be 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. 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. For example- international automobile manufacturers are already manufacturing automobiles with embedded SIMs which are capable of communicating with various entities like automobile maintenance services to remotely and dynamically monitor the performance of the machine, or with law enforcement agencies and emergency services in the event of the automobile facing emergencies like accident, theft etc. There should be a policy framework in place to facilitate seamless operation of such machines when imported to Indian ecosystem.

2.33 Similarly, there is a need to have policies to ensure that when a machine manufactured in India gets exported to a foreign land, its operation is

guaranteed seamlessly. The global nature of M2M in fact requires international alliances to be developed between the main mobile operators across countries. While such tie ups provide for international operation of M2M systems, it will also give rise to technology lock in as the users won't be able to move out of the agreement so reached between two operators. Such tie ups by major players may put barriers in the way of smaller players entering global competition in the field of M2M services. Other challenges include identity management and security, configuration management, service layer, and connection management for M2M roamers.

2.34 M2M device manufacturers would face challenge when seeking to deploy M2M products and services on a global scale if they follow traditional handset or tablet business models. For each country, the manufacturer would need a SIM card with a country-specific International Mobile Subscriber Identity (IMSI) code embedded in each M2M device to be distributed in that particular country. This would mean maintaining country-specific inventory at each place of manufacture, leading to very high inventory management costs.

2.35 Globally there are commercial models between mobile operators that provide a practical solution for accommodating and facilitating the extra-territorial use of IMSIs and MSISDNs on a bilateral commercial basis. Foremost among these is the "International M2M roaming framework"[13] that addresses and makes transparent international roaming used explicitly for M2M services. This roaming framework enables the use of the home carrier's IMSI and MSISDN to provide services on a global basis through a single SIM architecture.

2.36 TSPs presently have been catering to their subscriber's international wireless connectivity through roaming agreements with service providers' in other countries. To facilitate adoption of these types of international

[13] www.cept.org/Documents/wg-nan/15775/ATT_Consultation-Submission

roaming arrangements on commercial terms, the GSMA has developed a series of roaming contract templates. These roaming templates[14], contain common industry-accepted terms and conditions that expedite the negotiation of roaming agreements. Commercially negotiated roaming arrangements that enable these subscribers to receive service outside their home country have been in place since last few years. In 2012, GSMA adopted an "M2M Annex" template for international roaming. The Annex mandates transparency in the provision of M2M services by requiring the parties to agree to identify their M2M traffic separately from other traffic and to exclude traditional wireless services.

2.37 There are also concerns of security and identity of the roamer. The M2M device may be required by Lawful Enforcement Agencies (LEA) for any reasons and it is cumbersome to trace the credentials of device in short duration of time. Therefore, there must be mandatory clauses in the roaming agreements of operators to define and circumvent the threats arising out of roaming on permanent basis, or at least have some special terms regarding permanent roamers. Recently in Germany, Federal Network Agency (BNetzA) released new rules, according to which the use of extraterritorial IMSIs for M2M services provided in Germany as well as the use of German IMSIs for extraterritorial services is possible.

2.38 On the basis of the national numbering plan, MNC codes are assigned to TSPs. MSP may be established TSPs or specialized operators (VNOs) who have their own products and applications riding on TSPs network for connectivity and network related arrangements. Mobile network codes (MNC) directly available with such service providers can be helpful for their branding and will also help to facilitate their roaming requirements efficiently. Such MSPs can have embedded Universal Integrated Circuit Card (eUICC) comparable with the SIM card which describes physical

14 http://www.gsma.com/newsroom/wp-content/uploads/2012/06/IR2180.pdf

characteristics of the SIM. SIM or USIM (UMTS SIM) software are resided over eUICC as an application.

2.39 Opening up access to MNCs could stimulate competition by enabling balanced negotiations that promote the growth of M2M. A large MSP holding its own MNC could have more leverage when entering negotiations with a potential TSP partner 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 independently, competition in the marketplace for M2M would be enhanced. Furthermore, switching to a new TSP at any stage would be much simpler and less costly for an MSP because the SIM cards that are installed in the M2M devices would not need physical replacement. However, it is important to estimate segment wise the percentage of M2M devices shall require national and international roaming.

2.40 The Authority has prescribed the tariffs for national roaming services in the form of ceiling tariffs through the Telecommunication Tariff (60th Amendment) Order, 2015 dated 27.02.2015 as tabulated below:

Table 2.4: Ceiling Tariff

Item	**Ceiling tariff as per Telecommunication Tariff (60th Amendment) Order, 2015**
Outgoing local voice call	Re. 0.80 per minute
Outgoing long distance (inter-circle) voice call	Rs. 1.15 per minute
Incoming voice call	Re. 0.45 per minute
Outgoing local SMS	Re. 0.25 per SMS
Outgoing long distance (inter-circle) SMS	Rs. 0.38 per SMS

2.41 In view of the above the issues for consultation are as below:

Q7. In your opinion should national roaming for M2M/IoT devices be free?

(a) If yes, what could be its possible implications?

(b) If no, what should be the ceiling tariffs for national roaming for M2M communication?

Q8. In case of M2M devices, should;

(a) roaming on permanent basis be allowed for foreign SIM/eUICC; or

(b) Only domestic manufactured SIM/eUICC be allowed? and/or

(c) there be a timeline/lifecycle of foreign SIMs to be converted into Indian SIMs/eUICC?

(d) any other option is available?

Please explain implications and issues involved in all the above scenarios.

Q9. In case permanent roaming of M2M devices having inbuilt foreign SIM is allowed, should the international roaming charges be defined by the Regulator or it should be left to the mutual agreement between the roaming partners?

Q10. What should be the International roaming policy for machines which can communicate in the M2M ecosystem? Provide detailed answer giving justifications.

Q11. In order to provide operational and roaming flexibility to MSPs, would it be feasible to allocate separate MNCs to MSPs? What could be the pros and cons of such arrangement?

D. Security and Privacy of Data

2.42 With the development and proliferation of M2M services, it becomes increasingly important to ensure secure and reliable communication among connected M2M devices. Different services will have different requirements for security and resilience. Many consumer services will not require a highly resilient network connection since temporary service interruptions will not significantly impact the integrity of the service

provided. On the other hand, services that control important processes will require high levels of security and service availability.

2.43 According to a document by TEC of DoT, following general security requirements are applicable to M2M networks:

- **Availability**: Information network should be available for use of the concerned parties in the manner intended. This can be ensured by monitoring the network at device level, communication level and at the control centre end.

- **Authentication**: This should provide assurance that a party in data communication is who or what they claim to be.

- **Authorization**: This security service should ensure that a party may only perform the actions that they are allowed to perform.

- **Integrity**: Integrity should ensure that data/ information cannot be altered in an unauthorized or malicious manner. Architecture should include strong point to point communication schemes to prevent spoofing and injection of false data.

- **Confidentiality**: Data and information should be protected from being disclosed to third party. Confidentiality of data and information is achieved by providing role based access at both data and information level and at device level.

2.44 Further, as per the 'National Telecom M2M Roadmap' for M2M services, in general data security and privacy issues will arise at the following levels:

i. **M2M data within telecom operator's domain**: License conditions enjoin all TSP's to take all necessary steps so as to maintain security of the network & confidentiality of data related to third parties. The encryptions used in the network should conform to the guidelines contained in IT Act. TSPs are limited to providing data transfer

mechanism/media transparently from end devices to M2M platform, hence existing security & encryption related regulation in licenses & IT Act governing current data services should be sufficient to deal with them. The existing provisions of the licenses applicable for TSP's for interception & monitoring of data by the LEAs shall also be applicable in case of M2M services.

ii. **M2M data within M2M service provider's domain**: M2M will enable creation of a wealth of information covering various aspects of economy and society which will have immense potential use for public welfare but at the same time it can give rise to privacy concerns of individuals. The magnified potential for breach of privacy emanate in M2M is due to multiplicity of data recording points in the network i.e. Database of M2M service provider, Data points in database of TSPs, Home Gateways/devices. The issues require comparison of M2M security and privacy framework with those of existing provisions of IT Act. Also M2M security framework is closely interlinked to interface and architecture standards, on which it is learnt that oneM2M alliance and TEC working groups are currently deliberating. Standards need to be followed in conjunction with IT Act, governing current data services, which should be sufficient to deal with such requirements.

iii. **Security at sensor/ device level**: M2M device should use only genuine IMEIs & ESNs due to security concerns. Non-genuine IMEIs & ESNs should not be allowed in devices. Thus, existing IMEIs guidelines for handset could be applicable in the case of M2M devices as well.

iv. **Security at Network level**: M2M will result in availability of large number of devices on Internet or public network and any unauthorized access to/ by these devices may have serious implications. MSPs and TSPs need to device suitable mechanism for their respective network protection.

2.45 With the advent of cloud computing, a plethora of M2M applications and databases will be hosted on the cloud. For instance, one of the key issues to be noted for hosting of application on cloud is the fact that as per the existing telecom licensing guidelines, subscriber data cannot be taken outside India. However, in cloud computing many of the M2M applications will be hosted on servers located outside India. This poses both a regulatory compliance challenge and data security issue.

2.46 The National M2M Roadmap states that "*From security perspective, there is a strong case for all M2M Gateways and application servers, servicing the customers in India, to be physically located in India. But MSP with small customer base in the country may find it difficult to have complete back-end technical setup due to lack of economy of scale. Also, trade reciprocity, privacy, non- disclosure conditions etc. may require us to have view based on practices adopted by other countries in this regard. Decision regarding location of servers in various other services i.e. e-mail, social media etc. is likely to have a bearing on M2M services as well. All such relevant factors need consideration and physical location shall be in consonance with decisions in other services*."

2.47 The presence of servers outside the country also poses a challenge for Law Enforcement Agencies (LEAs). Lawful Intercept (LI) is the legally approved surveillance of a telecom network. It is an important tool for investigating and prosecuting criminal (cyber) activities and terrorism. In terms of regulation, LI reposes an obligation on TSPs to grant Law Enforcement Agencies (LEAs) access to their network/services.

2.48 Besides security challenges at the national level, M2M communications can pose a threat to privacy. Deriving value from IoT depends on the ability of organizations to collect, manage and mine data. Securing such data from unauthorized use and attacks will be a key concern.

2.49 The predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car and with

wearables and ingestible, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely to want privacy. Because of the constant 'always on' connection, it is difficult to determine the types of personally identifiable data being collected. Today organizations are carrying out Big Data analytics; information so extracted is used for carrying out marketing activities amongst other things. It is said that Big Data can even predict an individual's future actions. Although Big Data provides immense opportunity for organizations, individuals, governments and society to mine information for several uses; along with these opportunities emerge additional risks. Many of the future benefits from the M2M are likely to be delivered by new services based on the analysis of data from a wide range of sources. Some of this data may be personal or commercially sensitive, so it will be important to ensure that it is stored and processed securely and in the manner in which users have previously agreed.

2.50 With IoT, devices typically gather data and stream it over the Internet to a central source, where it is analyzed and processed. A number of applications data on health, location, financial, and other sensitive information. This information may be used to commit a crime, or the location itself may be the target of a crime. Such threats can impact the nation's security and financial health. There are related problems of loss of privacy when confidential information is lost or intercepted, lawfully or otherwise.

2.51 The GSMA has developed 'The GSMA IoT Security Guidelines', in consultation with the mobile industry and offers IoT service providers and the wider IoT ecosystem practical advice on tackling common cyber security threats, as well as data privacy issues associated with IoT services. The GSMA's IoT Security Guidelines have been designed for all players in the IoT ecosystem including IoT service providers, IoT device manufacturers and developers. They will help service providers build

secure services by outlining technologies and methods to address potential threats, as well as how to implement them. They also establish the need for risk assessment of all components of an IoT service to ensure they are designed to securely collect, store and exchange data and successfully mitigate cyber security attacks.

2.52 On 1st October, 2015, Body of European Regulators for Electronic Communications (BEREC) released a draft report on "Enabling the Internet of Things"[15]. According to it, Article 13a of the Framework Directive has already imposed certain security and integrity obligations on providers of publicly available networks and services. These are:

- Networks and service providers must take appropriate measures to appropriately manage the risks posed to security of networks and services, in particular these measures shall ensure a level of security appropriate to the risk presented and to prevent and minimize the impact of security incidents on users and interconnected networks.

- Network providers must take all appropriate steps to guarantee the integrity of their networks and thus ensure continuity of supply of services provided over those networks.

- Networks and service providers must notify the competent NRA of a breach of security or loss of integrity which have a significant impact on the operation of networks or services.

Q12. Will the existing measures taken for security of networks and data be adequate for security in M2M context too? Please suggest additional measures, if any, for security of networks and data for M2M communication.

[15] http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5430-draft-berec-report-on-enabling%20the%20inter%20_0.pdf.

2.53 According to this BEREC report, the general rules of the Privacy Directive are not sector-specific and apply in general; the rules of the ePrivacy Directive apply to the processing of data from both individuals and legal persons in connection with the provision of publicly available electronic communication services in public communication networks in the Community. Overall, the following rules contained in the two Directives are of particular interest in the IoT context:

- Purpose limitation;
- Information about data processing;
- Consent to data processing;
- Security measures;
- Notification obligation of the competent national authority in case of a personal data breach;
- Storing of information in terminal equipment;
- Processing of traffic and location data.

However, there are no specific rules in these two directives with regard to M2M services as such. Until now, BEREC has not identified a need to deviate from the basic principles of data protection law in the M2M context, i.e. no need for a special treatment of M2M services has yet been considered. However, with regard to certain M2M applications it might be worthwhile to consider rules which are more suitable to the M2M environment. For example the methods for giving information, offering a right to refuse or requesting consent could be evaluated in order to make them as user-friendly as possible.

2.54 In Indian context, currently data services are governed by Information Technology (IT) Act, 2000[16] and IT (Amendment) Act, 2008[17]. In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000),

[16] http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

[17] http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

the Central Government made Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[18]. Service provision through M2M communications involving big data may warrant modification of some provisions of these rules. Some of these provisions are deliberated below.

2.55 Currently the Rules apply to Body Corporate and digital data. As per the IT Act, Body Corporate is defined as "*Any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.*" The Rules would not apply to government bodies or individuals collecting and using Big Data alongwith M2M communications. With the coming up of a number of Smart Cities across India – a range of government, public, and private organizations and actors could have access to Big Data.

2.56 Rule 2(i) defines personal information as "information that relates to a natural person which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Rule 3 defines sensitive personal information as that relating to:

- Password,
- Financial information such as Bank account or credit card or debit card or other payment instrument details,
- Physical, physiological and mental health condition,
- Sexual orientation,
- Medical records and history,
- Biometric information

The present definition of personal information encompasses the data that is capable of identifying a person. Yet this definition does not include the information that is associated to an already identified individual - such

[18] http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

as habits, location, or activity. Also, the definitions of sensitive personal information or personal information do not address how personal or sensitive personal information - when anonymized or aggregated – should be treated.

2.57 Rule 5(1) requires that Body Corporate must, prior to collection, obtain consent in writing through letter or fax or email from the provider of sensitive personal data regarding the use of that data. In a context where services are delivered with little or no human interaction, data is collected through sensors, on a real time and regular basis, and is used and re-used for multiple and differing purposes - it is not practical, and often not possible, for consent to be obtained through writing, letter, fax, or email for each instance of data collection and for each use.

2.58 Besides these, various other rules related to the purpose limitation, security, data breach, opt in and out and ability to withdraw consent, disclosure of information, privacy policy etc. may need to be deliberated upon in the context of Big Data.

2.59 On 16th October, 2012, a "Report of the Group of Experts on Privacy"[19] constituted by the (then) Planning Commission was released. This report covered international privacy principles, national privacy principles, rationale and emerging issues along with an analysis of relevant legislations/Bills from a privacy perspective. On the basis of deliberations and in depth analysis, the group had identified a set of recommendations to be considered by the government while formulating the proposed framework for a Privacy Act. This report mainly recommends the establishment of the office of the Privacy Commissioner, both at the central and regional levels. The Privacy Commissioners shall be the primary authority for enforcement of the provisions of the Act. However, rather than prescribing a pure top-down approach to enforcement, this report recommends a system of co-regulation, with

[19] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

equal emphasis on Self-Regulating Organisations (SROs) being vested with the responsibility of autonomously ensuring compliance with the Act, subject to regular oversight by the Privacy Commissioners. The SROs, apart from possessing industry-specific knowledge, will also be better placed to create awareness about the right to privacy and explaining the sensitivities of privacy protection both within industry as well as to the public in respective sectors.

2.60 To promote investment and innovation concurrently in the emerging sector of M2M communications, India needs to have in place balanced and clear rules for data security and privacy. Globally, it is being acknowledged that secure and reliable communication among connected M2M devices is an important issue for deliberation. The perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, leading to less widespread adoption and hence hamper the growth of M2M communications in our country.

2.61 In view of the forgoing, the following issues are raised for consultation of the stakeholders.

Q13. (a) How should the M2M Service providers ensure protection of consumer interest and data privacy of the consumer? Can the issue be dealt in the framework of existing laws?

(b) If not, what changes are proposed in Information Technology Act. 2000 and relevant license conditions to protect the security and privacy of an individual?

Please comment with justification.

E. QoS Issues

2.62 From the foregoing discussion it is clear that in M2M systems different communication networks converged into one large heterogeneous network that is used to establish end-to-end communication. Different

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

2.63 In future, in order to provide end-to-end QoS support for application services over the converged networks in 5G, a common QoS framework will be required to be adopted. In hyper-connected 5G network, M2M scenario would be a major challenge for the 5G wireless cellular systems. Hence, in addition to increased bit rate, 5G will be required to provide minimal latency to seamless integration of Internet of Things (IoT) nodes, and to support energy efficiency of the terminals and of the whole system.

2.64 Quality-of-Service can be looked at from two major perspectives: network perspective and application/user perspective. From the network perspective, QoS refers to the service quality that networks offer to applications or users. Network QoS parameters are latency or delay of packets, reliability of packet transmission etc. From user perspective, QoS parameters can be subjective e.g. presentation, quality of the video, sound quality of streaming audio, etc.

2.65 QoS parameters differ from application to application. For instance, in multimedia applications, bandwidth and delay are most common parameters. In military services, these parameters rely mostly on security and reliability aspects. In routing protocols, besides delay and packet delivery ratio, the routing overhead is also taken into account (i.e., the number of routing packets transmitted per data packet). However, the

common metric includes only parameters like delay, delay variance (jitter), packet loss ratio, and data rate.

2.66 In M2M systems since there are a large number of M2M services, like mobile streaming, smart metering, emergency alerting, or mobile payment etc, one possible mechanism is to describe services according to the high or low need for a real-time transmission, accuracy, and priority. For instance service that includes emergency alerting has a high delay variety and high real-time requirements, while a regular metering service does not have such strict requirements. QoS parameters can also be defined separately for different technologies e.g. ITU-T defines various standards for IP Networks and Services. Similarly manufacturers and TSPs also define their own QoS specifications for routers, servers, etc.

2.67 Based on the forgoing discussion some common QoS parameters can be defined for M2M communication based on the bandwidth of the applications. Different kinds of M2M services have varying network requirements broadly categorized as under:

a. Very low Bandwidth <1Kbps (Monthly usage 10KB to 1MB) e.g. remote sensors etc
b. Low Bandwidth, 1kbps to 50 kbps (Monthly usage 1 MB to 10 MB) e.g. utility, health, security monitoring etc
c. Medium Bandwidth, 50kbps to few MB, (Monthly usage 10MB to 300MB) e.g. retail, ticketing, inventory control, gaming, digital picture frames etc
d. High Bandwidth, in Mbps (Monthly usage >300MB to 90GB) e.g. Digital signage, Video surveillance etc

2.68 For each of the above category delays, latency, jitter, can be considered as QoS parameter. Achieving high QoS has trade-offs associated with it. E.g. latency is often caused by network congestion, and over-sizing the network can improve QoS, but at a cost. Secondly, short delay times typically limit the ability of devices to move into idle mode, thus resulting in much shorter battery life. Another QoS parameter is the allocation and

retention priority (ARP). The ARP determines the priority that a device gets to maintain connectivity in the case of congestion in the network. Contrary to the different traffic classes, the ARP works on the connection instead of on individual IP packets. Many M2M applications can deal with a lower ARP than e.g. standard Internet connectivity. These M2M applications are not time-critical and can delay their data transfer until the congestion is over.

2.69 For mission-critical applications, support of QoS is mandatory. Following service parameters which are relevant in a resource-constrained network, is a non-exhaustive list of:

- Data bandwidth - the bandwidth might be allocated permanently or for a period of time to a specific flow. Some flows may also share bandwidth in a best effort fashion.

- Latency - the time taken for the data to transit the network from the source to the destination. This may be expressed in terms of a deadline for delivery.

- Transmission phase - process applications can be synchronized through coordinated transmissions.

- Precedence and revocation priority - Networks may have limited resources that can vary with time. This means the system can become fully subscribed or even over subscribed. System policies determine how resources are allocated when resources are over subscribed. The choices are blocking and graceful degradation.

- Transmission priority - the means by which limited resources within objects are allocated across multiple services. For transmissions, an object has to select which packet in its queue will be sent at the next transmission opportunity. Packet priority is used as one criterion for selecting the next packet. For reception, an object has to decide how to store a received packet. The objects are

usually memory constrained and receive buffers may become full. Packet priority is used to select which packets are stored or discarded.

- Reliability - Data provided for further processing should be transported reliably because if one part of the whole data set is lost, the entire sampled data may be useless.

- Path capabilities - The path recovery scheme might be different depending on the role of the failed path.

2.70 It is sometimes claimed that only networks using licensed spectrum can reliably provide high QoS. This is on the assumption that in unlicensed spectrum interference cannot be controlled and without full control of all relevant factors the operator cannot provide the guarantees needed. Clearly having more control over all key factors makes it easier to meet requirements, but it is not necessary. Interference will tend to build slowly over time and be predicable and increasingly "mapped", thus leading to high QoS gradually. Solutions such as frequency hopping can mitigate the worse effects and in the longer term interfering users could opt to coordinate between themselves or additional frequency bands could be added to the solution.

2.71 The best approach can be a flexible system that can deliver different QoS outcomes according to need, prioritising the high QoS traffic over the low. One of the options is to have Service Level Agreements (SLAs) based on types of networks and requirement of speed/bandwidth. For this purpose certain parameters like delay, latency, jitter etc need to be defined.

2.72 In an M2M environment, concurrent and massive access of devices may cause performance degradation, such as intolerable delay, packet loss, and unfairness due to possible congestion and interference. To fulfil the requirements of IoT, the main design challenge for M2M communications is to effectively manage the massive access of energy constrained devices

while satisfying different Quality of Service (QoS) requirements. To resolve this issue one option could be to have duty cycle control to improve the end-to-end network performance by optimisation of energy efficiency, delay and reliability. In M2M ecosystem, due to the coexistence of cellular and capillary networks, it is crucial to optimise the overall network performance by simultaneous optimisation of access control and duty cycle control.

2.73 In view of the forgoing the issues for consultation are:

Q14. Is there a need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets)? What parameters must be considered for defining such SLAs? Please give your comments with justifications.

Q15. What should be the distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network?

2.74 The concept and technology of M2M communication is still at its nascent stage. The standards and policies for M2M communication are being deliberated at international forums and by regulators across the world. Since this concept touches multiple verticals and will impact the lives of the citizens, detailed deliberations are required before finalizing the policy and regulatory framework for M2M communication. Inputs from the stakeholders are vital to prepare comprehensive recommendations on the issue.

Q16. Please give your comments on any related matter not covered in this consultation paper.

CHAPTER – III: INTERNATIONAL PRACTICES

EUROPE

3.1 On 1st October, 2015, Body of European Regulators for Electronic Communications (BEREC) released a draft report on "Enabling the Internet of Things". It is aimed at presenting the most common M2M characteristics and assessing whether M2M services might require special treatment with regard to current and potential future regulatory issues. Some excerpts from the report are as follows:

i) NRAs should monitor market developments and spectrum use. Based on the harmonized European Standards and frequencies, National Regulatory Authorities (NRAs) are invited, where appropriate, to make spectrum available to support these applications.

ii) The identifiers used for M2M applications in public networks are: E.164 (e.g. MSISDN) and E.212 (IMSI) numbers as well as IPv4 and IPv6 addresses. In the short and medium term – and perhaps even in the long term – classical telecommunications numbers (E.164 and E.212) will continue to be one solution to identify M2M entities. In the longer term, the use of IPv6 addresses might become the preferred solution.

iii) Under the present regulatory framework, the connectivity service provider who provides connectivity over a public network for remuneration is generally the provider of an ECS in the M2M value chain. In contrast, the M2M user (e.g. car manufacturer, provider of energy including smart meter) typically does not seem to provide an ECS. According to such an approach, M2M users would not be subject to the rules of the EU regulatory framework. However, there would be a finding of an ECS if the M2M user wholly or mainly resells connectivity to the end-user. Overall, since there are so many different types of packages including connectivity and since business models are just beginning to evolve, it has to be carefully assessed by NRAs in which situations an

M2M user may – or may not be – be qualified as a provider of an ECS.

iv) Many M2M services are nowadays based on connectivity which makes use of permanent roaming, the Roaming III Regulation is unclear regarding (i) the admissibility of permanent roaming as such (ii) its applicability of the Roaming III Regulation to these situations. The Roaming III Regulation does not explicitly prohibit permanent roaming, nor explicitly permit it. A case-by-case evaluation should be envisaged taking into consideration the specific (technical) details and parameters of the respective M2M service in light of the purpose of the Roaming III Regulation. Further clarification in the Roaming Regulation and/or in a Commission Communication as to (i) the admissibility of permanent roaming in the M2M context and (ii) the application of the Roaming Regulation to permanent roaming in the M2M context might be helpful.

v) With regard to M2M roaming agreements, BEREC notes that, on the basis, of the available data, there are no issues such as refusal to conclude roaming agreements or tariffs exceeding the price caps under current regulation conditions. However, debates concerning obligation to grant or a right to refuse access might occur in the future if "Roam like at home" (RLAH) applies. The use of permanent roaming might in some instances reflect the absence of national roaming.

vi) Remote re-programming of SIM over the air (i.e. OTA provisioning) in order to switch connectivity service provider remotely is likely the key to mitigate the lock-in issue.

vii) National legislation of a Member State concerning network security does not specifically address M2M services. All obligations apply also to M2M services provided that they are considered ECS or to the ECS which is underlying any M2M service.

viii) The respect and protection of end-users' privacy is a critical success factor for the realisation of the prospects and growth of M2M services. If users do not trust that their data is being handled appropriately there is

a risk that they might restrict or completely opt out of its use and sharing, which could impede the successful development of M2M. While the general rules of Privacy Directive are not sector-specific and apply in general, the rules of ePrivacy Directive apply to the processing of data from both individuals and legal persons in connection with the provision of publicly available electronic communication services in public communication networks in the Community. There are no specific rules in these two directives with regard to M2M services. BEREC has not identified a need to deviate from the basic principles of data protection law in the M2M context. However, with regard to certain M2M services it might be worthwhile to consider rules which are adapted to the M2M environment.

UNITED KINGDOM

3.2 There are currently in excess of 40 million devices in the IoT within the UK. A study recently commissioned by Ofcom predicted that this figure will grow more than eightfold by 2022, when the IoT will consist of 360 million devices and more than a billion daily data transactions. Therefore, Ofcom had published a call for input in July 2014 which aimed to identify potential barriers to investment and innovation in the IoT sector. Thereafter, Ofcom has set out its conclusions and proposed next steps[20], grouped into following four key themes, based on responses and its own analysis.

i) **Data privacy and consumer literacy**

Competition and Markets Authority (CMA) has initiated a call for information on the commercial use of data, aspects of which have relevance to data privacy within the IoT. Ofcom notes that in the UK the Information Commissioner's Office (ICO) has the primary role.

[20] http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf

ii) **Network security and resilience**

The Communications Act 2003 (the "Act") places certain security and resilience obligations[21] on providers of publicly available[22] networks and services.

iii) **Availability of spectrum for IoT services**

Ofcom concludes that the availability of spectrum will not pose a barrier to the development of the IoT in the short to medium term.

List of possible bands for IoT applications:

There are already a number of spectrum bands in UK which are suitable for deployment of IoT applications. These include:

- Spectrum recently made available by Ofcom in the bands 870 – 876 MHz and 915 – 921 MHz[23];
- A subset of licence exempt bands that are potentially relevant for IoT use like Short Range Indoor Data Links, Railway Applications, Road Transport and Traffic Telematics and Intelligent transport Systems etc. ;
- A subset of bands currently used for Business Radio and Fixed Links. The bands that may be used can be found by searching the UK Plan for Frequency Authorisation (UKPFA)[24] for licences for Business Radio (technically assigned) and Fixed Links (scanning telemetry); and
- Unused spectrum between 55 and 68 MHz. Ofcom will consider requests for use of this spectrum on a case-by-case basis.[25]

In the future, IoT applications could also be deployed in white spaces. In

[21] Sections 105A to D of the Act

[22] As set out in section 151 of the Act, a public communications service is one that is provided so as to be available for use by members of the public. A public communications network is one that is provided wholly or mainly for the purpose of making electronic communications services available to members of the public.

[23] http://stakeholders.Ofcom.org.uk/binaries/consultations/short-range-devices/statement/statement.pdf and http://stakeholders.Ofcom.org.uk/binaries/consultations/network-relay-points/statement/NRP_statement.pdf

[24] http://spectruminfo.Ofcom.org.uk/spectrumInfo/ukpfa

[25] http://stakeholders.Ofcom.org.uk/spectrum/spectrum-awards/prospective-awards/award_55/

addition, it is exploring options for liberalising licence conditions on mobile spectrum use to support the IoT.

iv) **Telephone number and address management**

Ofcom believes that 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 Internal 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.

3.3 On 10th September, 2015, Ofcom issued a consultation paper on "More Radio Spectrum for the Internet of Things"[26] to encourage investment and innovation in the Internet of Things (IoT) using 10.1 MHz of spectrum within the 55-68 MHz, 70.5-71.5 MHz and 80.0-81.5 MHz bands by using their existing license products. At the same time, they sought views on whether any changes to the existing license products are necessary to promote innovative uses in these bands, especially for serving rural and remote locations. In this consultation paper, Ofcom has set out the consideration of the licensing regime for IoT services in the VHF bands. They have asked whether the existing BR licence[27] regime is the most appropriate for IoT providers or whether they should introduce changes.

3.4 Figure 3.1 replicates Ofcom's illustration of two broad approaches that might be used to meet the future needs of IoT services.

[26] http://stakeholders.ofcom.org.uk/binaries/consultations/radio-spectrum-internet-of-things/summary/more_radio_spectrum_internet_of_things.pdf

[27] If a radio system is used for the business, then a BR (Business Radio) licence is needed from Ofcom. Business radio users range from taxi companies and factories, to hospitals, care homes, industrial sites and transport operators.

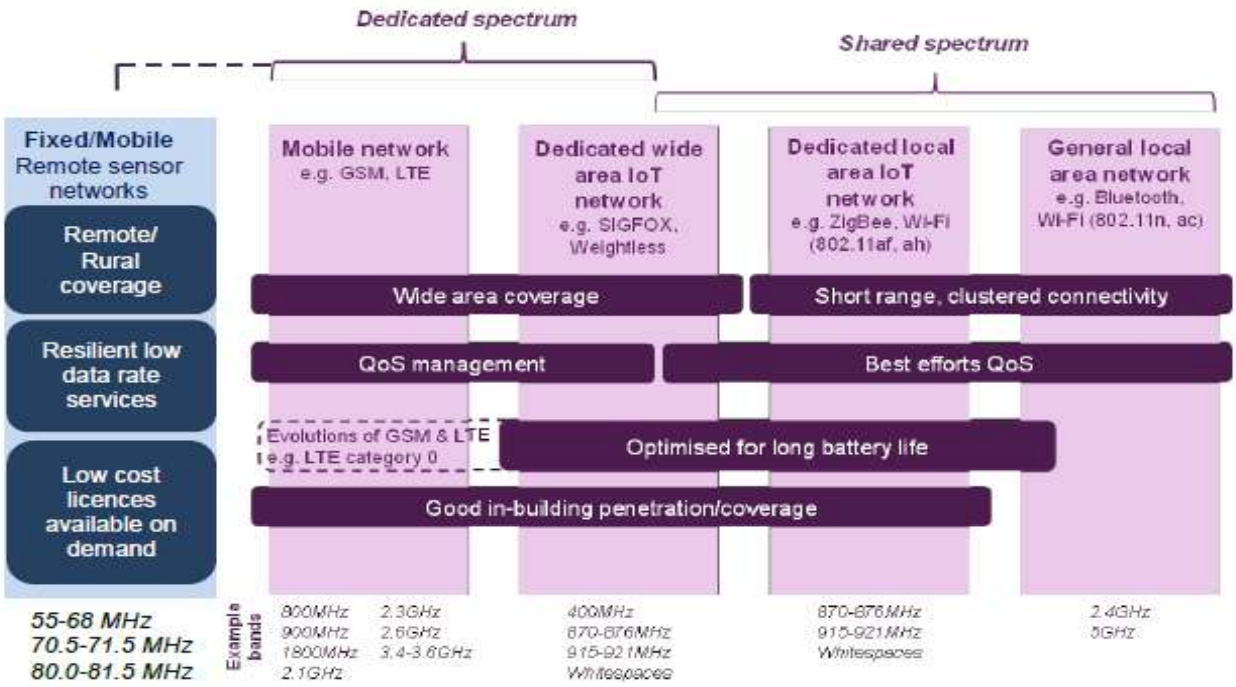


Figure 3.1: OFCOM's framework for considering IoT spectrum requirements

SINGAPORE

3.5 Licensing in Singapore is categorized into two segments:

- **Facility Based Operators (FBOs)** refers to the deployment and/or operation of any form of telecommunication network, systems and/or facilities by any person for the purpose of providing telecommunication and/or broadcasting services outside of his own property boundaries to third parties, who may include other licensed telecommunication operators, business customers or the general public. Licensees who are licensed as FBO will be able to offer the services that Services-Based Operators (SBO) can offer, but not vice versa.
- **Service Based Operators (SBOs)**[28] are operators intending to lease telecommunications network elements such as transmission capacity, switching services, ducts and fiber from any FBO licensed by IDA to provide telecommunications services to third parties or resell the telecommunications services of FBO.

[28] http://www.ida.gov.sg/~/media/Files/PCDG/Licensees/Licensing/SBOLicence/SBOGuide.pdf

3.6 M2M services can be provided by both groups of Licensees (SBO (individual) & FBO) depending on the business proposition and models of Licensees.[29]

3.7 **Terms & conditions for M2M Services under SBO(Individual) Licence**

- Machine-to-Machine ("M2M") Services are defined as the services that are provided to enable the automated communication between machines and devices using equipment with embedded SIM card(s) ("M2M Equipment").
- All SIM cards which are used in the provision of M2M Services by the Licensee are configured to be used only for the automated communication between machines and devices and not for other purposes unless the prior written approval of IDA has been obtained.
- The Licensee shall maintain a register containing full and accurate records of all SIM cards which are used in connection with the provision of M2M Services by the Licensee.
- The Licensee shall work and cooperate fully with the authorised Singapore government agencies to render assistance in any investigation in connection with the provision of M2M Services by the Licensee.

National Numbering Plan ("NNP")[30]

3.8 M2M access code allocated may be used with international connectivity and international roaming services[31]. 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.

---

29 https://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20130131_M2MFramework/Decision%20paper%20for%20M2M%20AC%20framework.pdf

30 Revised NNP can be accessed at the link: http://www.ida.gov.sg/Policies-and-Regulations/Industry-and Licensees/Numbering/National-Numbering-Plan-and-Allocation-Process.

31 M2M international interconnectivity refers to a M2M device in Singapore using a Singapore M2M number to communicate with a device or service outside Singapore, while international roaming refers to an M2M device with a Singapore M2M number that can continue to be used overseas outside of the Singapore networks.

ITALY

3.9 The Italian Communications Authority launched a fact-finding survey[32] on Machine to Machine (M2M) communication services to identify any regulatory barriers to the development of M2M services. The analysis revealed that at the beginning of 2014 there were an estimated 225 million SIM based M2M connections in the world. Of these, 27% (61 million connections) was in Europe, showing a growth trend of over 20% a year.

3.10 The fact-finding survey identified the following main spheres of possible regulatory intervention:

- investment in the infrastructures and in the development of the services;
- regulation of connectivity;
- the final service;
- the vertical M2M markets.

3.11 One of the most important aspects regards the public network infrastructures available at present, which are partially inadequate for the supply of M2M connectivity, in consideration of the specific technical needs required by the demand and the relatively high costs for the supply of the connection itself[33]. These critical aspects are pushing the M2M service suppliers to create ad hoc networks and architectures, alternative to the public networks, based on closed and non-interoperable proprietary networks, with a consequent risk of market

32 http://www.agcom.it/documents/10179/1667676/Allegato+17-6-2015/271ed933-6af4-4dc2-a0bc-3812e3c1cbe5

33 From a technical viewpoint, the large scale spread of M2M technology on traditional networks could generate congestion of the network because of the maximum signal capacity supported (rather than in terms of maximum traffic limits supported). In the case of SIM based services, for example, the dimensioning of the 2G/3G networks was originally defined to ensure the support of a relatively low number of terminals per resident person. In the case of M2M, each person could have a few dozen units connected. In short, a traditional network (not developed for M2M applications, featuring very low but very widespread traffic volumes) cannot be expected to be adequate to supply connectivity to either today's users or the users of M2M technology services.

concentration and dispersion of resources.

3.12 With regard to international roaming, some uncertainties have emerged relative to the applicability of the EU Roaming Regulation. Various doubts of regulatory nature are raised, such as: which Institution should be given juridical/regulatory competence; the congruity of the regulated prices with the underlying costs. It seems necessary to identify solutions alternative to permanent roaming, which can operate nationally and reduce the incidence of opportunistic behaviour, at the same time creating a level playing field for the operators.

3.13 With reference to spectrum management policies, the following are of great importance:

i) the possibility of use in very particular indoor environments;
ii) the availability of a capillary coverage of the territory;
iii) the transfer speed of the channel from the device to the network *(upload).*

3.14 With reference to security, M2M communications must guarantee a suitable level according to the diverse type of the services to which such communication can be dedicated or the routes that must be protected.

3.15 With reference to the General Authorisation Regime provided by the EU Regulatory framework for electronic communications, the definition for Electronic Communication Services (ECS) is difficult to apply in the M2M sector because of the appearance of new subjects in the value chain. The transnational nature of M2M also stimulates reflection on the institutions which are in force to simplify the administrative procedures linked to the disclosure obligation in all States where the sale of the final service is expected.

BRAZIL

3.16 Brazil is fifth-largest country in the world by population, and has significant demand for M2M. The M2M market in Brazil looks set to enter a high-growth phase as a result of recent regulatory activity. A history of

protectionist telecom policies and social unrest have created uncertainty in the minds of investors and constrained the development of M2M in the country. However, the regulatory activity needed to support M2M market growth appears to be gaining momentum.

3.17 A number of regulatory developments have significantly improved prospects for the M2M market in Brazil.

- The M2M service providers are being registered in MVNO (Mobile Virtual Network Operator) category and brought under regulatory framework.

- Special Tax incentives were also granted to boost services. In September 2013, Minister of Communications announced plans to reduce the tax on M2M communications. It is worth highlighting that the Brazilian Government has significantly reduced SIM card tax on M2M devices by 80% providing a stimulus for operators to develop M2M services.

AUSTRALIA

3.18 In November, 2015, Australian Communications and Media Authority (ACMA) released an occasional paper titled "The Internet of Things and the ACMA's area of focus"[34]. According to this paper, "Internet of Things (IoT)" refers to the inter-connection of many devices and objects utilising internet protocols that can occur with or without the active involvement of individuals using the devices. The IoT is the aggregation of many machine-to-machine (M2M) connections.

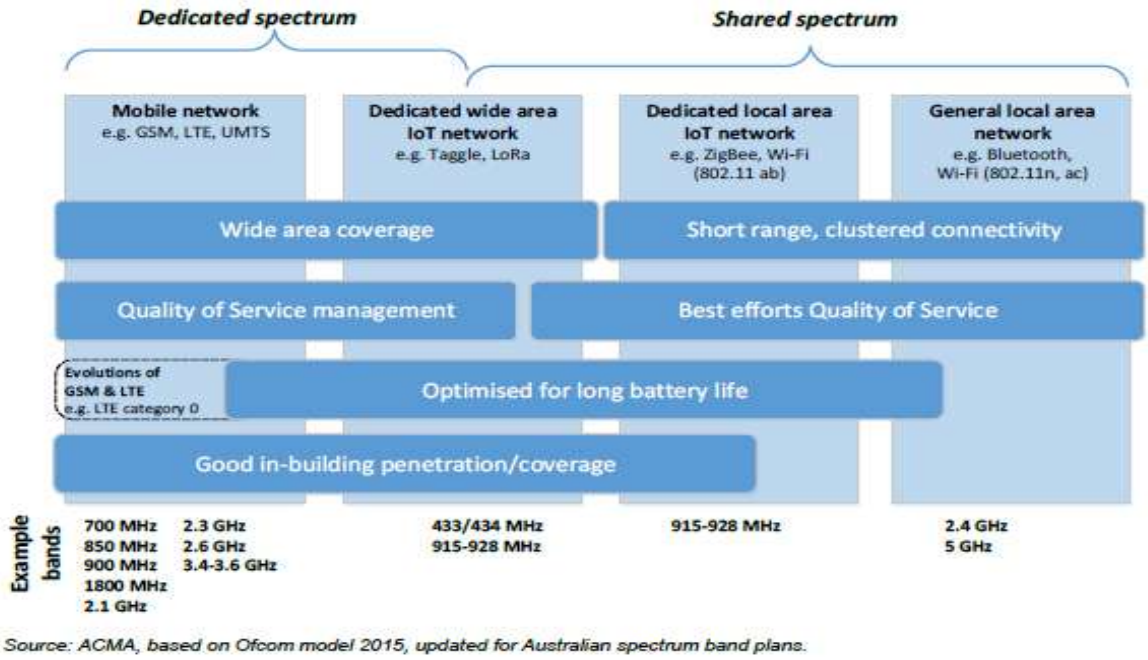
3.19 ACMA considered the effect of M2M on the demand for mobile numbers. At the time (2011), the early estimates suggested a requirement for numbers for M2M communications of between 5.8 and 61.9 million by 2020. In responding to this expected demand for new mobile numbers,

[34] http://www.acma.gov.au/theACMA/~/media/18E314A0C00A41F9B4D629DAB9397436.ashx

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.

3.20 To some extent, M2M and IoT applications may utilise existing class licensed spectrum (that is, spectrum 'commons). Class licences authorise users of designated segments of spectrum to operate on a shared basis. A class licence is not issued to an individual user and does not incur licence fees.

3.21 Spectrum bands identified for IoT are shown in figure below:



Source: ACMA, based on Ofcom model 2015, updated for Australian spectrum band plans.

Figure 3.2: ACMA's framework for considering IoT spectrum requirements

3.22 Other specific spectrum bands under review during 2015–16:

- the scheduled review of the 803–960 MHz band will explore future opportunities as a candidate band for mobile broadband and M2M
- the review of the 5.9 GHz band for intelligent transport systems applications is also relevant as intelligent transport systems represent one of many IoT applications.

3.23 Currently, some internet security risk concerns are addressed via the Australian Internet Security Initiative (AISI), which is a co-operative program between the ACMA, internet service providers and citizens. The AISI was developed with the objective of protecting Australian internet users from malware (malicious software) and cyber security threats on the internet.

3.24 ACMA's medium-term focus—the next two to five years:

- It is likely that M2M communications will broaden from current technologies reliant on mobile numbers, to be supplemented by IP-based communications using IP addresses (IPv6).
- Continue to review bands that will support M2M and IoT applications.
- Work in international forums will be important in considering future spectrum needs for a broad range of services.
- Planning processes for the international standardisation of 5G technologies that will support the 'anytime, anywhere, anyone and anything' capability needed for the IoT will continue through this period.

CHAPTER – IV: ISSUES FOR CONSULTATION

Q1. What should be the framework for introduction of M2M Service providers in the sector? Should it be through amendment in the existing licenses of access service/ISP license and/or licensing authorization in the existing Unified License and UL (VNO) license or it should be kept under OSP Category registration? Please provide rationale to your response.

Q2. In case a licensing framework for MSP is proposed, what should be the Entry Fee, Performance Bank Guarantee (if any) or Financial Bank Guarantee etc? Please provide detailed justification.

Q3. Do you propose any other regulatory framework for M2M other than the options mentioned above? If yes, provide detailed input on your proposal.

Q4. In your opinion what should be the quantum of spectrum required to meet the M2M communications requirement, keeping a horizon of 10-15 years? Please justify your answer.

Q5. Which spectrum bands are more suitable for M2M communication in India including those from the table 2.3 above? Which of these bands can be made delicensed?

Q6. Can a portion of 10 MHz centre gap between uplink and down link of the 700 MHz band (FDD) be used for M2M communications as delicensed band for short range applications with some defined parameters? If so, what quantum? Justify your answer with technical feasibility, keeping in mind the interference issues.

Q7. In your opinion should national roaming for M2M/IoT devices be free?

(a) If yes, what could be its possible implications?

(b) If no, what should be the ceiling tariffs for national roaming for M2M communication?

Q8. In case of M2M devices, should;

(a) roaming on permanent basis be allowed for foreign SIM/eUICC; or

(b) Only domestic manufactured SIM/eUICC be allowed? and/or

(c) there be a timeline/lifecycle of foreign SIMs to be converted into Indian SIMs/eUICC?

(d) any other option is available?

Please explain implications and issues involved in all the above scenarios.

Q9. In case permanent roaming of M2M devices having inbuilt foreign SIM is allowed, should the international roaming charges be defined by the Regulator or it should be left to the mutual agreement between the roaming partners?

Q10. What should be the International roaming policy for machines which can communicate in the M2M ecosystem? Provide detailed answer giving justifications.

Q11. In order to provide operational and roaming flexibility to MSPs, would it be feasible to allocate separate MNCs to MSPs? What could be the pros and cons of such arrangement?

Q12. Will the existing measures taken for security of networks and data be adequate for security in M2M context too? Please suggest additional measures, if any, for security of networks and data for M2M communication.

Q13. (a) How should the M2M Service providers ensure protection of consumer interest and data privacy of the consumer? Can the issue be dealt in the framework of existing laws?

(b) If not, what changes are proposed in Information Technology Act. 2000 and relevant license conditions to protect the security and privacy of an individual?

Please comment with justification.

Q14. Is there a need to define different types of SLAs at point of interconnects at various layers of Heterogeneous Networks (HetNets)? What parameters must be considered for defining such SLAs? Please give your comments with justifications.

Q15. What should be the distributed optimal duty cycle to optimise the energy efficiency, end-to-end delay and transmission reliability in a M2M network?

Q16. Please give your comments on any related matter not covered in this consultation paper.

LIST OF ACRONYMS

Acronyms	***Description***
3GPP	3RD GENERATION PARTNERSHIP PROJECT
ACMA	AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY
AISI	AUSTRALIAN INTERNET SECURITY INITIATIVE
AM	AMPLITUDE MODULATION
APT	ASIA-PACIFIC TELECOMMUNITY
ARIB	ASSOCIATION OF RADIO INDUSTRIES AND BUSINESSES
ARP	ALLOCATION AND RETENTION PRIORITY
ATIS	ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS
B2B	BUSINESS TO BUSINESS
B2B2C	BUSINESS TO BUSINESS TO CONSUMER
B2C	BUSINESS TO CONSUMER
BEREC	BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS
BLE	BLUETOOTH LOW ENERGY
CAGR	COMPOUND ANNUAL GROWTH RATE
CCSA	CHINA COMMUNICATIONS STANDARDS ASSOCIATION
CDMA	CODE DIVISION MULTIPLE ACCESS
CEPT	CONFERENCE OF EUROPEAN POSTAL AND TELECOMMUNICATIONS
CMA	COMPETITION AND MARKETS AUTHORITY
CMRTS	CAPTIVE MOBILE RADIO TRUNKED SYSTEMS
CP	CONSULTATION PAPER
DeitY	DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY
DoT	DEPARTMENT OF TELECOM
DSL	DIGITAL SUBSCRIBER LINE
ECC	ELECTRONIC COMMUNICATION COMMITTEE

ECS	ELECTRONIC COMMUNICATION SERVICES
EPOS	ELECTRONIC POINT OF SALE
ESN	ELECTRONIC SERIAL NUMBER
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
EU	EUROPEAN UNION
eUICC	EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD (EMBEDDED SIMS)
FBO	FACILITY BASED OPERATORS
FDD	FREQUENCY-DIVISION DUPLEXING
FG CarCom	FOCUS GROUP FROM/IN/TO CARS COMMUNICATION
FG Cloud	FOCUS GROUP ON CLOUD COMPUTING
FG DR & NRR	FOCUS GROUP ON DISASTER RELIEF SYSTEMS, NETWORK RESILIENCE AND RECOVERY
FG M2M	FOCUS GROUP ON M2M SERVICE LAYER
FG Smart	FOCUS GROUP ON SMART GRID
FG SSC	FOCUS GROUP ON SMART SUSTAINABLE CITIES
FG SWM	FOCUS GROUP ON SMART WATER MANAGEMENT
FM	FREQUENCY MODULATION
GSM	GLOBAL SYSTEM FOR MOBILE
GSMA	GROUPE SPECIALE MOBILE ASSOCIATION
HAN	HOME AREA NETWORK
HetNets	HETEROGENEOUS NETWORKS
ICO	INFORMATION COMMISSIONER'S OFFICE
ICT	INFORMATION AND COMMUNICATION TECHNOLOGIES
IDA	INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE
IETF	INTERNET ENGINEERING TASK FORCE
IMEI	INTERNATIONAL MOBILE EQUIPMENT IDENTITY
IMSI	INTERNATIONAL MOBILE SUBSCRIBER IDENTITY

IMT	INTERNATIONAL MOBILE TELECOMMUNICATIONS
IoE	INTERNET OF EVERYTHING
IoT	INTERNET OF THINGS
IP	INTERNET PROTOCOL
IPR	INTELLECTUAL PROPERTY RIGHTS
IPv4	INTERNET PROTOCOL VERSION 4
IPv6	INTERNET PROTOCOL VERSION 6
IrDA	INFRARED DATA ASSOCIATION
ISP	INTERNET SERVICE PROVIDER
IT	INFORMATION TECHNOLOGY
ITU	INTERNATIONAL TELECOMMUNICATION UNION
KYC	KNOW YOUR CUSTOMER
LAN	LOCAL AREA NETWORK
LEA	LAW ENFORCEMENT AGENCIES
LI	LAWFUL INTERCEPT
LPWAN	LOW POWER WIDE AREA NETWORK
LRWPAN	LOW RATE WPAN
LSA	LICENSED SERVICE AREA
LTE	LONG-TERM EVOLUTION
M2M	MACHINE TO MACHINE
MFCN	MOBILE/FIXED COMMUNICATION NETWORKS
MNC	MOBILE NETWORK CODES
MNOs	MOBILE NETWORK OPERATORS
MNP	MOBILE NUMBER PORTABILITY
MSISDN	MOBILE STATION INTERNATIONAL SUBSCRIBER DIRECTORY NUMBER
MSP	M2M SERVICE PROVIDERS

MVNOs	MOBILE VIRTUAL NETWORK OPERATORS
NFAP	NATIONAL FREQUENCY ALLOCATION PLAN
NNP	NATIONAL NUMBERING PLAN
NRA	NATIONAL REGULATORY AUTHORITIES
NTP	NATIONAL TELECOM POLICY
OECD	ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
OSP	OTHER SERVICE PROVIDERS
OTA	OVER THE AIR
PAN	PERSONAL AREA NETWORK
PMR	PRIVATE MOBILE RADIO
PMRTS	PUBLIC MOBILE RADIO TRUNKED SYSTEMS
POS	POINT OF SALE
PSTN	PUBLIC SWITCHED TELEPHONE NETWORK
QoS	QUALITY OF SERVICE
RLAH	ROAM LIKE AT HOME
RLAN	RADIO LAN
ROLL	ROUTING OVER LOW POWER AND LOSSY NETWORKS
SBO	SERVICE BASED OPERATORS
SC & C	SMART CITIES AND COMMUNITIES
SDO	STANDARDS DEVELOPMENT ORGANIZATIONS
SIM	SUBSCRIBER IDENTITY MODULE.
SLA	SERVICE LEVEL AGREEMENTS
SMS	SHORT MESSAGE SERVICE
SRD	SHORT RANGE DEVICES
SRO	SELF-REGULATING ORGANISATIONS
SRTP	SPECIAL ROAMING TARIFF PLAN

TEC	TELECOMMUNICATION ENGINEERING CENTER
TIA	TELECOMMUNICATIONS INDUSTRY ASSOCIATION
TOC	TOTAL COST OF OWNERSHIP
TRAI	TELECOM REGULATORY AUTHORITY OF INDIA
TSAG	TELECOMMUNICATION STANDARDIZATION ADVISORY GROUP
TSDSI	TELECOMMUNICATIONS STANDARDS DEVELOPMENT SOCIETY OF INDIA
TSPs	TELECOM SERVICE PROVIDERS
TTA	TELECOMMUNICATIONS TECHNOLOGY ASSOCIATION
TTC	TELECOMMUNICATION TECHNOLOGY COMMITTEE
UKPFA	UK PLAN FOR FREQUENCY AUTHORISATION
UL(VNO)	UNIFIED LICENSE (VIRTUAL NETWORK OPERATORS)
UMTS	UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM
UNB	ULTRA-NARROW BAND
USB	UNIVERSAL SERIAL BUS
USIM	UMTS SIM
USSD	UNSTRUCTURED SUPPLEMENTARY SERVICE DATA
V2I	VEHICLE TO INFRASTRUCTURE
V2V	VEHICLE TO VEHICLE
VHF	VERY HIGH FREQUENCY
VNOs	VIRTUAL NETWORK OPERATORS
WAN	WIDE AREA NETWORK
WHAN	WIRELESS HOME AREA NETWORK
WLAN	WIRELESS LOCAL AREA NETWORK
WLL	WIRELESS LOCAL LOOP
WPAN	WIRELESS PERSONAL AREA NETWORK

Annexure

F. No. 4-16/ 2015-NT
Government of India
DoT, Networks and Technologies Cell

Dated: 5th Jan, 2016

To,

The Secretary,
Telecom Regulatory Authority of India,
N. Delhi

Sub: - Reference to TRAI seeking recommendation on Quality of Service (QoS), Spectrum and Roaming related requirements in M2M Communications.

'National Telecom M2M Roadmap' has been released by DoT in May 2015 with the objective of proliferating the growth of M2M ecosystem and to bring tangible social and economic benefits to consumers, businesses, citizens and government.

2. Certain actionable points have evolved from the Roadmap document which needs to be taken up to further the M2M ecosystem growth. Addressal of M2M Quality of Service (QoS), Spectrum and Roaming aspects are such actionable points emerged from M2M Roadmap. These items have been deliberated in various sections of the M2M Roadmap. Softcopy of the document is available on the DoT website.

3. TEC has also come up with 9 technical reports on M2M detailing sector specific requirements/ use cases to carry out gap analysis and future action plans with possible models of service delivery. Some of these reports have also touched upon requirements related to Spectrum, Roaming and QoS and are available at website http://www.tec.gov.in/technical-reports/

4. Accordingly TRAI recommendations are sought for following points related to M2M communications:

A. QoS in M2M Services
B. M2M Roaming Requirements
C. M2M Spectrum Requirements

The relevant information on the above points is extracted from the DoT M2M roadmap, compiled for easy reference and is attached as Annexure-I to this letter.

5. Accordingly, TRAI is requested to provide its recommendations under section 11 (1) (a) of TRAI Act, 1997 as amended in TRAI (amendment) Act; 2000, for recommendation on Quality of Service (QoS), Spectrum and Roaming related aspects of M2M communications in a holistic manner.

Encl: Annexure-I

(Rajiv Sinha) 05/01/2016
DDG (NT)
+91 11 23372606
ddgnt-dot@nic.in

Annexure-I

Background Note

(For Seeking TRAI recommendations on QoS, Spectrum and Roaming related aspects of M2M communications)

Quality of Service (QoS):

The notion of QoS has been introduced to capture the qualitatively and/ or quantitatively defined performance contract between user applications and the service provider. 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. Thus in Machine to Machine (M2M) systems, different communication networks converged into one large heterogeneous network thereby making the fulfillment of QoS requirement more complex. 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.

M2M communication show quite different characteristics compared with the traditional Human-to-Human (H2H) communications. QoS categorization of H2H communications is mainly based on delay, because voice is the main service in H2H communication. However, providing M2M data communications to large numbers of M2M devices and providing services to M2M application owners rather than end-users implies a different optimization of the network. Although many M2M applications have no stringent QoS requirements and can deal perfectly well with best-effort QoS, some M2M applications have higher QoS or priority requirements than normal data services. TSP's and ISP's are increasingly providing QoS differentiation in their packet-based networks. This will represent an added value for many M2M applications.

QoS has become a stringent requirement for real time applications and enables more efficient sharing of network resources. It manages time-sensitive multimedia and voice application traffic to ensure it gets a higher priority, since greater delays cause serious deterioration in the provided service. QoS parameters differ from application to application. For instance, in multimedia applications bandwidth and delay are most common parameters. In military services, these parameters rely mostly on security and reliability aspects. In routing protocols, besides delay and packet delivery ratio, the routing overhead is also taken into account (i.e., the number of routing packets transmitted per data packet). However, the common metric includes only following parameters: delay, delay variance (jitter), packet loss ratio, and data rate.

M2M systems have their own QoS requirements. Since there are a large number of M2M services, like mobile streaming, smart metering, regular monitoring, emergency alerting, or mobile payment, it is suggested that these services are described according to the high or low need for a real-time transmission, accuracy, and priority. For instance, service that includes emergency alerting has a high delay variety and high real-time requirements, while a regular metering service does not have such strict requirements.

M2M Roaming Requirements:

In M2M domain, there are scenarios, wherein M2M Service provider or manufacturer may be an entity located in foreign country and it may prefer to fit the foreign telecom service provider's SIM in the machine to be used in India always. Like, a car may be manufactured in a foreign country with a foreign telecom operator's SIM in it. In such cases, SIM shall be always in roaming state outside its home network (permanent roaming).

Present licensing regime allows licensees to enter into roaming agreements with other licensees as per their commercial arrangements for national roaming. For International Roaming, licensees can enter into agreements with foreign telecom Service Providers to provide roaming facility to its subscribers & vice versa. Roaming subscribers can only access services to which they have subscribed in their home networks. The guidelines are applicable to voice as well data services. There are concerns on non-availability of M2M services in North Eastern States and J&K in case of imported devices pre-fitted with foreign SIM cards. This is due to restrictions placed on international SIMs roaming to these areas.

As per stakeholders, in general, quantum of M2M traffic and correspondingly ARPU is very less and therefore it may require separate roaming arrangements/ interconnect charges among TSPs. GSMA has also finalized separate template for roaming of M2M subscribers. In long run, separate identifier like IMSI or MSISDN may be allocated to M2M services, which is different from voice or data SIMs to enforce and regulate M2M specific roaming.

In line with declared policy objective of One Nation - Free Roaming and no roaming charge across the nation in NTP - 12, there should not be any inter-circle roaming charges for M2M services. This may give a boost to M2M services, as machines i.e. automobiles are more often likely to roam in different circles. The volume of data exchanged for mobile machines is small and this provision is not likely to have much revenue impact for operators. TRAI may look into M2M specific roaming charges in case of M2M services for both intra-operator and inter-operator roaming scenarios in view of low data volume, objectives of NTP - 12 and with an aim to providing a boost to M2M services.

M2M Spectrum Requirements:

M2M covers various Industry verticals and use different frequencies for various kinds of service offerings covering short range communication on high frequencies like Bluetooth, ZigBee, and 6LoWPAN to low frequency range for RF mesh etc. in neighborhood network connectivity requirements. Technological developments enabling utilization of White Space in different licensed bands have thrown new possibilities for efficient spectrum utilization benefitting M2M services as well. Globally, the trend is to use telecom network of TSP and/ or free wireless bands for M2M communications. In line with the requirement, there may be a need to fine-tune free spectrum bands. Also detailed planning and guidelines are required for effective and efficient use of white spaces protecting interest of primary spectrum usages. TRAI may take up the M2M Spectrum requirements in totality covering relevant aspects as detailed above.