ERICSSON

Reference: RINAT-16: 0053
Date: 2017-01-03
Attending to this matter: Sreenivasa Reddy

Your Reference: Consultation Paper No. 21/2016
Your Date: 2016-10-18

Shri Sanjeev Banzal,
Advisor (NSL-II),
TRAI, Old Minto Road,
New Delhi-110002

Sub: Ericsson Response to TRAI Consultation Paper on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications"

Dear Sir,

We thank TRAI for initiating the consultation process on "Spectrum, Roaming and QoS related requirements in M2M Communications" inviting response from industry. Ericsson is pleased to respond to this consultation.

Ericsson is the driving force behind the Networked Society – a world leader in communications technology and services. Our long-term relationships with every major telecom operator in the world allow people, business and society to fulfil their potential and create a more sustainable future. Our services, software and infrastructure – especially in mobility, broadband and the cloud – are enabling the telecom industry and other sectors to do better business, increase efficiency, improve the user experience and capture new opportunities.

Developing a digital transformation strategy has become an increasingly important task, as new consumer behaviour demands new digitized offerings. There are several factors driving digital transformation among Citizens, Industries, Government, Regulators and Policy Makers, from identifying new growth opportunities and improving cost efficiency to enhancing consumer/ citizen experience via new digital services eco-system. Digital transformation will allow citizens/ consumers to benefit from these opportunities and – through engaging in new business models and developing the required skills to compete in the market.

IoT can be segmented into critical and massive applications. Critical IoT applications have stringent requirements on availability, delay and reliability; examples include traffic safety, automated vehicles, industrial applications and remote surgery in healthcare. Whereas, Massive IoT, on the other hand, is characterized by a very large number of connections, small data volumes, low-cost devices and stringent requirements on energy consumption; examples include smart buildings, smart metering, transport logistics, fleet management, industrial monitoring and agriculture.

IoT presents new opportunities for mobile operators to leverage their core assets and move up the value chain. Telia and Telenor Connexion are examples of operators that are already adding IoT value beyond connectivity by providing intelligent platforms, facilitating ecosystem collaboration, and even becoming a transformation partner to other industries.

In the past, M2M started as single solution/ application, created for one specific task. However, today it is becoming more common for devices to be connected than not. Hence, we get to the Internet of Things, where we might get a sharing of data across different sectors and between different devices in a way that wasn't envisioned when M2M first came about.

**Ericsson India Pvt. Ltd.**

Ericsson Forum
DLF Cyber Citi, Sector 25-A
Gurgaon 122 002, Haryana,
www.ericsson.co.in/

Tel: +91 124 270 1201
Fax: +91 124 256 5420

Registered Office
4th Floor, Dakha House
VAT: 18/17, W.E.A, Pusa
New Delhi 110 005 INDIA

Service Tax No.:
IV916)ST/GGN-/CE/18/2002
TIN: 06911822715

Both traditional vertical market applications and new cross-sector services are likely to exist, based on a data-rich environment. These will vary immensely between the enterprise, or B2B, and B2B2C worlds. Connected homes and connected cars provide current early examples of the direction this is heading towards.

The Internet of Things is about utilizing data from billions of connected devices – the value is in the data. In order for this to happen, much more is required to get these devices to connect seamlessly. Getting billions of devices connected easily and cost-effectively in a way that allows interoperability is critical and does not yet exist. Evidence of this lack includes the high return rates (up to 90%) for home alarm and control products. M2M horizontal platforms are key to solving this challenge.

M2M communications is different from other mobile network communication (Human to Human communications) services as it involves potentially very large number of communicating devices with, to a large extent, little traffic per device. More and more M2M devices using a connection with a Mobile network operator (MNO), will result in expansion of the M2M traffic share from the total mobile traffic volumes. M2M traffic can in some circumstances put enormous strain on mobile network infrastructure and, in severe cases, can disrupt or diminish the capability and quality of service the MNO can offer to not only M2M devices but also other human end users.

Most M2M applications generate a distinctively different pattern in signalling, circuit or packet switched communication than human mobile communications do. There are three main characteristics of M2M communication:

- High number of simultaneous (data) sessions
- Frequent retry rate in case of unsuccessful connection attempts
- Large number of M2M devices in a relatively small geographic area.

As a consequence, this could result in following network congestion situations:

- **Radio Network Congestion**: Radio network congestion because of mass concurrent data transmission takes place in M2M applications.
- **Core Network Congestion:** When a high number of M2M Devices are sending/receiving data simultaneously, data congestion may occur in the mobile core network or on the link between mobile core network and M2M Server where the data traffic is aggregated.
- **Signalling Network Congestion**: Congestion in the signalling network is caused by a high number of M2M Devices trying almost simultaneously to attach to the network or to activate/modify/deactivate a connection. Also some M2M applications generate recurring data transmissions at precisely synchronous time intervals (e.g. precisely every hour or half hour). Hence, the network should be able to deal with small amount of data when transferring without generating an overhead.

To avoid a large number of active M2M devices disrupting the MNO's capability and quality of service to not only M2M devices but also other end users, a number of guidelines must be formulated for M2M service providers and Home Operators, Serving Operators, M2M device

manufacturers and application developers. The goal of framing any such national guidelines[1] should ensure that all players can perform their functions while avoiding situations that can be harmful to the network, including Visiting Public Mobile Network (VPLMN) and Home Public Mobile Network (HPLMN, DCP), so that VPLMN and HPLMN can always have the features available and keep the quality of service to all its M2M home users, roaming users and end users.

Also, to address the above mentioned challenges, IoT operators need to work closely with roaming operators to shut down or redirect control plane messages for all IoT roaming devices. This impacts all IoT customers, as the whole roaming network range is blocked. Once a network is fully congested, it can take up to two hours to completely re-route roaming IoT devices, and then another two hours for network operations to normalize. For roaming operators, this can negatively affect consumer traffic and customer experience, resulting in negative brand impact.

**Emerging applications**
Data and information generated by both "machines" and "human activities" will be key assets. Open access to data puts new requirements on finding data, accuracy of data including provenance and ownership of data and information. **Data and information brokering is a key capability** taking care of both technical and business integration. Participatory sensing is another possible application area in which large numbers of "independent" devices volunteer to share collected (anonymized) environmental and other information to be used for new applications. A **high degree of cross-industry reuse and knowledge sharing** is necessary to obtain the needed scale and to drive transferable ICT between industries.

**Smart and connected things**
There is a need to make a distinction between smart things and connected things. Connectivity can in itself be the driver. This is typically the case in the consumer electronics domain where usefulness and usability is increased if the gadget is always connected. On the other hand, for smart things, connectivity is just an enabler, even though connectivity itself may have to be "smart" and fit the purpose of the smart application. Smart things are deployed to serve a particular purpose.

The purpose of a smart thing is to interact with the physical environment, i.e. acts as a means to identify, monitor and control a specific part of the physical environment. In this view, the smart thing is just a tool. It is the real world entity, e.g. a building or a road segment, that is the ultimate target of interest. Connected things and smart things are deployed in a number of different environments.

Typical examples are:

- Personal environments like consumer electronics that is carried by the person or sensors for fitness or health purposes.
- Homes and buildings including commercial buildings
- Process and manufacturing industries environment, e.g. factory

---

1 http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/GSMA-Whitepaper-Embedded-Mobile-Guidelines-Release_3-Network-Aspects1.pdf
http://www.gsma.com/newsroom/wp-content/uploads/IR.49-v1.0.pdf

- Public infrastructures like road, rail, urban environments
- Utility infrastructures like electricity, water, gas, waste, heating and cooling
- Nature resource harvesting areas, like farmland, fish farms

The Digital Indians, young and emerging middleclass citizen, by definition, requires resources, starting with basic energy for better living, cooking, refrigeration, and transport. energy and fuel supply demands required to meet the middle class growth. Digital India can benefit from enhancing and utilizing the new regional competencies even more with both the macro-economy alternative scenario, as well as the demographic challenges give an increasing emphasis on the "frugal" and sustainability scenarios.

We at Ericsson strongly believe that TRAI will consider the facts from emerging global trends on IoT/ M2M business models, global framework, evolving standards, global M2M alliances, leading to penetration of billions of globally connected devices in the coming years making them an integral part of Digital India, Make in India initiatives by Government of India.

We also request TRAI to consider the following aspects captured in this document at pre-amble, response to questions and the framework captured at Annexure positively with a light touch regulation on M2M/ IoT licensing, allowing cloud based global platform implementation to facilitate uniform, scalable, flexible M2M/IoT services which would also help to have international harmonization of services and achieve economies of scale.

Best Regards

Manoj Dawane- VP and Head of Technology, Govt. & Industry Relations, Sustainability
Email id: manoj.dawane@ericsson.com

Reference: RINAT-16: 0053
Date: 2017-01-03

ANNEXURE

**Proposed Architectural Framework for M2M/ IoT Services Deployment in India**

The M2M ecosystem comprises of various domains starting with end users to their respective M2M application/service providers.

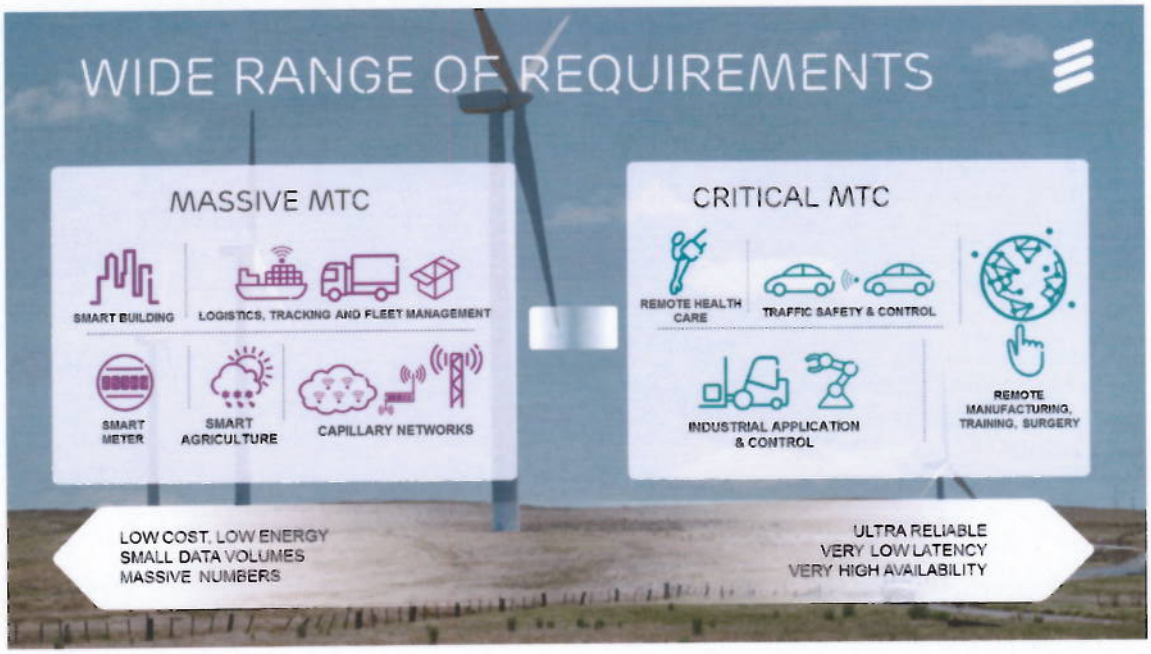
The ideal framework for global interoperable, uniform and affordable M2M implementation framework is as follows –

M2M is a low ARPU business with humongous diversity of application and device types, thereby imposing critical scalability and flexibility requirements at network, M2M platform and Application layer. To offer cost effective M2M services on a global scale, various regional alliances like Global M2M Alliance and Bridge Alliance created by operators in cooperation to share a cloud based M2M platforms, SIM/Subscripting Handling, Billing etc.

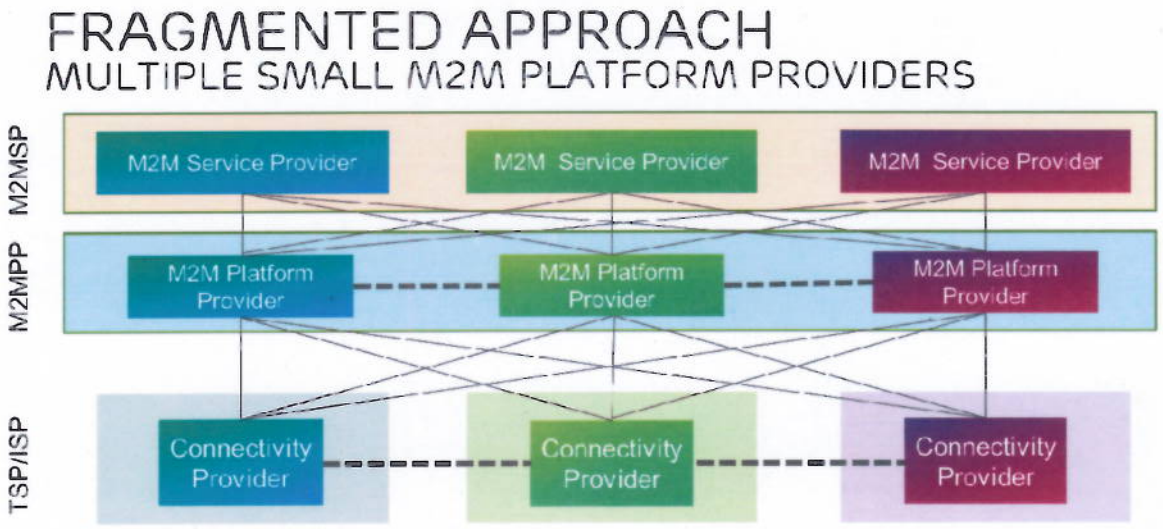
Therefore, to conclude we propose

1. It is M2M enterprise which is providing M2M/ IoT services to their end users who should be termed or classified as M2M SP.
2. Rest are enablers who are Platform providers and Connectivity Providers to the M2M SP
3. In order to secure the global play e2e interoperable and secure M2M eco-system, TRAI is requested to ensure the global cloud platform architecture for M2M Platforms to ensure economies of scale and reach (not to fragment this layer)

M2M comes with a peculiar challenge having two extremes of massive-M2M and critical-M2M and the range in-between, demanding different treatment. There is a need for end to end capabilities to support services with required quality of services and scalability involved from underlying network and M2M enablement layer.



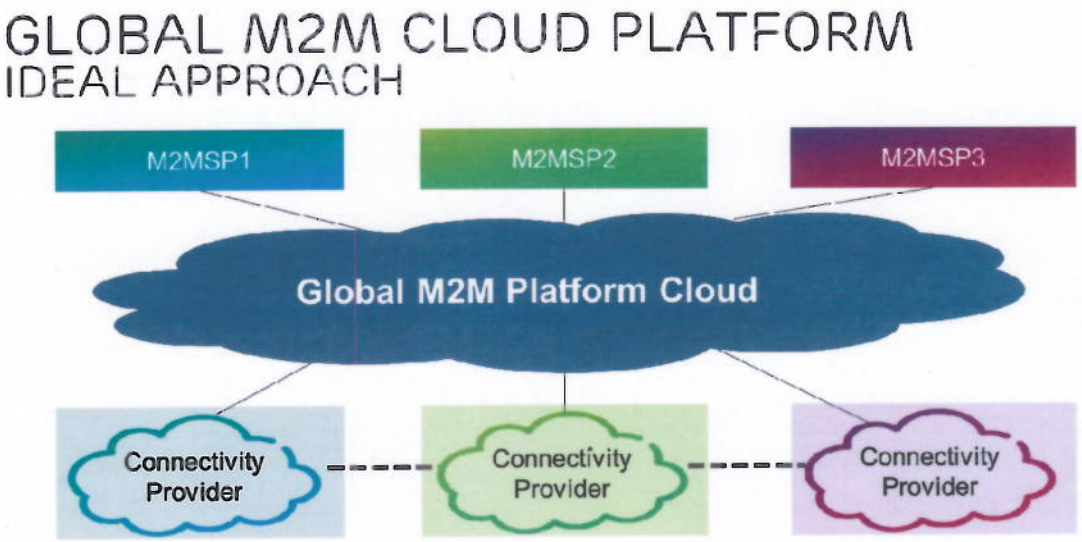
The key requisite to ensure a massive global play necessitates that fragmentation at various layers are avoided. A fragmented ecosystem would entail complex connectivity across the layers including congestion at signalling, core and access network of MNOs/TSP. In short fragmentation does not allow uniformity, scalability and flexibility on a global scale.




In order to simplify the interconnection, seamless integration, easy troubleshooting, uniform QOS, we need to simplify the delivery chain.

Having foreseen these challenges, global ecosystem reckoned that major TSP's and technology/platform providers forming a national/regional M2M alliance would be able to overcome these business, operational and scaling challenges. As a result, M2M Global Association was formed in Americas which covers all major operators in the region, and accordingly Bridge Alliance in APAC region combining all major operators. This provides economies of scale and global play for M2M/IoT players.

Finally, the architecture would provide a seamless interplay at global scale as follows-



Response to Questions

**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.**

Request TRAI to consider having a light touch regulation on M2M/ IoT services offering, without putting any additional license requirements on MNO's/ VNO's/ ISP's for full scale offering of M2M/ IoT services across all verticals, as they are already covered under DOT licenses/ guidelines. An MNO/ VNO's can potentially be M2MAP/ M2MSP as well as Enablers too.

Request a simple registration process that includes a light-touch regulation for M2M Service Providers/ M2M Application Providers (M2MSP/ M2MAP) if they are not already covered under any DoT prescribed license guidelines. M2MSP/M2MAP are Enterprises providing M2M services/applications to end users as well as service API's to third party applications.

M2M ecosystem comprises of the following:

M2MAP or M2MSP

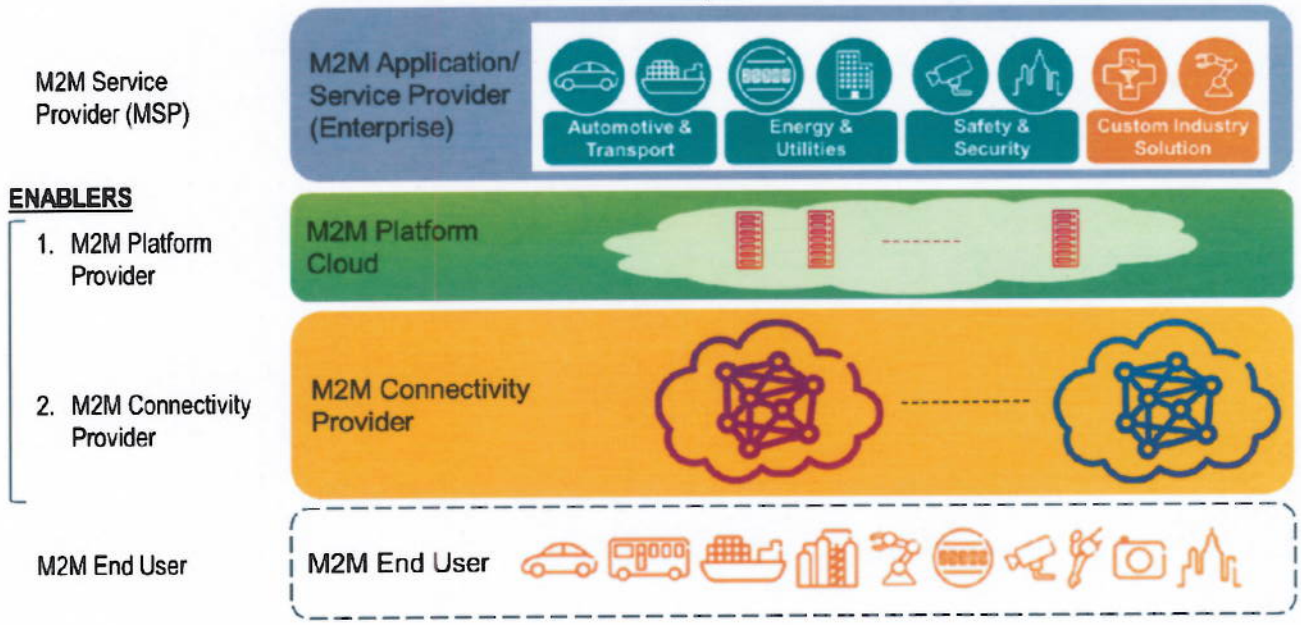
1. M2M Application Provider (enterprise) M2M Service Provider – E.g.: Manufacturer's, Enterprises, Utilities, Medical, Fleet, Asset management etc. (Consumer Electronics/ Automotive/ Appliances/ Hospitals/ Pharma, etc.)

Enablers:

1. M2M connectivity provider (MNO/ TSP/ ISP/ VNO)
2. M2M Cloud Platform Providers (Ericsson, Jasper etc....as well as Regional Alliances such as Bridge Alliance, Global M2M Alliance etc.)

End Users:

1. M2M end user devices and applications




The M2M/IoT platform provider is an Enabler to execute various functions required for M2M/IoT services. This platform layer will be integrated with application provider (M2MSP/M2MAP) as well as Telecom Service provider's network infrastructure.

**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.**

We request TRAI that there should be no entry fee and no license fee structure for M2M/ IoT services to facilitate exponential growth in the Indian market along with global penetration. M2M/ IoT will also spur growth in economy, Industrial automation, digitalisation and transformation as part of Make in India and build innovation based economy in start-up ecosystem. Digital India will be a reality sooner if there is a light touch regulation and a simplified registration process along with allowing centralized cloud based global platforms on M2M/ IoT services.

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

In continuity to the response to Q2, we reiterate that simple M2M SP registration without any licensing requirements with a light-touch regulation similar to global best practices be employed.

**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.**

In general, existing licensed and unlicensed spectrum framework in India would be able to cater the needs for M2M/IoT services and may not require dedicated spectrum allocations for M2M/ IoT services today. Based on the type of application and latency requirements, M2M SP will choose the appropriate network i.e. either existing licensed networks (2G, 3G, 4G, 5G) or the unlicensed network by ISP's.

For 3GPP or non-3GPP, our view is that the deployments have to be done as per the global harmonised standards of ITU for the respective technologies. However, if there are any considerations to allocate spectrum for M2M/ IoT, we strongly recommend India to follow ITU's WRC-15 Radio Regulations and to study and engage with ITU in WRC-19 standardisation process. We request TRAI to encourage deployments of globally standardised technologies including radio interfaces as per ITU for M2M/ IoT applications. Otherwise it will lead to dis-harmonious growth of fragmented islands in M2M/ IoT eco-system

Our view for M2M spectrum is to leverage all existing spectrum and network assets. In this context 3GPP has standardised various technology options for all IMT bands (licensed and un-licensed) to accommodate IoT connectivity requirements with the existing framework with slight alterations as may be needed for narrowband technologies. The 3GPP standardisation work is not just limited to Radio Access to scale, but also optimising the Core and Service Layer to cater to all M2M scenarios (Critical and Massive)

We bring to your kind attention that, the latest Ericsson Mobility Report of November 2016, where the spectrum requirement aspects have also been analyzed. The report can be accessed at-
https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf

**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?**

3GPP candidate technologies EC-GSM, NB IOT and LTE-M can work in all deployment bands for GSM and LTE respectively. We would thus like to stress the need for enabling deployment of M2M functionality in the already available and soon to be deployed frequency bands for commercial mobile networks. This will provide quick access to already deployed infrastructure in frequency bands that will provide excellent coverage, and with capacity that can be adapted to the increasing requirements. [new comments from MS]. However, the operation of NB IOT in unlicensed mode is planned for Rel-15. 3GPP is targeting to study NB IOT in unlicensed mode for sub-GHz unlicensed ranges and also coexistence with other unlicensed non-3GPP technologies.

If V2X spectrum is of relevance, we would suggest making a reference to European/American assumptions of roughly 30 MHz in the 5.9 GHz range. This amount of spectrum may need to increase in the future for more advanced applications.
From a general perspective, we would suggest considering frequency bands that are of international relevance, to ensure availability of equipment and also focussing on M2M applications in these bands without changing existing regulations. This is the approach being followed by CEPT.

**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.**

3GPP candidate NB IOT can work in all licensed deployment bands for LTE in in-band, guard-band and standalone mode. But the study for unlicensed mode operations for interface and coexistence and operational & regulatory implications is targeted for Rel-15 by 3GPP.

There are multiple technical challenges in embedding a 10MHz at the centre of 700MHz. This being a FDD band, having a delicensed portion in this can interfere with licensed FDD systems around it. Sufficient technical study is needed for such co-existence before parameters like guard band, Max-transmit power, ACI mask can be quantified. Trade-off between delicensed spectrum vs (interference, energy efficiency, impact on MBB systems on the adjacent licensed carrier) needs evaluated. We recommend to consider other globally agreed unlicensed bands in the sub-GHz than to consider the 700MHz band, which also gives the benefits of scale for low-cost M2M/IoT devices.

For interference between M2M UL and SDL with a 2 MHz guard band one may refer to ECC Report 242.

**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?*

National roaming for M2M/ IoT should be allowed without any restrictions. The tariff for roaming may be left to market forces to decide based on their commercial agreements similar to national and international roaming agreements in Telecom.

**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?*

We request TRAI to allow foreign eUICC's, as most of the devices imported to India may come with pre-fitted foreign eUICC at the factory with bootstrap profile.

National and International Roaming on Permanent basis be allowed for eUICC, embedded in M2M module/ devices. In that way, illegal use of removing it from device and using it in another device or porting is avoided.

Foreign eUICC should also be allowed, with the possibility to download local subscription profiles for local regulatory requirements. Foreign eUICC needs to be registered to the local network to be able to swap the profile using subscription management technology as per GSMA global guidelines

In the event, foreign eUICC is not allowed, there will be challenges to maintain separate eUICC SKUs in production line and supply chain logistics for the devices manufactured to ship to India. It adds cost, delay to the IoT devices shipped to India.

**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?**

We request TRAI to allow market forces to define and agree the commercial terms based on mutual agreement between the roaming partners under the prevailing regulations.

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

We request TRAI to allow market forces to define and agree the commercial terms based on mutual agreement between the roaming partners under the prevailing regulations.

**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?**

We request TRAI to consider the work carried out by TEC on numbering plan for M2M services. In the proposed plan by TEC provisioned two options as follows:

| Country Code<br>2 digits (+91) | M2M Identifier<br>2 digits | Licensee identifier<br>4 digits (10000 blocks) | Device Number<br>7 digits (10 Million) |
|---|---|---|---|

DoT has allotted 5 codes of three digit each ( 559, 575, 576, 579 and 597) for use as M2M identifiers as 2 digit spare code is not available at present. With 3 digits M2M identifier, the following two options are available-

Option -1:

| Country Code<br>2 digits (+91) | M2M Identifier<br>3 digits | Licensee identifier<br>3 digits (1000 blocks) | Device Number<br>7 digits (10 Million) |
|---|---|---|---|

Option – 2:

| Country Code<br>2 digits (+91) | M2M Identifier<br>3 digits | Licensee identifier<br>4 digits (10000 blocks) | Device Number<br>6 digits (1Million) |
|---|---|---|---|

As per DOT, it has provided 5 codes of 3-digit length – 599, 575, 576, 579, 597.

We request TRAI to consider a two digit M2M identifier instead of three, which could provide very large scalability.

While the scheme under both options of TEC mail may scale up to 50 billion count (each series 1000*10 million = 10 Bn), provided there is no dedicated identifier for M2MSP/MNO, M2M operation is operated at national level with no PLMN demarcation at circle level. However, such a scenario needs deeper analysis from feasibility and operability aspects.

The difference between option 1 and option 2 is numbering block-size. In option 1, the block size is 10 million and option 2 is more granular with 1 million block size.

Option 1, with 10 million block size, is more suitable for national operations by large players who run in to larger volumes of M2M connections while option 2 would be more effective for smaller operations.

**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.**

While we strongly agree that there should be necessary safeguards to maintain the security and privacy as per the law of the land, we request TRAI to consider and accept the existing security measures for USAL/UL/ VNO/ ISP's as they may be adequate to address the security measures for connectivity part and GSMA IoT security guidelines may be referred to for broader perspective.

**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.**

We request TRAI to consider that the policies may be adopted for cloud based services with the necessary security and privacy guidelines e.g., cloud services can be considered as long as Law Enforcement Agencies are provided mechanism for the Lawful Interception and the prevailing IT Act 2000 laws are followed.

**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.**

We request TRAI to allow the SLA's to be defined and followed mutually by the M2MSP/M2MAP with TSP/ ISP/ VNO, in the context of M2M services for that specific segment; since such services are evolving and require maturity and adoption

**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?**

The energy efficiency, end-to-end delay and transmission reliability etc., are specific to a particular use-case and technology specific and therefore may be left for M2MAP/M2MSP to be co-ordinated with the MNO/TSP/ISP/VNO.