By Speed Post

No. 2(5)/2016-CC&BT & ATC
Ministry of Electronics & Information Technology
6, CGO Complex, Electronics Niketan
New Delhi – 110003.

Dated : 01/03/2017

Subject: **Responses/comments from MeitY on the TRAI Consultation Paper on M2M Communications**

Please refer to your letter No. 103-3-2016-NSL-II dated November 25, 2016 regarding comments on TRAI Consultation Paper "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications".

I am directed to forward herewith the response from MeitY on the above Consultation Paper.

(R. Pitchiah)
Scientist 'G'
R&D in CC&BT Group
Tel: 011 24365755
24301231

Shri U.K. Srivastava
Principal Advisor
(Networks Spectrum & Licensing)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg, Old Minto Road
New Delhi-110002.

MeitY's response/comments on the TRAI Consultation Paper on "Spectrum, Roaming and QoS related requirements in M2M Communications"

Framework for M2M

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.

The business opportunity offered by M2M is huge and there may be several small players who would like to act as M2M service provider. There should be provision for amendment in existing license agreement for TSP/ISP/UL and also provision should be made to allow small player to enter into this area by way of new license for M2M service provisioning.

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.

M2M communication is expected to provide basic connectivity for devices mostly at low level and where minimal communication is required. As a result the proposal is to have a registration fee but no onerous performance of financial bank guarantee requirements. There can be many local instances of M2M communication — a large university /enterprise campus limited to local connectivity; a village where local devices are connected and are able to talk to each other for facilitation of agriculture and other services. In most of such cases the communication will remain local and not get onto any public network. In such, cases the requirement should be just registration — information about frequency band being used, possible range, power and expected device density but nothing more. It would be the responsibility of operator to ensure that the communication is local and does not get onto any public network.

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

They should follow all the extant guidelines of DoT and no other regulatory framework.

Spectrum Requirement

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

The current global trend is to use telecom network of TSP and or free wireless bands in non-TSP frequency domains for M2M communications. Currently countries are providing 10MHz or above for the services. The India scale of IoT/M2M devices communicating with centralized data servers or talking to each other will be in billions so atleast 20MHz spectrum be made available. As IoT devices grow exponentially in number, this space is going to be totally inadequate and needs to increase. Further, the quantum of spectrum required would depend on the services offered and the number of devices operating. It is, thus, difficult to predict the quantum of spectrum required to meet the M2M communications requirement, keeping a horizon of 10-15 years at this stage.

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 de-licensed?

Globally, the trend is to use telecom network of TSP and/or free wireless bands for M2M communications. Sub-GHz bands - 700 MHz, 800 MHz and 900 MHz spectrum bands, may be more suitable for M2M due to higher efficiency and better propagation characteristics. For short range communication high frequencies like Bluetooth, ZigBee, and 6LoWPAN could be used.

The quantum of spectrum available with TSPs and the de-licensed Spectrum available in country at this stage may be sufficient for M2M Communications.

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 de-licensed 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.

Adjacent channel interference for FDD system for M2M communications will have to be first analyzed.

National Roaming for M2M Communications

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

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

In compliance with NTP-12 policy of free Roaming/no roaming charge across the nation, roaming charges in case of M2M services for both inter-operator and intra-operator roaming could be free to begin with to help boost M2M services. Similarly, Inter-circle roaming charges for SIM's & services by the same operator, should also be free. This would require, separate template for roaming of M2M subscribers, allocation of separate identifiers like IMSI or MSISDN for M2M services and separate arrangements interconnect charges among TSPs. Similarly, separate identifiers may be required for policy decisions specific to the M2M communications based on the data relating to it.

(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

In line with the National Telecom M2M Roadmap, to begin with, foreign M2M devices sold and manufactured in India may be allowed to be equipped with SIMs of Indian TSPs only. Devices which are imported from foreign country may use embedded or soft SIMs or other such feasible technologies, where TSP profile/IMSI can be updated over the air. Permanent roaming of M2M devices fitted with foreign SIM/eUICC should be permitted in the devices to be used in India on the condition of fulfillment of traceability criteria in the long run.

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

c. There be a timeline/Iifeccycle of foreign SIMs to be converted into Indian SIMs/eUICC?

The timeline for switchover of already operational machines with foreign SIMs to Indian SIM be decided in consultation with relevant stakeholder so as to enable them to enter into commercial arrangements with Indian TSPs and perform requisite technical integration & testing to enable them to use alternate feasible technologies i.e. Soft-SIMs, Embedded SIMs etc.

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 time mutual agreement between the roaming partners?

The M2M ecosystem is seamless and global in nature and therefore, requires global agreements for international roaming charges for each vertical of device, services, etc. The Government / Regulator may in consultation with International entities work out international roaming charges for M2M communications.

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

The M2M ecosystem is seamless and global in nature and therefore, requires global agreements for international roaming policy. The Government / Regulator may in consultation with International entities work out international roaming policy for M2M communications.

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?

Allocation of separate Mobile Network Code (MNC) to MSPs will allow them to change the TSP as per their convenience and will not force them to tie to a TSP.

Security & Data Privacy

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 don't want to burden the system with too much regulation that impedes its adoption. However, we must recognize that M2M/IoT devices present a variety of potential security risks that could be exploited to harm consumers by:

(1) enabling unauthorized access and misuse of personal information;
(2) facilitating attacks on other systems; and
(3) creating safety risks by compromising the actual functioning of devices in the field

Therefore, the security framework for IoT needs to ensure: -
- security of the M2M/IoT device interface
- security of the data held by the device
- security of the data during transition
- security of the interface between the device and rest of the data network

So having regulation in place to ensure that companies developing M2M IoT products should implement reasonable security during design an manufacturing stages. There should be guidelines for device manufacturers to be followed. It should be necessary to build enough protections in the device which would prevent their take-over and usage to disrupt the traffic. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Initially it can be an advisory but later it should be enforced via regulation so that every device gets an appropriate certificate before it comes to the market.

Also, the regulation should require the manufacturers and service providers to be responsible for any security threats that are detected pos the device is deployed in the field. In such cases, the regulation should work the way it currently works for automobile sector wherein there is a well defined process of recall or in this case it could be proper remediation.

It is also true that different devices may be subject to different levels of security risks. Therefore, the regulation may prescribe a graded level of security certification so that the low risk devices do not have to deal with the burden of the regulation.

Companies/service providers should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.

Also, companies/Service providers should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

The regulation should also encourage companies to encourage adopting industry best practices that will continue to evolve from time to time.

Comments of CERT-In

- Policy and standards for devising naming, numbering and addressing schemes for M2M devices to support identification and traceability of connected objects by various parameters should be considered.
- Regulations for quality of service for connected devices having different bandwidth requirements as well as standards for dynamic lawful interception for M2M devices and security of data retention systems for the use of law enforcement should be ensured.
- M2M should be capable of managing heterogeneous data which would be continuously communicated through numerous devices.
- In order to ensure that the flow of data between devices does not run into latency issues, appropriate standards based protocols need to be deployed so as to minimize the latency

For manufacturers:

- Build and incorporate security at the design stage and enable security by default during production/operations stage.
- Use secure hardware such as computer chips that integrate security at the transistor level, embedded in the processor and provide encryption and anonymity.
- Use trusted and hardened operating system. Dev se mechanisms and process to detect vulnerabilities, develop patches to plug the same and mechanism/protocols to apply patches to the end devices with customer consent. There is a need for secure device firmware which could be signed by an irreversible device identifier and securely delivered to the machine over a secure communication channel.

For network operators:

- Put in a place a mechanism for authenticating the identity of the machine/ device, authorizing the devices for access and managing the specific privileges and services available to the device including management of groups of devices connected via a gateway.

- Devise appropriate logging mechanisms to facilitate identification of end device and user. The end deice may be compromised and used as a conduit for cyber/physical attacks. In order to mitigate attacks on compromised devices, cyber security agencies need to reach out to operators and end users to notify mitigation measures. This activity need to be facilitated through proper logging systems and processes.

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.

Data Capture

An M2M/IoT device should limit the amount and extent of data it collects and retains, and dispose of it once they no longer need it. This approach is required because the footprint of security risk is directly proportional to the size and lifetime of the consumer data captured by the device. Therefore, by limiting the amount of data and its lifetime, the risk to consumer's data and privacy can be reduced/minimized.

Consumer Consent

IoT devices generally offer limited user interface. This may encourage the manufacturers/service providers to avoid taking consumer's consent before capturing consumer's data. However, there is a greater need for consent in the IoT landscape because there is a higher degree of risk to consumer's data & privacy. Therefore, the regulation should enforce all manufacturers/service providers to provide a foolproof method of seeking consumer's consent before they collect any data. The evidence of such consent must be recorded, verifiable and must be shared with the consumer.

Considering that the IoT devices may have a limiting user interface to implement such a consent dialog, manufacturers/service providers should be encouraged to utilize 'out of band' channels like SMS, email etc. or offer a web/mobile app based interface for implementing the consumer consent.

Provision in IT Act

Information Technology Reasonable Security Practices Procedures and Sensitive Personal Data or Information (IT RSPPSPI) Rules 2011 must be read in conjunction with Section 43A of the IT Act. It recognizes International Standard ISO/IEC 27001 on "Information Technology — Security Techniques. Information Security Management System — Requirements" (ISO/IEC 27001). A body corporate or any person who on behalf of the body corporate collects, receives, possesses, stores, deals with or handles information must have a privacy policy (Rule 4). The privacy policy must be published on the website of the body corporate or any person acting on its behalf, and include the following:

- A clear and easily accessible statement of the body corporate's practices and policies.
- The type of personal or sensitive personal data collected under Rule 3 of the IT RSPPSPI Rules.
- The purpose of collection and use of the information.
- Details regarding the restriction on publishing sensitive personal data or information under Rule 6(3) of the IT RSPPSPI Rules.
- Reasonable security practices and procedures as provided under Rule 8 of the IT RSPPSPI Rules.

Consent

Consent to disclosure is usually required. However, information collected can be shared, without obtaining prior consent from the data subject, with government agencies mandated under the law to either (Rule 6, IT RSPPSPI Rules):

- Obtain information including sensitive personal data or information to verify identity.
- Prevent, detect and investigate I relation to cyber incidents, prosecution and punishment of offences among other things.

Rights of individuals

The IT RSPPSPI Rules do not require any information to be provided to data subject at the point of collection of the personal data. There are no relevant provisions under the IT Act. No other specific rights are granted to data subjects.

The IT RSPPSPI Rules do not provide data subject with the right to request the deletion of their data. However, the data subject can withdraw consent previously given to a body corporate (Rule 5 (7), IT RSPPSPI Rules). In addition, the body corporate or any person on its behalf must not retain the information obtained for longer than required either (Rule 5(4), IT RSPPSPI Rules):

- For the purpose for which the information may lawfully used.
- Under any other law for the time being in force.

Security requirements

Rule 8 of the IT RSPPSPI Rules requires a body corporate (or any person acting on its behalf) to comply with reasonable security practices and procedure. Reasonable security practices and procedure. Reasonable security practices and procedures means those designed to protect personal data from unauthorized access, damage, use, modification, disclosure or impairment.

These may be specified in an agreement between the parties or in any relevant law in force (or, if there is no agreement or relevant law, by the central government in consultation with professional bodies or associations) (section 43A, IT RSPPSPI Rules). The IT RSPPSPI Rules recognised ISO/IEC 27001 provides implementation advice and guidance on best practice, including in relation to:

- Information security.
- Asset management security.
- Human resources security.
- Physical and environmental security.
- Communications and operations management.
- Access control.
- Information system acquisition.
- Development and maintenance.
- Information security incident management.

The IT RSPPSPI Rules do not provide a requirement to notify personal data security breaches to data subjects or the national regulators.

Liability for body-Corporate under Section 43A

Section 43A introduces a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

The "reasonable security practices" which the section obliges body corporate to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central government

Quality of Service

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.

The M2M ecosystem is composed of a large number of diverse players, deploying innovative services across different networks, technologies and devices. Therefore, different types of SLAs will have to be defined at point of interconnects at various layers of Heterogeneous Networks to meet diverse QoS guarantees. Some of the parameters for defining SLAs for communications/IP network are throughput (100%). latency(less than 45 milliseconds), packet loss (less than 0.3%), jitter (less than 0.5 millisecond).

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?

No specific comments.

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

i) The policy should be technology neutral, service neutral. Once basic framework is in place, service providers should be free to provide any kind of service over the network, competition should not be prevented by providing any kind of monopoly to services (example of VoIP comes to mind which competed with normal GSM based voice services).

ii) IoT/M2M will lead to new systems/products/services where machine will take decision based on certain available data. Legal frameworks should be created for issues that might arise due to IoT related product/systems/services.