Telenor (India) Response to TRAI Consultation Paper on Review of the Regulatory Framework for Interconnection (No.21/2016 dated 18 October'16)

Preamble

Telenor India welcomes the opportunity to provide comments to this TRAI consultation paper. TRAI has rightly mentioned that M2M communication will be a game changer for the industry and the economy at large. The M2M and IoT service business models are different from traditional telecom business model. Therefore, the success of M2M will depend upon the cross sector policies and entail modernization of existing regulatory framework.

The positive impact of the M2M and IoT services on citizens, consumers, businesses, and governments promises to be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety. Governments can realize these significant social and economic benefits through the growth of M2M and IoT services by ensuring supportive policies and regulations that are relevant, light touch, flexible, and technology neutral.

Regulatory reforms are imperative for the success of M2M

The role of licensed TSPs is to provide connectivity for the M2M services, nevertheless this is the most critical and important role in the entire value chain of M2M services. The present licensing conditions are designed keeping in view the traditional voice and SMS services provided by networks interconnected through national / international carriers for transport of traffic. In the IOT space, the platform and networks are designed for global deployments and are fundamentally different from traditional networks.

Thus there is a need for modernization of existing regulations to facilitate M2M services.

There are various licensing restrictions imposing threat to the growth of M2M services in India. These legacy regulations not only create regulatory challenges, impose additional costs on consumers & businesses, discourage innovation, but, they often become ineffective to achieve economic and social objectives for which they were designed. There is a need to take a fresh look at policies and their regulatory approach to reflect changes in technologies and markets of tomorrow. The future will require a more technology-agnostic and flexible approach, where legacy regulations do not weigh down the pace of march of digital eco-system where every stakeholder can compete on a level playing field. We are of the view that these regulatory reforms will not only help in faster development of M2M ecosystem in India but also improves competition in the communication sector.

Regulatory framework for M2M

Regulating M2M and IOT will also pose a risk to regulate other sectors (other than communication) involved in M2M services by default disrupting the growth of M2M services. Thus, specific policies / regulations for M2M and IOT regulations / policies are not required. Instead, government should promote interoperable and industry-developed specifications and adoption of global standards across the M2M industry verticals. Interoperable platforms and services reduce deployment costs and complexity, facilitate scalability and enable

consumers to enjoy intuitive connected experiences. The M2M policy guideline should facilitate adoption for this future technology used by machines rather than imposing restriction similar to traditional telecom services used by humans and proposed policy frameworks should be technology and service neutral with very light touch regulatory framework.

Global solutions and economy of scale

There are popular deployments of the M2M services that are using global platforms; this is to achieve scale and availability of trained and specialized resources at a common location. Further, the cloud-based solutions are increasingly the technology of choice for M2M deployments. Any strict data residency within the country requirements would restrict these solutions to be deployed. In our view, in order to effectively utilize the benefits for the success of M2M services, there should not be a blanket restriction on cross border data transfer & storage. Cross border data transfer should in turn be regulated not restricted to fully harness the benefits of cloud computing.

We quote from the BEREC report (page 4 of the CP) *'Many M2M services are provided via devices designed and produced for the world market and for usage based on global mobility.'*

International permanent roaming

The global distribution models and use of embedded SIMs in devices at the manufacturing stage are the key attributes of the M2M business model. The M2M devices are connected to multiple networks and necessarily not its home network. This flexibility of international roaming should continue in the future. The international permanent roaming enables scalable, well-tested and speedy deployment of M2M and IoT Services. Any prohibition of the use of foreign SIMs based on permanent roaming would impact early deployments of M2M and IoT services, resulting in commercial loss for different providers in the value chain.

Data and privacy rules

The issues relating for data privacy of consumers and users should be equally applicable for all stakeholders. A new act for privacy should be designed and enforced – the intent being that M2M and IoT services will impact all citizens with some service or the other e.g, eCommerce, eGovernance, e-payments, skill development, education, health etc. A comprehensive centralized act should be brought in. The rules relating to transfer of information or storage of data should be equally incorporated in the Unified Licenses as in the 'Reasonable Security Practices and Procedures and sensitive personal data or information 2011 Rules' dated 11th April 2011 of the IT Act 2000.

Key submissions

- Modernize the existing telecom regulations to facilitate M2M services
- Recognizing the global network architecture of M2M networks, standards for security and privacy should be designed, which are horizontally applicable to all
- Facilitate rather than regulate, Authority has noted that M2M is at a nascent stage in India

Question wise Response

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.

Response:

Telenor India is neither in favour of any licensing framework nor advocates for mandating registration for M2M service providers. At best a registration may be required with obligations to follow the technical standards and conform to security and privacy horizontal regulations.

TRAI and DoT should ensure enabling, relevant, technology and service neutral policies and regulations across the entire M2M ecosystem and treat equivalent services in the same way. This becomes more important due to the involvement of large number of diverse stakeholders in the M2M value chain catering to multiple verticals/ areas. Following are our arguments to support our view –

- Presently, M2M communication and IoT industry are at nascent stage of growth globally and would become an important part of human life in next few years. These services will have multiplier effect in accelerating socio-economic growth of any economy. The positive impact of the M2M and IoT services on citizens, consumers, businesses, and governments promises to be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety. Thus, M2M is serving various sectors / verticals including Automotive & transportation, Energy, Health, Safety & surveillance, smart cities etc.

- The business models, markets and services for M2M and IOT services are fundamentally different from traditional mobile voice and data messaging. It has global dimension and involved complex value chain including Module, Device / Sensor manufacturers, online platforms, connectivity providers, system integrators, application providers and other vendors like billing & support. TRAI has acknowledged these facts in the paper. In para 2.4, TRAI has mentioned that the M2M service provider could be alone a platform provider or application provider or gateway provider or any combinations of these layers. Moreover, these M2M services / applications have different functionality / usage for different verticals.

- In the entire M2M value chain, connectivity is a smaller piece but critical and has a major role in delivering end to end services. Therefore, the Licensor and Regulator should work

towards enabling a regulatory framework for connectivity provider by simplifying the existing restrictive license conditions to stimulate innovation, investment and growth of M2M services. Some of these conditions are: reselling of services, cross border data sharing, data protection and privacy, stringent KYC norms, maintenance of end user data base, SIM ownership etc. Any temptation to over regulate should be resisted, else it will hamper the growth of M2M services in India.

- The underlying assumption here is that any standalone M2M service provider will take the telecom resources from a TSP providing services using licensed spectrum.

- Therefore, Telenor India is of the view that specific policies / regulations for M2M and IoT regulations / policies are not required. Instead, government should promote interoperable and industry-developed specifications and adoption of global standards across the M2M industry. Interoperable platforms and services reduce deployment costs and complexity, facilitate scalability and enable consumers to enjoy intuitive connected experiences. Globally, ITU and various Standards Development Organisations are engaged in standardization activities. In India, TSDSI and C-DOT is working on M2M standards. GSMA has M2M and IoT guidelines in place and same can be adopted by India.

- However, in case TRAI still feel the requirement of regulatory framework for M2M services, we recommend that the registration for M2M service provider under M2M Category registration with light touch licensing and obligations to follow the technical standards and conform to security and privacy horizontal regulations. The validity of registration should be for 20 years. This is very important for the successful proliferation of M2M services in India.

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

Response:

Not applicable in view of our above response to Q1 & Q2.

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?

Response:

- We are of view that there is no need for any separate allocation / earmarking of Spectrum exclusively for M2M communications. M2M and IoT services have very different characteristics, a plethora of existing and planned technologies as well as diverse spectrum usage and access methods. Thus, spectrum requirements for M2M are purely dependent on the nature of service offered and connectivity structure deployed by M2M service provider.

- As far as spectrum is concerned, India has shifted from spectrum deficit era to spectrum surplus era. TSPs are having sufficient capacity to cater to M2M services. Before allocating any specific spectrum band for M2M services, the available capacities with TSPs should be optimally used first and understand the challenges /spectrum requirements during M2M evolution journey.

- Mobile cellular solutions already play a significant role given M2M can operate in spectrum allocations intended for mobile. In addition, a number of harmonised standards have been developed recently (e.g. 3GPP or GERAN) to optimise the use of mobile spectrum bands for IoT. Thus, the mobile industry is an important enabler and well placed to lead the sector.

- Cellular networks support M2M devices alongside conventional subscribers so existing and future mobile spectrum licenses support M2M as standard. As long as TRAI continues its positive efforts to license sufficient additional amounts of spectrum for mobile use, it will be able to support cellular M2M. Crucially, the M2M technologies in the latest 3GPP standard, Release 13, significantly build on the coverage capabilities of existing spectrum. For example, initial trials have demonstrated that 2G networks require only a software upgrade to enable a seven-fold improvement in the range of low-rate M2M applications and extended device battery life (up to 10 years).

- Currently there is no harmonised dedicated spectrum allocation for M2M and operators are using spare capacity on 2G, 3G and 4G systems for M2M services within existing spectrum allocations. We support harmonisation of frequency bands for mobile services as it would ensure the efficient use of spectrum while also galvanising the cellular IoT market by driving the widespread creation of low cost devices, which can be used worldwide. In order to realise this goal, government should work with the mobile and M2M ecosystem, including mobile network operators and vendors, to examine which bands should be harmonised and band plan considerations. Harmonised bands need to be able to support the full range of potential M2M scenarios. This includes high data-rate applications, which could require substantially more spectrum than forecasts based on today's usage profiles would suggest.

- The de-licensed spectrum under ISM band which has already been earmarked globally by ITU for industrial, scientific and Medical applications will be sufficient for different requirements of M2M and IOT services for short ranges.

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.

Response:

- We differ with TRAI proposal of using portion of 700 Mhz centre gap for unlicensed M2M services. This approach represents a significant threat to the viability of the 700

MHz band for mobile broadband services. The centre gap in the APT 700 MHz plan is very narrow which means that unlicensed services would inevitably be operating in spectrum that is in very close proximity to future mobile broadband services.

- The 700 MHz band is central to the future of widespread, affordable mobile broadband access in India so every effort must be made to protect it. It is essential that any use of the centre gap does not create interference to future mobile services in the 700 MHz band, nor should it reduce the amount of spectrum that is licensed for mobile services in future.

- Furthermore, it should be noted that most unlicensed bands are either globally or regionally harmonised. Thus, creating India-specific unlicensed band without widespread international agreement, given that economies of scale are very important for M2M applications in order to reduce the cost of the devices/technology used. Also, given the band have extremely good propagation qualities there are also implications for cross border interference so needs to involve consultation with neighbouring countries.

- Going by the current experience, Cellular networks are already suffering from interference from various sources such as illegal repeaters, jammers etc. Presently, the 700 MHz Band is free from interference effects and any de-licensing of frequency range in the 10 MHz centre gap would pose considerable interference risks without providing any significant benefits due to uncoordinated use.

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?

Response:

National roaming for M2M/IoT devices should not be made free. It should continue to govern by the existing TRAI roaming regulations. We have following points to support our view -

- There are costs involved in providing national roaming services and TSPs should be suitably compensated for the same by M2M service provider.

- Economically, the business model of M2M services is entirely different from traditional retail voice, SMS and data services and a very large number of M2M and IoT applications do not involve personal consumers. There are wide range of deployment models, alternatives and often a combination can be utilised for M2M and IoT services - all have their own advantages / disadvantages. The ultimate choice of deployment model depends on a number of factors, such as M2M service provider, the end-user, the scale and geographical footprint of the deployment, the type of application, the device lifetime, its accessibility and the bandwidth requirements etc.

- We suggest that TRAI should allow for the dynamics of a competitive market to deliver the solutions for the social and economic benefits to be derived for the economy as a whole and consumers. Operators are well placed to make these decisions and to negotiate commercial agreements to deliver the benefits of M2M and IoT. The incremental investment required to support M2M and IoT is dependent on the ability for mobile operators to arrive at sustainable commercially agreed complex agreements.

Q8. Whether 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.

Response:

- Telenor believes both domestic SIM/eUICC and Permanent roaming foreign SIM/eUICC should be allowed. Restricting adoption to one or another SIM and business model would be a mistake and could potentially hamper the uptake of M2M and IoT services in India. The M2M and IoT space is composed of a variety of verticals, with different justifiable needs. In some instances the need is global but in others it is local. It should be left to the market to decide the type of SIMs and model to be used. As an example, for an international automotive maker selling vehicles globally a foreign SIM/eUICC would better to address the needs of a cost efficient, scalable and centralized solution. However, a company selling M2M and IoT services locally in India only would not have the same need to adopt a foreign SIM.

- There is no embargo in India today on permanent roaming and the same should be continued. International Permanent Roaming enables scalable, well-tested and speedy deployment of M2M and IoT Services. Several automobile firms like Volvo Cars, Nissan, Renault etc operate on the same model in other countries as well. It can facilitate a rapid deployment of M2M and IoT services in India by international multinationals and, in reverse, provide an opportunity to multinationals of India to export M2M and IoT services and devices.

- From a Make in India perspective, M2M/IoT devices will be manufactured in India with SIMs from local Operators and exported world over. Any restrictions in international permanent roaming could be seen as a protectionist measure and may also encourage similar action by other nations.

- Prohibition of the use of foreign SIMs based on permanent roaming would impact early deployments of M2M and IoT services, resulting in commercial loss for different providers in the value chain. In most cases, the cost for changing a SIM installed in

an M2M/IoT device is considerable and rarely justifiable. For that reason, it is not appropriate to have a timeline for conversion into domestic SIMs.

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?

Response:

- It should be left to the parties involved to freely agree on the appropriate international roaming charges. It would, however, be wise for regulators to follow-up the development of the charges applied in these cases, as to avoid having a party with significant power applying unreasonable commercial conditions which would in fact lock the market.

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

Response:

- We believe there is no need at this point to have a separate International roaming policy for machines, the existing ones for voice and data should apply.

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?

Response:

- Telenor does not believe the benefit justify having MNCs allocated to MSPs. Today, there are different solutions (proprietary and GSMA) in the market to allow a SIM Card to be re -provisioned over the air with a new Service Provider, avoiding the MSP lock-in.
- Benefit: Easier for MSP to switch Service Providers of connectivity, avoiding lock-in, as the costs of swapping SIMs deployed in field are usually prohibitive.
- Negative: Increased technical complexity for the MSP. It could be argued that security could be compromised by having an unexperienced private third party handling identifiers.

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.

Response:

- The connectivity providers (TSPs) are offering licensed services and governed by security conditions stipulated in their Unified license. These conditions are comprehensive and sufficient. Thus, there is no need for any additional requirements for specifying security of networks as existing conditions in Unified License are

adequate for M2M services. The standalone M2M service provider has the option to sources telecom resources from any of the licensed TSPs which are governed by conditions of UL.

- Further, the SIMs/Connections for M2M Services would be provisioned with restricted services i.e. would be allowed to communicate to predefined telephone number or a server.

- The 'best practice' principles for securing networks and data are a good starting point for offering M2M services. GSMA IOT security guidelines can also be implemented by M2M and IoT service provider. These set of security and privacy best practice guidelines that explain how an M2M Service Provider can secure their M2M service from most cyber security attacks and can serve as rules and a security benchmark for M2M service providers. Essentially, for a sustainable eco-system for M2M services the GSMA rules and the self assessment should be followed by all M2M service providers.

- The rules relating to transfer of information or stored data should be equally incorporated in the Unified Licenses as in the Reasonable Security Practices and Procedures and sensitive personal data or information 2011 dated 11th April 2011 of the IT Act 2000. Rule 7 of the said rules allow for transfer of information to any corporate within India or another country as long as the same data protection rules are being followed.

- The Unified Licenses should be suitably amended to enable this transfer of personal information as well.

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.

Response to (a):

- In M2M value chain there are various stakeholders involved enabling end-to-end seamless M2M communications among connected devices. The M2M data generated by these connected devices will be recorded and saved in the systems maintained by M2M service provider.

- In M2M/ IoT domain, different applications and services will have different requirements for security and resilience. As pointed out in para 2.45 of the paper, majority of M2M applications and databases will be hosted on cloud in order to achieve higher economic efficiency. Some of the global M2M application providers

are possibly using cloud servers located in their home country / central location catering multiple countries.

- We acknowledge that there are challenges on enforcing regulations regarding placing servers outside India for hosting consumer data. In our view, effective jurisdiction needs to be established to enforce relevant regulations. Further, it is also our view that in order to effectively utilize the benefits for the success of M2M services, that there should not be a blanket restriction on cross border data transfer. Cross border data transfer should in turn be regulated not restricted to fully harness the benefits of cloud computing.

- Restrictions in licence conditions on the use of data and cross-border transfer of data should be removed and government should allow data from M2M devices to flow to service providers and responsible parties in other countries. Placing restrictions on the flow of data (a) creates costs for companies, (b) deters inward investment, and (c) is disproportionate.

- In reality, a blanket restriction on cross border data transfer across all citizens is no longer achievable today. Many online communication providers, including social networking and VoIP providers as well as a wide range of application service providers are already providing services to Indian citizens where data is processed, stored and transferred cross border. Google search engines also collect data from users each time a search is conducted.

- Some of the concerns about cross border data transfer relate to national security can also be mitigated through:

    a. Formulating a list of countries that provide adequate protection of personal data and restricting personal data transfer only to countries on the list
    b. Enforcing use of modal contractual clauses to regulate transfer of data (as it had been done in the EU)
    c. Enforcing approved binding corporate rules where transfer is conducted within the same group of entities which are located in different jurisdictions
    d. Achieving mutual understanding with the relevant regulators within the foreign jurisdiction on the facilitation of cross border transfer (such as the US-EU Privacy Shield that is currently being developed).
    e. The APEC's[1] Cross Border Privacy Framework[2] can also be looked into as an international cooperation initiative with an aim to facilitate (as opposed to restrict) flow of data across borders and at the same time ensure consistent privacy standards.

[1] Asia Pacific Economic Commerce - a forum of economies recognizing importance of protecting privacy and maintaining information flows among economies in Asia Pacific region and among their trading partners.
[2] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

These are the regulation that the European Union has adopted to regulate cross border data transfer. Similarly, the Government of India may publish the list of countries where cross border data can be hosted.

The issues relating for data privacy of consumers and users should be equally applicable for all stakeholders. M2M or IoT will impact the lives across the spectrum of citizens and users in India. Therefore, a separate act for Data Privacy and Protection that governs the principles, rules and remedy is essential for India. This will form the trust edifice of Digital India and allow structured and protected adoption of digital services across various industries in the B2B and the B2C Space.

Response to (b):

- TRAI has righty expressed its views on importance of data security and privacy for M2M communications in para 2.60 and envisaged to have in place balanced and clear rules for data security and privacy. Therefore, there is an immense need to have proper and implementable privacy policy in place for consumer trust which is critical for the development of M2M solutions and to realise the benefits of IoT for individuals and society in general.

- The main key to consumer trust in the digital ecosystem is transparency towards the individual, but other principles are also very important such as collecting only relevant data, making sure the data are not processed for incompatible purposes, keeping the data secure, checking the accuracy of the data and making sure individuals' rights are not prejudiced by transmitting data to another jurisdiction.

- The existing IT Act 2000 is horizontal in its approach as it applies to use of 'personal information' regardless of sector, but it falls short of the omnibus-style laws adopted in other countries. The current law should be reviewed to include all stakeholders involved in the handling of consumer data.

- Some of the suggestions are as follows to amend IT Act 2000 :

    - It should be applied to all parties who make use of the data regardless of sector or technology used
    - Include the idea of privacy-by-design and default to reassure consumers making applicable to entire value chain of M2M service.
    - Allow data from M2M devices to flow to service providers and responsible parties irrespective of location.
    - Concerns about consumers interests when data flows abroad can be addressed by putting duties on organisations to procure service providers with good security standards and to check and enforce those standards on behalf of their consumers
    - The rules relating to transfer of information or stored data should be equally incorporated in the Unified Licenses as in the Reasonable Security Practices and Procedures and sensitive personal data or information 2011 dated 11th April 2011 of the IT Act 2000. Rule 7 of the said rules allow for transfer of

information to any corporate within India or another country as long as the same data protection rules are being followed.

- Restrictions in licence conditions on the use of data and cross-border transfer of data should be removed in favour of the omnibus-style provisions outlined above. The unified licenses should be suitably amended to enable this transfer of personal information as well.

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?

Response:

- The ecosystem for M2M and IOT services in India at nascent stage. We of the view that at this juncture there is no need to define QoS parameters exclusively for M2M Communication / IOT services and applications. Moreover, TSPs are already governed by QoS parameters applicable for data services and same should be applicable to M2M services.

- The M2M and IOT services are of different nature and spread across various sectors having very different characteristics, a plethora of existing and planned technologies as well as diverse spectrum usage and access methods. The QoS and SLAs for M2M services are purely depend upon the type of service offered, connectivity structure deployed by M2M service provider. Therefore, the standard SLAs for each M2M service will not be applicable and should be mutually agreed between the M2M service provider and connectivity provider.

- Further, licensed and unlicensed spectrum will have different QoS for M2M services. The licensed spectrum is uniquely able to provide high quality of service guarantees over wide areas without any interference and can control usage levels as they have exclusive access to their spectrum bands. The licensed spectrum will have higher assurance level for crucial M2M services such as security, transportation and medical applications. Whereas, unlicensed spectrum having low power and high risk of interference, may not always support such critical applications which demands higher QoS levels.

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

Response: We would like to submit our comments on the following:

Numbering Series: We have submitted our recommendation to TEC on their proposal. Key suggestions are reiterated below -

- The 10 digit for voice/SMS/ data and 13 digits for M2M devices and gateways should continue to co-exist.
- Any additional allotment for M2M beyond first block should be based on actual utilization. It is suggested to form a Committee having industry representation to decide the criteria for number series allocation for M2M services.
- Allocation of number series should be licensed service area wise, however deployment can be pan-India basis as it will be for captive network/ VNO parented to the licensed TSP.
- The option of getting allocated fixed line series and demarcating specific blocks for M2M for specific TSPs should be made. Such arrangement will ensure easy identification of the connectivity service provider across the M2M value chain.

KYC –

We quote from the consultation paper – *'In most cases, the business model is B2B, even if devices may be aimed at consumers (B2B2C). The business model is usually not B2C4. '* In this scenario, the TSP should maintain the KYC details of the business partner and the quantity sold. Thereafter further details and traceability of devices should be the responsibility of M2M service provider. MSP may be registered with DoT and comply with the norms. Retails KYC norms for M2M modules should be separately developed.

- TSP should not be held responsible for any misuse of the telecom resources provided to M2M service provider. TSPs responsibility ends with activation of SIM after carrying out the subscriber verification as per current procedure.
- TSP should maintain the KYC details of the business partner along with the quantity of SIMs sold.
- M2M service provider who will be interfacing and maintaining the relationship with end user using the M2M devices should be mandated to maintain the database of MSISDN and IMSI. This can be shared with TSP and designated LEAs.
- Traceability guidelines as applicable to humans should not be imposed on machines as there is no single user of a device viz. wearable device.

***