GSMA response to the TRAI Consultation on:

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

12 January 2017

New Delhi

Executive Summary

The GSMA welcomes the opportunity that the Telecom Regulatory authority of India (TRAI) has offered to provide comments to its consultation paper: "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M)."

Machine-to-Machine (M2M) and Internet of things (IoT) represent a huge opportunity and can bring substantial socio economic benefits to Indian users, businesses and government. The Indian government and policymakers can unlock this opportunity and make a difference to its citizens and businesses.

The following parts of the document provide a brief summary of the GSMA position on key topics covered within the TRAI consultation, followed by a dedicated section with answers to the specific questions raised. In summary, the GSMA submits the following:

On **Spectrum**, it is essential that TRAI recognises that licensed spectrum is at the heart of India's sizeable M2M market today. Cellular networks support M2M devices alongside conventional subscribers so existing and future mobile spectrum licences 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.

The GSMA discourages TRAI from considering the 700 MHz centre gap for unlicensed M2M. This approach represents a significant threat to the viability of this band for mobile broadband. Also, most unlicensed bands are either globally or regionally harmonised. So the GSMA advised India government not to create its own unlicensed band without widespread international agreement, given that economies of scale are particularly important for M2M applications.

On **Mobile Network Codes,** the GSMA believes that TRAI should not allocate separate MNC to M2M service providers. The solution presents security and fraud risks connected with private parties being assigned numbering resources, procuring and issuing SIM cards. Technical solutions, such as the GSMA Embedded SIM specifications, are available today and eliminate the need to change MNC allocation policy.

Answers to the consultation questions

Spectrum

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.

Currently, Indian mobile networks, which operate over licensed spectrum, already support over 6.5 million cellular M2M connections and this is growing fast[1]. It is essential that TRAI recognises that licensed spectrum is at the heart of India's sizeable M2M market today. Furthermore, the rapid evolution of cellular IoT technology, especially through new 4G solutions and in future 5G, means the importance of licensed-based mobile networks will increase rapidly in future. TRAI should ensure its planning for M2M considers licensed spectrum – not just unlicensed spectrum. This approach will encourage innovation and competition and ensure India takes advantage of widespread mobile network coverage and capacity to support the rapid growth of M2M.

For over a decade, cellular networks have supported M2M devices alongside conventional subscribers so existing and future mobile spectrum licences support M2M as standard. The key to this success has been empowering mobile operators to use their spectrum for any service or technology as long as it does not cause interference (through the terms of their licences). Furthermore, the existing licensed mobile spectrum is sufficient to support wide area IoT demands, and can support rapid advanced cellular IoT rollouts which can capitalise on existing networks (e.g. NB-IoT). As long as TRAI continues its positive efforts to license sufficient additional amounts of spectrum for mobile use, it will be able to support the requirements of conventional mobile users and wide area M2M – as mobile operators can bid for more spectrum in line with growing demand. Any decision to mandate that all IoT services must use specific, dedicated licensed or unlicensed spectrum would damage market competition, struggle to meet all IoT use cases, and may lead to services which are not commercially viable.

Current 2G networks support low bandwidth M2M applications, such as vending machines, while existing 3G and 4G-LTE support high bandwidth M2M applications such as streaming video for applications like CCTV. However, the latest M2M cellular standards – in 3GPP Release 13 –- support all Low Power Wide Area (LPWA) M2M applications (in almost all licensed mobile bands). This includes smart metering, where coverage is often required very deep inside buildings and the battery life of access points can need to last many years. Future M2M cellular standards, including 5G, will augment these M2M features and use cases still further.

It should also be recognised that licensed spectrum is uniquely able to provide high quality of service guarantees over wide areas, as operators are not at risk of interference and can control usage levels as they have exclusive access to their spectrum bands. As a result licensed cellular IoT may be crucial for M2M services which require concrete assurance levels such as for security and medical applications amongst others. Contrastingly, unlicensed spectrum may not always suit wide-area M2M applications, especially those requiring higher quality of service levels. This is due to the fact that permitted power levels are generally low and interference risks over long distances are high - especially as the number of service providers and usage levels scale up Furthermore, they don't receive any protection and have to operate within stricter limits to not cause harmful interference to licensed services.

[1] GSMAi Intelligence (2016)

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?

As highlighted above, the licensed mobile bands are crucial for M2M. There is a good, and growing, amount of licensed mobile coverage (i.e. sub-1 GHz) and capacity (i.e. above 1GHz) spectrum to support the rapid growth of M2M –. In practice, most of the bands that will be used for cellular M2M will be sub 3 GHz and especially sub 1-GHz for Low Power Wide Area applications. Mobile services in these bands are well established throughout India in mature networks. 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).

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.

We would discourage TRAI from considering the 700 MHz centre gap for unlicensed M2M. 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 and the state revenues that can accrue from 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. Interference from any unlicensed part of the band into licensed services cannot be managed since location of the unlicensed devices and hence source of interference is not known.

Furthermore, it should be noted that most unlicensed bands are either globally or regionally harmonised so India is not advised to create its own 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. The band plan from the ECC report mentioned in TRAI paper overlaps with the APT band plan and therefore the reference to the same is irrelevant. Furthermore, it is important to note that this band plan is not dedicated exclusively to M2M (there is the option to use it for PPDR as well), and the GSMA is not currently aware of any countries that intend to license that portion of spectrum for exclusive M2M use. Also, given the band has extremely good propagation qualities there are also implications for cross border interference so needs to involve consultation with neighbouring countries.

Roaming

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

International roaming policy for machines should be based upon presently existing international roaming policy for voice and data services.

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?

Changes in Mobile network codes (MNC) numbering allocation policies should be carefully assessed in light of their implementation costs, and their technical and logistical complexities. The solution of allowing MSP to have MNC allocated presents security and fraud risk connected with private parties being assigned numbering resources, procuring and issuing SIM cards. It also may cause, depending on the network architecture used, increased signalling load on other national networks.

Technical solutions for changing connectivity provider are available today that eliminate the need to physically replace the SIM or to change MNC allocation policy. The use of a remote provisioning capability, such as that defined in GSMA Embedded SIM specifications, provides a solution that enables MSPs to select a connectivity provider at a later stage in the product lifecycle, i.e. when it reaches its customers, potentially in another country. It is therefore more efficient in addressing concerns regarding the ability to switch connectivity providers for IoT connected devices.

The GSMA Embedded SIM specifications were developed specifically for M2M market where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical.

Security and Privacy of Data

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.

Current measures for securing communication networks and the data that such networks carry are adequate for achieving security and privacy of M2M data in transit. With the implementation of these security measures, TSPs are resilient enough to withstand the risks and vulnerabilities arising from the external environment. Furthermore, TSPs are subjected to heavy penalties in the event of non-compliance with any security norms.

However, the security of data in transit does not ensure the ‘end to end’ security of M2M data, particularly for any data stored within the ‘endpoints’ of the service (the user device and service platform, which typically lie outside of the communication network). It is the responsibility of the entity providing a cellular M2M service to ensure adequate security measures are applied ‘end-to-end’ within their services and that the data within the endpoints of their service is adequately protected.

We suggest that TRAI should facilitate a regulatory framework, which mandates 3GPP standards for cellular M2M devices. Furthermore, certain M2M devices may at times behave in a rogue fashion leading to issues such as signalling storms. In such events, we recommend that the TSP should have the flexibility to bar such M2M devices without any prior notice and with no liabilities thereof.

The GSMA IoT Security Guidelines (already referenced in section 2.51 of the consultation) act as a reference set of security and privacy best practice guidelines that explain how an entity providing a cellular M2M service s can secure their service "end-to-end" from most cybersecurity attacks.

Recently the GSMA has created an IoT Security Self-Assessment[2] scheme based upon our IoT Security Guidelines. The scheme enables entities providing cellular M2M services to demonstrate that their products are aligned with the GSMA guidelines. By completing a self-assessment such entities can demonstrate the security and privacy measures they have taken to protect their products and services from cybersecurity risk, enhancing their reputation as trusted service provider.

GSMA believe that a self-assessment scheme, such as the one we have developed, is a good starting point to enhance M2M security because such scheme is flexible and cost efficient – and as such aligns well with the many innovative M2M business models that are likely to develop in this space.

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?

Consumer trust is critical for the development of M2M solutions and in order to realise the benefits of IoT for individuals and society in general. The main key to 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.

These are the kind of principles that are reflected in the OECD data privacy guidelines of 1980 and the omnibus data privacy laws that have been adopted in many countries. They allow policymakers and regulators to focus on the fairness of the use of the data rather than on a particular technology or sector while at the same time allowing innovation to take place.

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 in other countries. Adoption of the draft Privacy Law proposed many years ago and the points mentioned in 13 b) below would be a step in the right direction and would provide consumers with the necessary reassurance. In the meantime, the IT Act 2000 and other regulatory requirements provide sufficient safeguards to ensure the protection of consumer interests and data privacy of the consumer.

One thing that omnibus-style laws do not generally do is provide for is that private communications should be kept confidential. To the extent that this is not already provided as a constitutional or human right, it may be worth calling this out in legislation, but caution should be taken so as only to include content that is intended as a communication between two or more natural persons and to make sure that ecosystems can use access/process the content data for legitimate reasons such as fraud prevention and security.

[2] GSMA IoT security self-assessment scheme (2016) - http://www.gsma.com/connectedliving/iot-security-self-assessment/

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.

Regulation that affects network operators' handling of mobile traffic is not required. Any regulation that limits their flexibility to manage the end-to-end quality of service and provide consumers with a satisfactory experience is inherently counterproductive.

In considering the issue, regulators should recognise the differences between fixed and mobile networks, including technology differences and the impact of radio frequency characteristics.

Consumers should have the ability to choose between competing service providers on the basis of being able to compare performance differences in a transparent way. Mobile operators compete along many dimensions, such as pricing of service packages and devices, different calling and data plans, innovative applications and features, and network quality and coverage. The high degree of competition in the mobile market provides ample incentives to ensure customers enjoy the benefits of an open internet.

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

Mobile operators believe that customer confidence and trust can only be fully achieved when users feel their privacy is adequately protected, and that public confidence requires cooperation with law enforcement, the court system and state emergency services, but the government should ensure that legislation is technology neutral and that its rules are applied consistently to all players in the digital ecosystem, as is the case for obligations under industry-wide legislation such as the IT Act. Any additional demand on the MNOs alone, applied through operators' licenses, creates an additional cost and compliance burden without any additional benefit. The licensing framework places an unsustainable, disproportionate burden on mobile network operators. Despite the shift in the competitive landscape as a result of OTT communication services, the current approach still operates from an antiquated perspective of the market based on legacy industry structure. While operators are subject to a number of regulatory and public policy obligations, OTTs have greater regulatory flexibility. Where obligations are still necessary to achieve legitimate public policy objectives, TSP-specific obligations should be minimized and replaced with horizontal regulations that apply to all providers. This approach not only levels the playing field between market players but also is necessary for the achievement of those policy objectives.

Definitions

Internet of Things (IoT): Coordination of multiple vendor machines, devices and appliances connected to the Internet through multiple networks. Devices include everyday 'objects' such as smartphones, tablets and consumer electronics, such as machines, vehicles, monitors and sensors equipped to support M2M services.

IoT Connected Services: are those delivered via devices where the connectivity is provided by authenticating a SIM and where the service has at least one of the following characteristics:

- Open internet or open voice communications are not the primary purpose of the service; mobile connectivity is utilised to deliver value-added functionality
  OR
- Services that have a closed user group and service provider managed connectivity which excludes open internet or open voice access

Machine to Machine (M2M): Devices and appliances connected wirelessly or via IP. In most cases, communication takes place autonomously, with limited human intervention. M2M is an integral part of the IoT.

M2M service providers: from DOT: M2M arrangements involve communication of end device with predefined back end platform either directly or through some gateway. Most of M2M implementations involve end devices tightly coupled with the platform either directly or through gateway. M2M end device and platform collecting and analysing information from end device are controlled by some entity/organisation. That entity/ organisation it termed as "M2M Service Provider" (M2MSP).

From TRAI 2.4:

"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
- 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."

KYC= Know Your Customer

LPWA= Low Power Wide Area

MSISDN= Mobile Station International Subscriber Directory Number

MNC= Mobile Network Codes.

QoS =Quality of Service

Additional References:

- McKinsey - Unlocking the potential of the Internet of Things 2015) - http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
- GSMA- IOT Security Self- Assessment scheme (2016) http://www.gsma.com/connectedliving/iot-security-self-assessment/
- Connected farming in India (2015), https://www.vodafone.com/content/dam/sustainability/2015/pdf/connected-farmers.pdf
- Machina research forecasts (2016), https://machinaresearch.com/forecasts/main/
- McKinsey-Unlocking the potential of the Internet of Things (2015), DALY =Disability adjusted life-years; QALY: Quality adjusted life years, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
- The GSMA Connected Living Programme, http://www.gsma.com/connectedliving/. This website covers GSMA's IoT activities and is a reliable reference for up-to-date information
- The GSMA Connected Living Programme (2015), http://www.gsma.com/connectedliving/wp-content/uploads/2015/04/Realising-the-benefitsc-of-mobile-IoTsolutions-v4_7Apr2015.pdf
- The GSMA: "Mandatory Registration of Prepaid SIM cards: addressing challenges through best practice" (2016), http://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards
- The GSMA Intelligence (2016), https://www.gsmaintelligence.com/
- The GSMA IoT security self-assessment scheme (2016), http://www.gsma.com/connectedliving/iot-security-self-assessment/

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.