T · · Systems ·

Response to TRAI Consultation Paper on Regulatory Framework on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications

December 5th, 2016

by:

T-Systems ICT India Pvt. Ltd.

671 - 75, Ganeshkhind Road

Narveer Tanaji Wadi, Shivajinagar

Pune, Maharashtra 411005

Telephone: +91 20 3800 5000

E-Mail contact: laszlo.posset@t-systems.com

I. BACKGROUND

About T-Systems in India: T-Systems ICT India Pvt. Ltd. was set up as a subsidiary of T-Systems International GmbH, which is a group company of Deutsche Telekom (DT) delivering ICT services to DT's corporate customers worldwide.

In 2016, T-Systems ICT India established its two ''Point of Production" (POP) centers in Pune & Bangalore employing 100+ employees. These two POP's are poised to grow in next few years in India and become an important delivery centers with over 1.500 employees in next two years for providing ICT services, including IoT and M2M services too, to its global customers like Audi, BMW, Mercedes, Volkswagen, Shell, ThyssenKrupp and many others who are present on the Indian market too.

About Deutsche Telekom M2M services: DT is already serving multiple industry verticals with M2M services. Major verticals are Smart Cities (incl. Smart Metering, Smart Home, Smart Parking), Industrial Automation, Transport & Logistics, and Automotive. For its M2M customers, DT provides global, centrally managed M2M connectivity via its own networks in Europe and in the U.S. and in other countries via roaming partners. Supported connectivity types include 2G, 3G, 4G, FTTx, DSL, LPWA, PSTN, Zigbee and Ethernet. On top of this, DT runs its own Application Enabling Platform which provides, among other services, Device Management, Hosting, Event Processing, Identity Management, and Security. Based on these platform capabilities, DT also provides vertical solutions for the above mentioned focus industries via its subsidiary T-Systems International.

About Deutsche Telekom M2M services in India: M2M customers of DT have expressed the intention to rollout the service also to their devices in India. For instance, DT is already providing the connectivity solution for a German car manufacturer in more than 50 countries in Europe, Africa and Australia. On the basis of this connectivity solution, the car manufacturer provides a broad range of telematics services including status monitoring, real time traffic information, automatic emergency calls, and concierge services. For the car manufacturer, it is important that only one connectivity provider is acting as a general contractor for their global connectivity requirements, that they can include the same (e-)SIM in all of their cars, and that the service can be rolled out quickly in as many countries as possible. The solution that was deployed by DT can fulfill these requirements because it is based on permanent international roaming. For this exemplary customer, as for other current and future DT M2M customers, it is desirable that they can provide their M2M services in India on the same basis. It is in their interest that the new ecosystems which are developing around their M2M core services are also emerging in India. Just like DT, they consider India to be a potential key market for M2M services and M2M application development in the future.

II. ISSUE-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.

In the countries where DT offers its M2M services outside of its own network footprint, M2M connectivity is provided on the basis of international roaming. In our view, the frameworks for international roaming provided by GSMA are sufficient to ensure that regulatory requirements are being met also by global M2M solutions that are made available based on international roaming.

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

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

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

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

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

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

(a) If yes, what could be its possible implications?
(b) If no, what should be the ceiling tariffs for national roaming for M2M communication?

Q8. In case of M2M devices, should;

(a) roaming on permanent basis be allowed for foreign SIM/eUICC; or
(b) only domestic manufactured SIM/eUICC be allowed? and/or
(c) there be a timeline/lifecycle of foreign SIMs to be converted into Indian SIMs/eUICC?

(d) any other option is available?

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

Answer refers to (a):

Over the last months, DT was approached by a number of customers who asked if it was feasible to provide their M2M services also in India. These customers are usually operating their own M2M platforms and pursue the intention to roll out their services efficiently on a global scale. They have two major requirements regarding M2M connectivity:

1. They want DT to act as a general contractor that provides connectivity in every country they want to serve
2. They need to roll out their M2M services with a short time to market on a global scale
3. They want to connect their devices with the best available local connectivity.

Providing connectivity based on permanent roaming is the only option to fulfill these requirements, based on already existing international roaming agreements. To roll out these services based on local connectivity would require individual agreements with local telecommunication providers in every country. The necessary effort would reduce the roll out speed of M2M platforms and local M2M applications for these platforms in the countries that require local connectivity. On top of this, it would be impossible to provide access to the best available connectivity on each device (unless national roaming is allowed and enabled). However, DT is willing to consider the possibility of local carrier relationships in countries such as India if the incentives provided by the regulatory body are appropriately structured.

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

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

M2M devices that are equipped with permanently roaming SIM cards are already fulfilling the regulatory requirements that are laid out in the international roaming agreements. For instance, lawful interception is possible at the SGSN, just like in the case of international roaming by travelers.

Regarding KYC norms, we differentiate between devices where there is no individual owner (turbines or elevators, for instance), or where no service is attached that requires user registration. KYC is not possible in these cases.

However, some M2M services require end user registration at least during initial set-up, for instance most telematics services for connected cars. In these cases, KYC is possible at least regarding the initial user of the service, and the M2M Service Provider will run a database which matches device numbers (for instance, vehicle identification numbers), IMSIs and personal data. In the exemplary case of a car manufacturer, access to this database could be provided to Law Enforcement Authorities by a local representative via a secure web interface.

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?

To allocate MNCs to MSP does mean that a MSP becomes a TSP (MNO or VNO). TSPs with own MNC is a business model used today in many countries for M2M, e.g. in Europe. It also results in the need for the TSP to register accordingly. TSP is in charge of any regulatory requirements and he must negotiate roaming agreements on its own. But the MSP is still depending on MNO's roaming offers, but on a wholesale level instead of retail.

With allocating a separate MNC the separation of traffic is possible. With the separation the M2M specific setting of technical parameters would be possible but requires an own infrastructure, at least a core network (VNE). If the change of the SIM is required by e.g. a customer, this will also be supported if the TSP/MSP supports Subscription Management and has introduced the eUICC. But as of today the standardization is not finalized and only propieratary solutions from SIM manufactures are available. This results for the TSP in the need to set up a Subscription Management eco system which allow changes within this eco system.

Traffic separation could be done with operator resources (e.g. 232 03 18), with local resources (e.g. MCC 404 MNC 999) but also with ITU resources (e.g. Shared Country Code; MCC 901 MNC04). DT sees the so-called non-geo SIM (MCC 901) as a proper instrument to fulfill M2M/IOT needs. Separation of traffic is advantageous to be able to set specific technical parameters as well as for negotiation of roaming rates. Usage of a non-geo SIM compared to any other foreign SIM in India is just dependent on the roaming agreements in place for the respective resources. "National Roaming" would be possible for both options / resources. Given that a Global SIM does not have any home country, it roams everywhere and could make use of any roaming network in the world, providing "Best Coverage".

Nevertheless, introducing a new MNC does always mean to setup/update new roaming relationships which comes together with a slow time to market for significant roaming coverage for international M2M solutions. Of course, this does not apply if the SIM is only used nationally. But with M2M very often there is a need for "Best Coverage" with does mean that roaming is required.

DT believes that the currently used solution which is based on GSMA/ITU standards, is much more effective: the extra-territorial use of a numbering resource (normal E.212 MNC code / E.164 MSISDN and MCC 901 types) for M2M services in both directions. Indian regulators should allow the permanent use of E.212/E.164/MCC901 type numbering codes outside Indian territories as well as the use of foreign IMSI/MSISDN within Indian territory.

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.

Global M2M service providers operate M2M services in many countries worldwide while their platform for delivering the service in many countries is typically hosted in one country. Hosting a platform in every country where the services is provided would lead to a) inferior QoS as the interplay of many platforms cause issues in many aspects, for instance difficulties with synchronizing real time data and b) very high costs for the service providers which in most cases could not be justified.

Therefore in general M2M service providers should have the necessary flexibility to offer their services in India and thus driving the development of the local IoT economy while being allowed to host their IoT platforms outside of India. From our point of view this should especially apply to majority of consumer oriented services. The obligation to host or mirror M2M platforms in India should be strictly limited to services with highest potential impact on national security, for instance military services.

With regards to the question if it is necessary to release additional rules to ensure data and network security for M2M services, we agree with BEREC that in general there is no need for a specific M2M regulation. The measures undertaken today by European telecommunication providers with regards to network and data security are based on very high security standards and therefore are sufficient for most use cases that we observe today.

However, as specific use cases in many verticals are still in a phase of development today, specific needs for certain use cases in the future might be coming up. One example that we see today is smart grids/metering. For specific use cases in this vertical the German regulation authorities released tailored security guidelines.

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.

DT as a German company has to follow the existing German and European law and rules given by the German regulatory authority (BNetzA) which is part of the BEREC. This framework gives proper and sufficient measures to fulfil the interests of a “M2M Service” user who sometimes could also be a consumer. To protect the interests of a consumer we consider three parts to be important:

1) Access to end-user data: TSP provides M2M services to his customers. Mostly these TSPs are also operating a M2M connectivity platform for assigning eUICC and MSIDN to a SIM. The SIM are identified by a dedicated M2M IMSI range (for example 232 03 18x) and a dedicated MSISDN range (e.g. 43676 18x). The TSP should have no access to either end-user or machine identity information. The operations are based on IMSI, eUICC and MSISDN without mapping them to a specific machine or end-users. This number information should be treated by the TSP as strictly confidential and protected according to data protection laws.

2) M2M SIM administration: The administration of the SIM cards is done by the customer. Therefore the customer has access to TSP’s M2M connectivity platform. The TSP should not initiate any M2M end-user operations, including the ones involved in connecting or disconnecting M2M devices to the network. All these operations are processed automatically by TSP’s systems upon electronic trigger by customer.

3) Tracking of M2M devices: The TSP must not collect or store any location information that could be used for tracking of M2M devices. This information might be collected by the TSP strictly based on a legal request from a competent authority based on the existing law. We see the German Code of Criminal procedure and the Telecommunications Act (StPo, TKG) as a sufficient framework.

StPO.pdf   TKG.pdf

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.

As TRAI correctly recognized, M2M business models are very different from traditional operator business and the need for different types of SLA is there. DT sees currently three perspectives on quality-of-service:

Network perspective - Network Service Parameters: represents the quality that is offered internally by a service management team in the national as well as in the roaming case. This includes for example “incident resolving time” or “availability of service node”..

Network perspective – Technical Parameters: refers to the service quality that networks offer to applications or users. Network QoS parameters are latency or delay of packets, reliability of packet transmission etc.

User perspective: parameters describing the quality which is recognized by the user of the M2M service. User QoS parameters can be e.g. quality of the video from a surveillance camera, refresh period of sensor data or SMS delivery time.

DT is already on the way to address all this topics in different manners. Most urgently, the network service perspective has to be addressed. If the M2M service is only provided nationally the existing contracts (e.g internal OLA with infrastructure vendors) are covering all needed parameters. But there are a lot of M2M devices rolled out internationally and the current KPIs which are included in the roaming contracts are not sufficient. Therefore DT sees a need to extend the contractual base between TSP (MNO).

The Technical Parameters are also under discussion. Trying to match the technical QoS parameters of a M2M service with the current implementation in GSM/LTE networks (e.g., QCI settings) does not fit. There are use cases which need high-bandwidth and transmission priority and also on the other hand use cases with low-bandwidth and low priority. DT sees currently no way to implement proper solutions in a current mobile network environment and is therefore very active in defining the next generation of mobile communications (5G). This standard is explicitly addressing the needs of M2M quality (mMTC).

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

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

Regarding the required location of platforms, gateways or servers:

For the provision of the service on a global basis it is very important for our customers that they can use their existing platforms which are usually located in Europe. This is important to avoid latency times between multiple platforms, to provide the same quality of service in every country (based on the same comprehensive data sets) and to ensure economic viability of the service.

Equally for DT, connectivity management and application enablement platforms are located in Europe and are set up to serve customers globally. Mirroring or multiplying platforms poses significant difficulties regarding performance (latency issues) and security and adds complexity in the roll-out of updates and new features. In the more than 50 countries currently served by DT with M2M services, regulatory requirements can be fulfilled without the need to set up local infrastructure, and usually these requirements are already covered by roaming agreements. If there are any additional regulatory requirements (for instance for services that include B2C components like in-car WiFi hotspots) these can be fulfilled via local representatives and interfaces which can be accessed by these representatives.

II. SUMMARY OF DT's SUBMISSIONS

i. DT believes that the currently used solution, which is based on GSMA standards, is much more effective: the extra-territorial use of a numbering resource (normal E.212 MNC code / E.164 MSISDN and MCC 901 types) for M2M services in both directions. Indian regulators should allow the permanent use of E.212/E.164/MCC901 type numbering codes outside their territories as well as the use of foreign IMSI/MSISDN within their territory.

ii. In general M2M service providers should have the necessary flexibility to offer their services in India and thus driving the development of the local IoT economy while being allowed to host their IoT platforms outside of India. From our point of view this should especially apply to majority of consumer oriented services. The obligation to host or mirror M2M platforms in India should be strictly limited to services with highest potential impact on national security, for instance military services

iii. We look to the Authority to formulate a forward looking regulatory framework that is future fit and meets the requirements of a M2M World.

iv. We welcome and appreciate the consultative approach adopted by TRAI and recommend a conducive environment in which the benefits of the M2M can be availed in a commercially viable manner in compliance with a legal and regulatory framework which compliments its implementation.