

No.:206/TRAI/2024-25/ACTO

Dated: 19th August, 2024

Shri Akhilesh Kumar Trivedi
Advisor (Networks, Spectrum & Licensing)

Telecom Regulatory Authority of India

Tower F, NBCC World Trade Centre,

Nauroji Nagar,

New Delhi-110029

Ref: **ACTO's Response to TRAI's Consultation Paper dated June 24, 2024 on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs**

Dear Sir,

With reference to the *Consultation Paper on Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs* issued by Hon'ble Authority, Association of Competitive Telecom Operators (ACTO), is pleased to provide our comments.

We hope that our comments (enclosed as Annexure – I & II) will merit consideration of the Hon'ble Authority.

Thanking you,
Respectfully submitted

Yours sincerely,
for **Association of Competitive Telecom Operators**

Director

Encl: As above

Annexure-I

ACTO's Response on TRAI's Consultation Paper on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs

The Association of Competitive Telecom Operators (ACTO) appreciates TRAI for bringing the Consultation Paper on "the Issue Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs dated 24th June, 2024. During last eight years, TRAI had made several consultations on M2M and had made several recommendations. Many of the recommendations are also implemented.

In last few years, M2M services has been rolled out in several sectors but the space of deployment still lacking. The ability to proliferate and sustain the benefits delivered by M2M/IOT services and ensure that they contribute to the wider sustainable development is critical for any country as the growth also brings challenges and risks that need to be managed. It is through innovation and partnerships that the evolving M2M ecosystem can adapt effectively to the rapidly changing technological and social environment. Telecom infrastructure underpins the connectivity and data processing capacity required for M2M/ IoT.

Indeed, some M2M/ IoT applications may run with low speed, low-capacity connectivity, but others will require high-capacity broadband connections. Even in a scenario with M2M/ IoT applications requiring low capacity, the simultaneous use of numerous devices may require a high-capacity backhaul or backbone connection. In addition, the processing of big data generated by M2M/ IoT will require high bandwidth. Critical services in M2M/IOT applications require higher bandwidth, reliable connectivity (along with redundancy), device level protection and low latency for end-to-end connection.

All M2M services/ applications of a sector can therefore not be treated as critical but the specific service which has life risk and larger implications due to non-availability of service. Regulators of each sectors covering the M2M services need to define as critical service/ application instead one body to determine it for all. But a broad guideline by one body like TRAI will definitely help to the respective sectors.

Further, putting the requirement to bring all M2M devices under trusted Source/ Product framework will be a humongous task and further delay the uptake of M2M services in India. Moreover, the nature of changes in M2M services are quite frequent due to innovation of use cases and applications. In our view, the requirement of approval from NSCS shall not be applicable to M2M devices.

With respect to transfer of M2M SIM among M2M service providers, it is too early to decide the framework and we may need to wait for M2M market to get more mature but work in this regard may be started.

ACTO's response to the specific questions raised in the consultation paper:

Q1. Whether there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service? If yes, what should be the guiding framework? Please provide a detailed response with justifications.

ACTO's response:

In the past TRAI recommendations, M2M services and applications were differentiated based on its nature as critical and non-critical. We feel that there is a need for a broad guiding framework for defining a service rather than just two category as critical and non-critical. It is mainly because there are many different services across different verticals and industry/sectors. There will be many more in the near future. TRAI recommendation may define broad categories and respective Sectors/ Departments/ Ministries can further include the specific requirements on the top of the broad guiding framework from regulation perspective. In our view the M2M/ IOT services can be broadly categorised in the following ways:

A. Bottom end M2M/ IOT service:

Very large number of M2M services will fall under this category. The criteria for this category to cover large number of low-cost, less time sensitive, requirement of narrow-bandwidth devices that infrequently send or receive small volume of data. It is indeed a low-cost model.

B. Mid end M2M/IOT service:

Relatively large number of M2M services will also fall under this category. This category requires high bandwidth, lesser latency, moderately time sensitive and frequently send or receive significant volume of data including voice in case of emergency. It is a mid-cost model from business perspective.

C. Industrial grade M2M/IOT service:

This category of services will meet the requirement of the industrial applications like manufacturing, automation, transport, surveillance etc. This category requires very high bandwidth, very low latency, time sensitive, redundancy and always on to send or receive high volume of data including voice in case of emergency. In this type of applications, there are high financial and other related risks in case of non-availability or disruption of M2M service. It is a relatively high-cost model.

D. High end M2M/IOT service for critical applications/usage:

This category of M2M services require robust, resilient, reliable, redundant and secure network. For example, M2M applications in healthcare like remote surgery or a driverless car etc. These kinds of applications require high QoS, ultra reliability, very low latency, very high availability including some kind of accountability as it involves life risks and may cause substantial damage to customers. Here cost can be very high for these services due to the fact as it requires all the components of the networks, devices and applications need to step up in terms of latency and reliability. Not just network latency but also end to end latency is important factor. It has to ensure the availability and reliability to meet the agreed guaranteed bandwidth/connection.

Our suggestions:

Critical M2M/ IoT connectivity is for time-critical communication. It enables data delivery within desired latency bounds. Only specific applications within the sector be defined as critical M2M services. Considering that it is important to ensure availability of such critical services unhindered, it may be a good case to look at enabling provisions of seamless roaming onto other available telecom networks operating in the country.

Based on above, we suggest that TRAI to recommend a broad guidelines and respective Departments/ Ministries to define the critical service/ application along with the specific operational requirements which will be part of their regulatory domain.

Q2. Through the recommendation No. 5.1(g) of the TRAI's recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum. Whether this recommendation requires a review? Specifically, whether critical services in the M2M sector should be permitted to be provided by using unlicensed spectrum as well? Please provide a detailed response with justifications.

ACTO's response:

It is beyond any doubt that M2M will make extensive use of wireless communication in both licensed and unlicensed spectrum bands. It is important to consider that the spectrum used only for M2M services being sparingly used has a much longer expected life before it gets fully used than the spectrum used in traditional wireless communication as noticed in the past from 2G to 4G.

There is a need for review of earlier TRAI recommendation to use licensed spectrum for providing critical M2M services. As stated in our response to Q1, right definition of critical M2M service is more difficult as M2M services covers wide range across many verticals of many different sectors. All the sectors may not fall under licensed spectrum requirement category and it may cause overreach to other sectors. Exact definition of critical service may also change with time to time.

The assumption of ensuring QoS through licensed spectrum is over simplification of actual facts. QoS in M2M service will depend on many other factors for critical M2M services. The existing QoS requirement for licensed spectrum may not also match the requirement for critical M2M services. QoS for critical services need to be defined on a wholistic level as defining it just for connectivity part through spectrum will not be enough for the critical services. There is a need to define the level of quality for critical M2M services and it may not be the same as defined for the services under the licensed spectrum. Any technology, which complies with the SLA/ QoS framework laid down by the concerned ministry/ sector regulator and meets the regulatory requirements, should be permitted for the provision of critical M2M/ IoT services. TRAI may recommend DoT for license amendment to ensure the QoS requirement meant for critical M2M application specific requirement as mandated by different Govt departments/ regulators so as to prioritize the carriage of information on their network based on the critical nature of information.

Our suggestions:

We suggest that there should not be any mandate to provide critical M2M services only through the licensed telecom operator over licensed spectrum. The choice for selecting telecom operators/ ISPs for usage of licensed bandwidth should be left to the customers/ M2M service Providers/ respective regulators of sector for that specific M2M service. Instead, TRAI may recommend DOT for license amendment to ensure the QoS requirement meant for critical M2M application meets the specific requirement as mandated by different Govt departments/ regulators.

Q3. Whether there is a need to bring M2M devices under the Trusted Source/ Trusted Product framework? If yes, which of the following devices should be brought under the Trusted Source/ Trusted Product framework:

- (a) All M2M devices to be used in India; or**
- (b) All M2M devices to be used for critical IoT/ M2M services in India; or**
- (c) Any other (please specify)?**

Please provide a detailed response with justifications.

ACTO's response:

Mandate to use trusted products from trusted sources was introduced in June 2021 with the endeavour to make our telecom network more safer. Customer premises equipment /devices including routers are put in the network either by TSPs/ ISPs or by the end users. Approval from NSCS (trusted body) in case it is procured by TSPs/ ISPs but not if it is procured by end users. Thus, it is not effective towards the stated goal. Due to large availability of CPEs in the open market with lesser or competitive prices, end users preferred choice is to buy from open market rather than from TSPs/ISPs. Further, the pace at which advancement/ changes take place in the CPE devices is phenomenal and it is not practically feasible to have CPEs run past the lengthy process of TTC approval.

M2M/ IOT devices are quite similar to CPEs. Coverage of M2M/ IOT services will require huge numbers of different types devices as it will be used across many sectors/ verticals. It will be much larger as compare to CPEs in telecom. Putting the requirement to bring all M2M devices under trusted Source/ Product framework will be a humongous task and further delay the uptake of M2M services in India. Moreover, the nature of changes in M2M services are quite frequent due to innovation of use cases and applications.

There is a need to review the requirement for trusted product/source approval based on data after implementation and pre implementation period.

Our suggestions:

In our view, the requirement of approval from NSCS shall not be applicable to M2M devices.

Q4. Whether there is a need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs? If yes, -

- (a) What should be the salient features of such a framework?**
- (b) In which scenarios, the transfer of ownership of M2M SIMs should be permitted?**
- (c) What measures should be taken to avoid any misuse of this facility?**
- (d) What flexibility should be given to a new M2MSP for providing connectivity to the existing customers?**

Please provide a detailed response with justifications.

ACTO's response:

With respect to deployment perspective, M2M/IOT is still at nascent stage in India. It may be a regulatory requirement at latter stage and definitely have work in the future. At this stage, we are not sure how it is going to span out. Many factors will be involved like number of M2M service providers across different sectors, competition, quality of service, availability of service etc. We need to wait for the M2M market to get mature enough for this kind of regulatory framework.

Q5. Whether there are any other relevant issues relating to M2M/ IoT services sector which require to be addressed at this stage? Please provide a detailed response with justifications.

ACTO's response:

We would like to bring to your kind attention to the recently released TRAI Recommendations on Usage of Embedded SIM for Machine-to-Machine (M2M) Communications issued on 21st March 2024. In this regard, we would like to raise concerns regarding the specific recommendation pertaining to restrictions on International Roaming as stated in clause 2.20 of TRAI Recommendation:

*“Earlier, through the recommendation No.5.7(b) of the recommendations on ‘Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications’ dated 05.09.2017, TRAI had recommended that “[d]evices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP’s SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition based on the developments and requirements”. Based on a review of the said recommendation, the Authority recommends that all communication profiles on any M2M eSIM fitted in an imported device on international roaming in India should be **mandatorily converted/ reconfigured into communication profiles of Indian telecom service providers within a period of six months from the date of activation of international roaming in India on such M2M eSIM or on change of ownership of the device, whichever is earlier.**”*

In our considered view, the above specific TRAI recommendations places undue costs and burdens on consumers and providers who benefit from the global marketplace of M2M devices and the ease of use that permanent roaming facilitates. Restrictions on permanent roaming of M2M devices in India goes against the global norms and international best practices and would make India an island while increasing costs to consumers. A seamless flow of devices operating on a permanent roaming basis across the globe is critical to effective functioning of the M2M services given the inherently global nature of M2M services.

In this regard, we request TRAI to kindly take into consideration our request for a review of the TRAI recommendations to ensure M2M devices can operate in India on a permanent roaming basis to ensure the customer can utilise the service in a seamless and globally consistent manner. Any undue restrictions will create uncertainty, limits the ability to provide global connectivity and harmonization, and increase costs. Detailed letter sent to DoT on the issue is also enclosed as Annexure – II.
