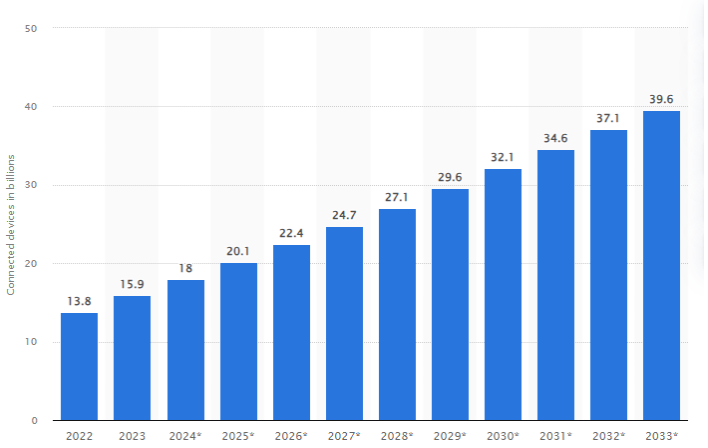
BIF Response to TRAI CP on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs

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.

BIF Response

No, there is no need of dividing M2M/IoT services into critical and Non-critical category. IoT/M2M technology has been in use in the industrial domain for many years where sensors and automated manufacturing processes have made the industrial sector efficient. M2M technology was first adopted in manufacturing and industrial settings, where other technologies, such as SCADA and remote monitoring, helped remotely manage and control data from equipment. As, the use of those devices and applications were limited to the premises of the respective industries, the need for securing such devices and applications were not so crucial. However, for the past few years IoT/M2M technologies have started shaping the way of life for citizens across the globe. Today, IoT/M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety & Surveillance, Health care, Agriculture, Smart homes and Smart cities etc.

As per statista 32.1 billion devices are going to there in the world by 2030[1].



[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Such a huge volume of devices do pose security concern and such a concern is primarily from the point of view of identification of the device IoT devices also classified as gateway devices and constraint devices.

a) The **gateway**-like devices use powerful processors, extendable memories and no constraints on power source. They can route data to the cloud servers or aggregate/store data to deal with network latencies. Typically, they run Linux operating system with application containers and provision for remote management.

b) The **constrained devices** are end nodes with sensors/actuators that can handle a specific application purpose. They are usually connected to gateway-like devices, low power lossy network, and in-turn communicates with the IoT cloud platforms. Typically, they communicate via low power wireless protocols like BLE, 802.15.4 (6LoWPAN, Zigbee, Thread, Wireless HART etc.), LPWAN etc. and mostly battery powered with low data rate.

There is no global example for classification of the IoT devices which is based on criticality of use case. However, there are global examples for classifications based on technical parameters.

We agree to view of DoT on criticality of services. View of DoT on this is as under:

"criticality in any sector may be use-case driven and the same may not be made applicable for the entire domain/ sector. The criticality of M2M services in any domain/ sector may be decided on the market requirement by concerned ministries on their own. Further, the SLA/ QOS framework along-with detailed regulatory requirement for the same may also be defined by respective concerned ministries/ regulatory bodies for different use cases (which are identified as critical) and implementing technologies may comply with the same"

Keeping above in view classification of M2M/IoT services on the basis of use case into critical and non-critical services is not recommended.

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.

BIF Response

There is need to review recommendations no. 5.1(g) of the TRAI recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017.

Despite the fact that there will be huge number of IoT devices installed across the globe and there has been concerns about the security of the network. TEC has done a lot of work in this direction and came out with technical reports titled "Framework of National Trust Centre for M2M/IoT Devices and Applications" and "Security by Design for IoT Device Manufacturers" in March 2022 and March 2023 respectively.

We echo view of Department of telecommunication expressed vide letter number 4-31/M2Mriticalservices/2019-NT dated 1st Jan, 2024 placed as annexure1 in the consultation paper. Para 2 (IV) of the letter states following:

"Critical M2M services may require robust, resilient, reliable, redundant and secure network. However, with the ever-growing interconnectivity of devices in the Internet of Things (IoT) and Machine-to-Machine (M2M) domains, it has now become crucial to ensure the security and trust worthiness of these devices. Therefore, bringing M2M/ IoT devices under the Trusted Source Trusted Product regulation, specifically mandating the procurement of M2M/ IoT devices for Critical Infrastructure Sectors, as defined in the National Critical Information Infrastructure Protection Centre (NCIIPC) regulations can significantly mitigate the threat landscape and enhance the security posture of critical infrastructure sectors rather than merely mandating provision of these services by connectivity providers using licensed spectrum."

From the above it is clear that the Trusted Source and Trusted Product regulations significantly mitigate the threat landscape of the M2M/IoT devices. Further, to this the report of TEC on "Framework of National Trust Centre for M2M/IoT Devices and Applications" clearly identified two key

areas namely Device identity and end to end security framework for making the M2M network secure.

To secure IoT/M2M, each connected device needs a unique identification – even before it has an IP address. Therefore, it is required to establish the root-of-trust for the device's lifecycle and should be an initial security requirement. Implementation of IoT devices for unique identification as well as authentication should be only known to the device and IoT platform.

End-to-end encryption allows all traffic from a source to a destination to be fully encrypted and authenticated, so that if someone captures that traffic, they cannot read the inside information.

As per reports WiFi and Bluetooth provides connectivity to 31% and 27% of the IoT devices in US[2]. Under the SLNP programme in India, over 1.03 crore smart LED streetlights have been installed till date, enabling an estimated energy savings of 6.97 billion kWh per year with an avoided peak demand of 1,161 MW and an estimated greenhouse gas (GHG) emission reduction of 4.80 million tonnes of CO2 annually. The smart LED street light ecosystem is largely based on Zigbee.

IGL uses LoRa based automatic meter reading (AMR) systems for collection of meter reading.

Use of technology must be left on to the market forces and innovators. Enforcing the provision of critical services through Licensed bands only by Licensed TSPs may hamper the growth of the market as well as market driven R&D /startups/ smaller companies.

Again, cellular network finds it difficult to penetrate the walls as the higher frequencies are being used with addition of each G in the cellular technology. Therefore, for smart devices installed in basements and inside the houses it is difficult to connect to cellular network even for devices with higher receiver sensitivity.

Even in the hospital for remote surgeries or remote operations of machines require more stable and robust network which is possible through WiFi as the customer may have bandwidths from multiple sources for redundancy, robustness and reliability.

[2] https://iot-analytics.com/number-connected-iot-devices/

Operational cost apart from upfront cost of devices is also a critical factor in the choice of technologies. And hence market forces shall adopt the technologies based on their own requirements.

IoT devices need stable connectivity for which innovators are using Non-cellular technologies like, 6LoWPAN, Zigbee, Thread, Wireless HART etc. Mandating use of licensed spectrum based connectivity 20 M2M domain use cases would be detrimental to not only existing IoT ecosystem but also innovation in this sector. Therefore, use of technology must be left to market forces and mandating use of unlicensed frequencies for connecting IoT devices or services is detrimental to the growth and innovation of this vital domain.

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.

BIF Response

As stated in the response of the question 1 we do not recommend classification of M2M/IoT services into critical or non-critical ie based on use case, therefore, we recommend that "Trusted source and trusted product" frame work must be adopted for all the M2M devices to be used in India. The justifications for this are submitted in response to question 2.

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 saliant 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.

BIF Response

M2M SIMs are owned by M2MSP only but there are many cases wherein either the M2MSP stops its services due to financial constraints or some other reasons or get acquired by other entity.

Regulations of non-transfer of M2M SIMs is detrimental to product innovation and monetization and continuity of services to the customers. In case M2MSP stops services then existing customer has no choice except to close the service or throw the device and buy new device.

Further, such a regulation is prompting innovators to use connectivity solutions other than SIM based solution.

Therefore, in case of closure or merger or buyout of the M2M SP the change in ownership of SIMs must be allowed. However, standard KYC rules must be followed for new entity in whose name the M2M SIMs are to be transferred to avoid misuse. Even the customers may be allowed to choose M2MSP in case existing M2MSP is not giving services or closed its shop. Under such circumstances based on consent of both customer and new M2MSP ownership of SIM may be transferred to new M2MSP. New M2MSP must give undertaking for taking over all responsibilities of M2M SP.

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.

BIF Response

This pertains 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 below:

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 cost burden on the consumers and providers who benefit from the global marketplace of M2M devices and the ease of use that permanent roaming facilitates permit. 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 imposing unnecessary additional costs to consumers. A seamless flow of devices operating on a permanent roaming basis across the globe is critical for the effective functioning of the M2M services, given the inherently global nature of M2M services.

In this regard the Authority is kindly requested for a review of the TRAI recommendations to ensure that M2M devices can operate in India on a permanent roaming basis or at least for a period of 3 years as was recommended by TRAI in its earlier recommendations on M2M in 2017, to ensure the customer can utilise the service in a seamless and globally consistent manner and also help to foster innovation, and scalability of IoT/M2M. In view of this, **we request that international roaming for M2M devices should continue without any restrictions, in line with well adopted global best practices**

Any undue restrictions will create uncertainty and limit the ability to provide global connectivity and harmonization, and thereby increase cost to consumers. A detailed rationale with suggestions on the same is attached herewith.

****