ITU-APT Foundation of India (IAFI)

Comments on the

TRAI Consultation Paper

Regarding Issues Related to Critical Services in the M2M Sector,

and Transfer of Ownership of M2M SIMs

IAFI Response No. IAFI/TRAI/20240722 dated 22nd July 2024

About IAFI

The ITU-APT Foundation of India (IAFI) is a registered non-profit and non-political foundation registered under the Cooperative Societies Act of India. IAFI has been recognized by the International Telecommunication Union (ITU) as an international/ regional Telecommunications organization and has been granted the sector Membership of the ITU Radio Communications Bureau (ITU-R), ITU Development Bureau (ITU-D) and ITU Telecommunication Standardization Bureau (ITU-T). IAFI is also an affiliate member of the APT. IAFI has been working for the last 21 years to encourage the involvement of professionals, corporate, public/private sector industries, R&D organizations, academic institutions, and other agencies in the activities of the ITU and APT. IAFI has submitted more than 100 contributions to Various ITU and APT committees during last two years and have physically participated in all major ITU and APT conferences and meetings. IAFI also organises various national and international events. The two Flagship annual events of IAFI are ISMC (India Spectrum Management Conference) and ISPC (India Space Policy Conference). IN addition, IAFI also organises 5-6 preparatory meetings for each World Radio Conference.

For more details regarding IAFI, please visit https://www.iafi.in/

Background regarding TRAI consultation of Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs:

In May 2015, DoT issued the National Telecom M2M Roadmap, defining IoT as a connected network of embedded devices capable of M2M communication without human intervention.

In May 2018, DoT released the National Digital Communication Policy-201818 (NDCP-2018), which outlined strategies for M2M growth, including: (a) promoting new technologies like M2M, 5G, and AI, and (b) streamlining licensing and security frameworks.

In Sept, 2017 TRAI sent its recommendations to DoT on 'Spectrum, Roaming and QoS for Machine-to-Machine (M2M) Communications. One of the recommendations of TRAI was with respect to identification of Critical Services in M2M sector - "*Government, through DoT, should identify critical services in M2M sector and these services should be mandated to be provided only by connectivity providers using licensed spectrum".*

Considering the specific and critical needs of such services and taking into consideration of evolving technologies, and to have a wider understanding of sectorial requirements of critical M2M applications, an Inter-Ministerial Working Group (IMWG) was constituted in Nov. 19 to deliberate on all issues concerning critical M2M services, which submitted its report in March 21. The IMWG recommended a list of 20 services to be classified as critical along with broad regulatory requirements for critical services.

IMWG recommendations were forwarded to stakeholder and M2M services providers for comments. Some comments were received from stakeholders regarding critical services by M2M and transfer of M2M SIM.

In January, 2022, DoT introduced a separate authorization and registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services under Unified License.

In October 2023, TEC provided a technical definition of M2M, describing it as technologies enabling communication between wired and wireless systems and devices.

For further clarity on TRAI recommendations of Sept, 2017, DoT vide letter dated 01-01-2024 requested TRAI to provide recommendations on:-

i. Identification of Critical Services in the M2M Sector
ii. Transfer of Ownership of M2M SIM

TRAI vide letter dated 12.01.2024 requested the DoT to provide clarification, whether the list of 20 services, identified as critical by the IMWG, has been approved by DoT. In response, the DoT informed, inter-alia, that "the list of 20 services, identified by the Inter-Ministerial Working Group (IMWG), doesn't have the approval of DoT".

So, the Telecom Regulatory Authority of India (TRAI) released a consultation paper to solicit comments of stakeholders on specific issues related to critical services in the M2M sector and the transfer of ownership of M2M SIMs.

IAFI has thoroughly examined the Consultation Paper and after due consultation with our industry partners, IAFI submits the following comments:

Q-1. 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.

Answer:

IAFI is of the view that there is a strong need to identify critical M2M/IoT services, as directly impact public safety, national security, and essential infrastructure. It is evident that M2M/IoT services are being used in Smart grids for power distribution, remote surgery systems, autonomous vehicles and many industrial control systems used in critical infrastructure. Any malfunctioning of these services may lead to devastating consequences. So, clearly defining the M2M/IoT services as critical will help the following.

1. A clear definition may help establishing accountability of the service providers and device manufacturers. Such framework can ensure implementation of appropriate security measures and contingency plans to minimize disruptions and vulnerabilities.
2. A standardized framework can promote consistency in security protocols, data formats, and communication standards. It will foster interoperability between different M2M/IoT systems, making them more adaptable and easier to integrate.
3. Defining critical M2M/IoT services allows for targeted risk assessments and mitigation strategies. Resources can be allocated effectively to prioritize security for the most impactful applications.

Following points should be considered while developing the guiding framework. The framework should be comprehensive and must consider the following factors.

1. Services vital to public health, emergency response, and national security should be classified as critical.
2. Services where disruption could cause significant economic or societal damage fall under critical category. (e.g., smart grids, industrial automation)
3. Services handling sensitive data like medical records, financial information, or critical infrastructure control systems require high levels of protection and would be considered critical.
4. As the risk profile may vary depending on the sector, industry regulators can collaborate to establish a framework with clear definitions, compliance requirements, and potential penalties for non-compliance.
5. While developing the framework, industry experts, government agencies, consumer protection groups, and security professionals etc must be involved, to ensure a comprehensive and balanced approach.

Therefore, IAFI is of the view that broad guiding framework for defining critical M2M/IoT services is essential for mitigating risks, ensuring robust security measures, and fostering public trust in the rapidly expanding field. By establishing clear definitions and promoting collaborative development, safe and reliable operation of critical infrastructure and applications can be ensured.

Q-2. **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.

Answer:

Yes, in view of the enhancement in wireless technologies, critical services in the M2M sector should also be permitted to be provided by using unlicensed spectrum.

Therefore, existing TRAI recommendation regarding critical services in the Machine-to-Machine (M2M) sector to be provided by connectivity providers using licensed spectrum only, should be reviewed and revised due to advancements in technology, present regulatory frameworks, and market dynamics. Following point should be considered while reviewing the existing framework.

1. Reliability and Quality of Service (QoS) – Due to technological developments and availability of additional unlicensed spectrum, both licensed and unlicensed spectrum offer a matching levels of reliability and QoS. Critical M2M services, such as those used in healthcare, emergency services, and industrial automation, require uninterrupted and highly reliable communications can also be permitted on un-licensed spectrum.

2. Security – Enhancements in unlicensed technologies offers similar security controls, essential for critical M2M services handling sensitive data. Both licensed and unlicensed spectrum offer the same level of risk of unauthorized access and security breaches. Critical services do need robust security measures to prevent data theft, hacking, and other cyber threats and these can be implemented irrespective of the type of spectrum.

3. Technological Advancements - The technology landscape has evolved since TRAI submitted its recommendations in 2017, with significant advancements in both licensed and unlicensed spectrum technologies. Technologies used to connect IoT uses Low Power Wide Area Networks (LPWANs) like LoRaWAN and Sigfox operate in the unlicensed spectrum and have been successfully deployed in various M2M applications. However, their suitability for critical services still needs thorough evaluation, particularly concerning reliability and security.

4. Market Dynamics and Innovation -Allowing critical M2M services on unlicensed spectrum could foster innovation and reduce costs. It could lower entry barriers for new players and encourage the development of new technologies and business models. However, this must be balanced against the potential risks to reliability and security.

5. International Practices – exploring international practices can provide valuable insights. Some countries permit critical M2M services on unlicensed spectrum with specific regulations and safeguards in place. Understanding how these frameworks operate and their outcomes can inform whether a similar approach could be viable in India.

6. Regulatory Flexibility - A flexible regulatory approach could be considered, where critical services are allowed on unlicensed spectrum under strict conditions and regular monitoring. This could include requirements for enhanced security protocols, regular audits, and mechanisms to mitigate interference.

While there are a few arguments for maintaining the use of licensed spectrum for critical M2M services, given the technological advancements and potential benefits, it may be

prudent to modify this recommendation, taking into account the current capabilities of unlicensed spectrum technologies, examining international best practices, and consider implementing strict regulations and safeguards, if unlicensed spectrum is to be permitted for critical services. Such a balanced approach could leverage the benefits of both licensed and unlicensed spectrums while ensuring the reliability, security, and quality of critical M2M services.

Q-3. **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**.

Answer:

The need to bring Machine-to-Machine (M2M) devices under the Trusted Source/Trusted Product framework is crucial, particularly considering the increasing integration of these devices in critical infrastructure and services. Ensuring the security and reliability of M2M devices is essential to prevent potential risks associated with cyber threats, data breaches, and unauthorized access. Advantages for bringing M2M Devices Under the Trusted Source/Trusted Product Framework are"

1. Security**:** M2M devices often handle sensitive data and perform critical functions. Ensuring that these devices come from trusted sources can mitigate risks associated with compromised hardware or software, reducing vulnerabilities to cyber-attacks.
2. Reliability: Trusted devices are more likely to adhere to quality standards, ensuring consistent performance and reliability. This is especially important for critical services where device failure can have severe consequences.
3. Regulatory Compliance: A trusted framework can ensure that M2M devices comply with national and international regulations and standards, promoting a safer and more standardized technological environment.
4. Data Integrity: Ensuring that M2M devices are from trusted sources helps maintain the integrity of data transmitted and received by these devices, which is crucial for decision-making processes in critical services.

Therefore, M2M Devices to be Used for Critical IoT/M2M Services in India should be brought under the Trusted Source/Trusted Product Framework, considering the security of the critical services, used in the most sensitive and vital parts of the infrastructure.

Flexibility should be allowed for M2M Devices to be Used for Non-critical IoT/M2M Services, considering emerging threats and technologies, as it balances the need for security with the practical considerations of cost and complexity.

Further, the most balanced and effective approach would be to bring all M2M devices to be used for IoT/M2M services in India under the Trusted Source/Trusted Product framework. This ensures that the most sensitive and essential devices are secured while allowing for a more manageable implementation process. However, this framework should remain

flexible/adaptable, allowing for expansion to other devices as needed based on ongoing risk assessments and technological advancements.

Q-4. **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.**

Answer:

Establishing an automated and hassle-free regulatory framework for the transfer of ownership of M2M SIMs among Machine-to-Machine Service Providers (M2M SPs) is essential to ensure a seamless, secure, and efficient transition, while safeguarding against potential misuse. Here are the detailed responses with justifications for each aspect:

(a) Salient Features of Such a Framework:

1. Clear Definition and Scope
   i. Clear Definition and Scope - Definition of M2M SIMs, clearly define what constitutes M2M SIMs to avoid ambiguity.
   ii. Scope of Transfer - Specify the scenarios and types of transfers covered under the framework.
2. Authorization and Consent
   i. Authorization Procedures - Outline the process for obtaining authorization from regulatory bodies before transferring ownership.
   ii. Consent Requirements - Ensure that both the current and new M2MSPs, as well as the end users, provide explicit consent for the transfer.
3. Transparency and Documentation
   i. Documentation - Maintain comprehensive records of the transfer process, including agreements, authorizations, and consents.
   ii. Transparency - Implement measures to ensure transparency throughout the transfer process, including notifying all stakeholders.
4. Security and Compliance
   i. Security Measures -Establish security protocols to protect data during and after the transfer.
   ii. Compliance - Ensure that the transfer complies with relevant laws, regulations, and industry standards.
5. Customer Protection
   i. Customer Notification - Require notification to customers about the transfer and any potential changes in service terms or conditions.
   ii. Dispute Resolution - Establish mechanisms for addressing and resolving any disputes or issues arising from the transfer.

(b) Scenarios Where Transfer of Ownership of M2M SIMs Should Be Permitted:

Transfer of ownership should be permitted in all cases as and when requested, with or without reason.

Following are some examples of where such transfer may be requested. However this is not an exhaustive list and is only for examples:

1. Business Acquisitions and Mergers

   When one company acquires another, transferring M2M SIM ownership ensures continuity of service for existing customers.

2. Service Provider Exits

   If an M2MSP decides to exit the market, transferring ownership allows another provider to take over the services without disrupting customer connectivity.

3. Customer Request

   Customers may request a transfer to a different M2MSP for better service, pricing, or other reasons. This should be facilitated to maintain customer satisfaction.

4. Network Optimization

   Transferring SIMs for network optimization or better resource management can enhance service quality and efficiency.

(c) Measures to Avoid Misuse of This Facility:

1. Strict Verification Processes:
   i. Implement strict identity verification procedures for both M2M-SPs involved in the transfer.
   ii. Fraudulent transfers should be rejected
2. Security Protocols:
   i. Data Protection**:** Enforce stringent data protection measures during the transfer process to prevent unauthorized access and data breaches.
   ii. Transaction Monitoring: Implement real-time monitoring of transfer transactions to detect any suspicious activity.
3. Penalties and Enforcement:
   i. Establish and enforce penalties for any misuse or fraudulent activities related to the transfer of M2M SIMs.
   ii. Provide the authority to revoke the transfer rights of M2MSPs found violating regulations.

(d) Flexibility for a New M2M-SPs for Providing Connectivity to Existing Customers:

1. Grace Period for Transition:
   i. Provide a grace period during which the new M2M-SP can smoothly transition the services without disruption to customers.
   ii. The duration should be sufficient to complete technical integrations and customer communications.
2. Interoperability Standards:

i. Ensure that the new M2M-SP's network and services are interoperable with the existing devices and systems to prevent service interruptions.
ii. Mandate compliance with interoperability standards as part of the transfer process.

3. Customer Retention Programs:
   i. Allow the new M2M-SP to offer incentives or special programs to retain existing customers and ensure a smooth transition.
   ii. These programs should be regulated to prevent anti-competitive practices.
4. Technical Support:
   i. Provide technical support to both customers and the new M2M-SP during the transition period to resolve any issues quickly.
   ii. Ensure that adequate resources are allocated for technical support throughout the transition.

By implementing these measures, the regulatory framework can effectively manage the transfer of M2M SIM ownership, ensuring security, reliability, and customer satisfaction.

Q-5. **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.**

Answer:

In addition to the regulatory issues already discussed, there are several other relevant issues relating to the Machine-to-Machine (M2M) and Internet of Things (IoT) services sector that require attention. These issues encompass regulatory, technical, and market considerations that are critical for the sustainable growth and security of the M2M/IoT ecosystem. Here are the key issues and justifications for addressing them:

1. Data Privacy and Security:

With the proliferation of M2M and IoT devices, vast amounts of data are being generated, transmitted, and stored. This data often includes sensitive personal information and critical operational data. Robust data privacy must be ensured and security measures are crucial to protect against unauthorized access, data breaches, and cyber-attacks. Data privacy concerns will helps in complying with national and international data protection regulations.

IAFI suggest for encryption of data both at rest and in transit and strict access control measures to ensure that only authorized personnel can access sensitive data. In addition, regular security audits and vulnerability assessments must be conducted.

2. Standardization and Interoperability

The lack of standardized protocols and interoperability between different M2M and IoT devices and platforms can lead to fragmented systems, hindering seamless communication and integration. Standardization promotes efficient integration and operation of diverse devices and systems. It should be ensured that the M2M/IoT ecosystem can scale effectively without compatibility issues. Similarly, to encourages innovation, a clear framework for developers and manufacturers should be provided.

IAFI suggest that the adoption of international standards such as those from ISO, IEC, and ITU should be encouraged and interoperability testing facilities and certification programs should be established.

3. Spectrum Allocation and Management

The growing number of M2M and IoT devices increases the demand for spectrum. Efficient spectrum allocation and management are essential to avoid interference and ensure reliable connectivity. Proper spectrum management is very much required to ensure optimal network performance and prevents congestion. Future spectrum need should be anticipated and spectrum should be allocated accordingly, to accommodate growing number of devices.

IAFI suggest that additional unlicensed spectrum should be allocated, particularly in 900 MHz, 5925-6425 MHz and V band.

4. Regulatory and Policy Framework

A comprehensive and adaptable regulatory framework is necessary to address the dynamic and rapidly evolving nature of the M2M/IoT sector. It should be ensured that the regulations are not overly restrictive, allowing room for innovation and growth. Similarly, regulations should be updated time to time, to keep the pace with technological advancements.

5. Environmental Impact and Sustainability

The large-scale deployment of M2M and IoT devices can have significant environmental impacts, including electronic waste and energy consumption, so environmental eco-friendly sustainable practices in the M2M/IoT sector should be adopted. Companies may be encouraged to adopt green practices and reduce their environmental footprint.

IAFI suggest to promote the development and use of eco-friendly and energy-efficient devices and implement programs for the recycling and proper disposal of IoT devices.
