Telecom Regulatory Authority of India

Consultation Paper on

the Issues Related to Critical Services in the M2M Sector,

and Transfer of Ownership of M2M SIMs

New Delhi, India

24.06.2024

Tower F, NBCC World Trade Centre, Nauroji Nagar, New Delhi-110029

Written comments on the Consultation Paper are invited from stakeholders by 22nd July 2024 and counter-comments by 5th August 2024. The comments and counter-comments may be sent, preferably in electronic form, to Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), TRAI on the email ID advmn@trai.gov.in. Comments and counter-comments received from stakeholders will be posted on the TRAI's website (www.trai.gov.in).

For any clarification/ information, Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), TRAI, may be contacted at Telephone No. +91-11-20907758.

CONTENTS

CHAPTER I: INTRODUCTION

A.   IoT and M2M

1.1   In September 1991, the Scientific American published an article named 'The Computer for the 21st Century' by Mark Weiser. In the Article, Mark Weiser developed a seminal vision of the future technological <u>ubiquity</u> – one in which the increasing "availability" of processing power would be accompanied by its decreasing "visibility". Mark Weiser observed that *"[t]he most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."* He added, *"only when things disappear in this way are we freed to use them without thinking and so focus beyond them on new goals."*

1.2   In November 2005, the International Telecommunication Union (ITU)[1] published a report on 'Internet of Things'[2]. In the report, ITU observed that *"[e]arly forms of <u>ubiquitous</u> information and communication networks are evident in the widespread use of mobile phones… These little gadgets have become an integral and intimate part of everyday life for many millions of people... Today, developments are rapidly underway to take this phenomenon an important step further, by embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communications between people and things, and between things themselves. A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, anyplace connectivity for anyone, we will now have connectivity for anything… Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things."*

---

[1] ITU is the United Nations specialized agency for information and communication technologies (ICTs).
Source: https://www.itu.int/en/about/Pages/default.aspx#qsc.tab=0
[2]Source: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

1.3   In June 2012, the ITU released its recommendation on 'Overview of the Internet of Things'[3]. In the recommendation, the ITU defined 'Internet of things (IoT)' as

"[a] global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". The recommendation provided the technical overview of IoT as below:
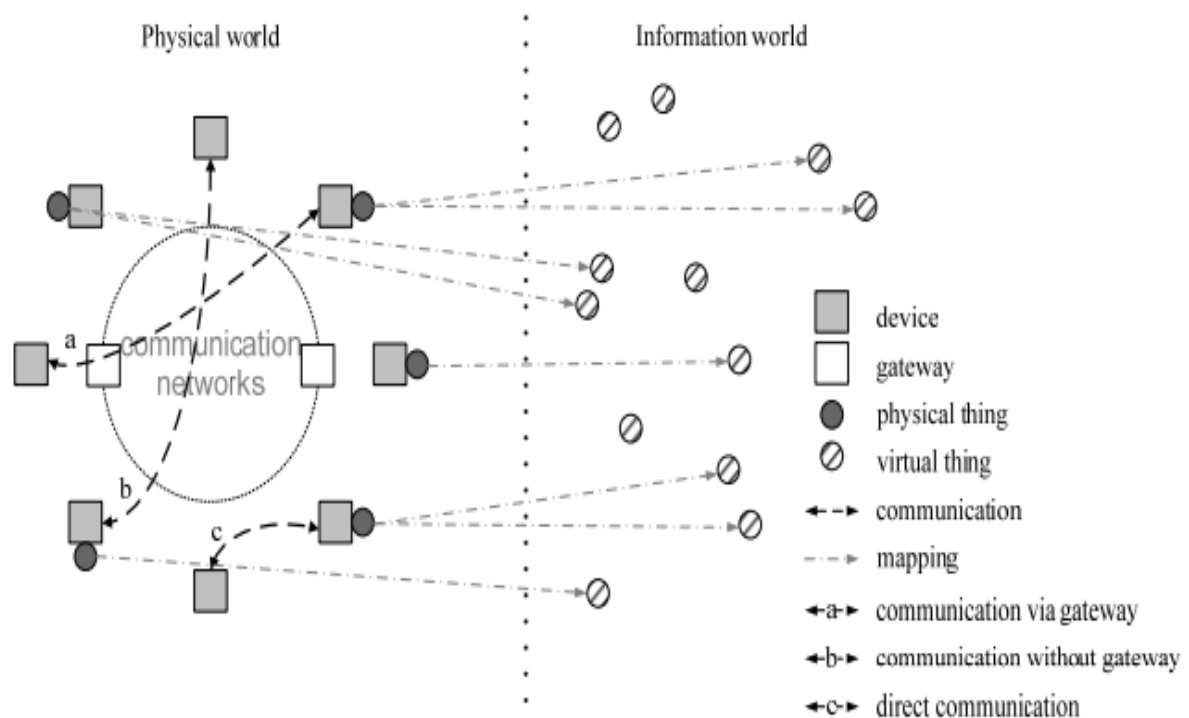
Figure 1.1: Technical Overview of IoT[4]

1.4   Notably, in the recommendation, the ITU provided definitions of the terms 'device' and thing' as below:

"device: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing."

---

[3] Source: ITU's recommendation ITU-T Y.2060 (06/2012), accessible at URL: Y.2060 : Overview of the Internet of things (itu.int)
[4] ibid

"thing: With regard to the Internet of things, this is an object of the physical world (physical thing) or the information world (virtual things), which is capable of being identified and integrated into communication networks".[5]

1.5   In the recommendation, the ITU depicted the relations between devices and physical things as below:
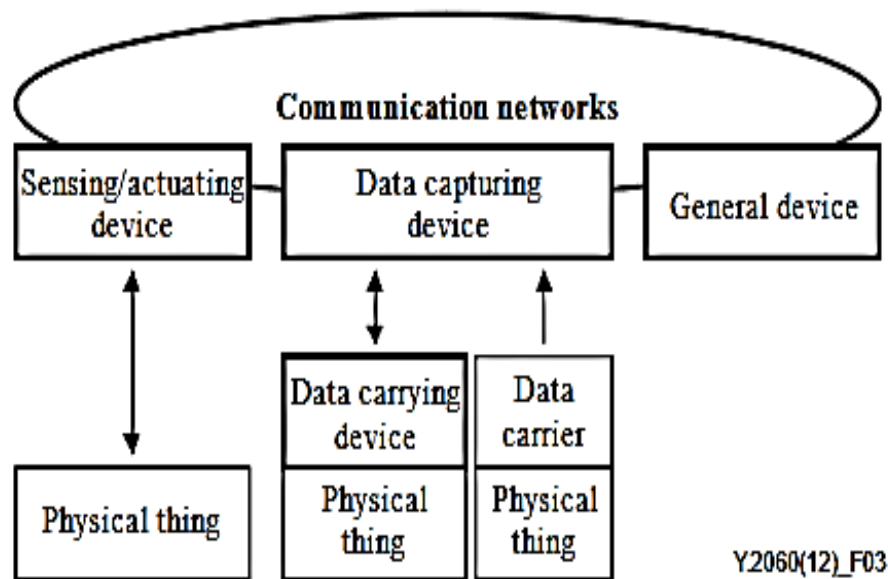

Figure 1.2: Types of devices and their relationship with physical things[6]

1.6   In the year 2015, ITU in its report named 'Measuring the Information Society Report'[7] depicted the path to IoT from people-to-people to machine-to-machine (M2M) communication as below:

---

[5] With respect to physical things and virtual things, ITU, through the recommendation ITU-T Y.2060 (06/2012), stated as below: *"Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment. Virtual things exist in the information world and are capable of being stored, processed and accessed. Example of virtual tings include multimedia content and application software."*

[6] Source: ITU's recommendation ITU-T Y.2060 (06/2012). In the recommendation, ITU observed that *"[t]he devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks. … The communication networks transfer data captured by devices to applications and other devices, as well as instructions from applications to devices. The communication networks provide capabilities for reliable and efficient data transfer."*

[7] Source: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf
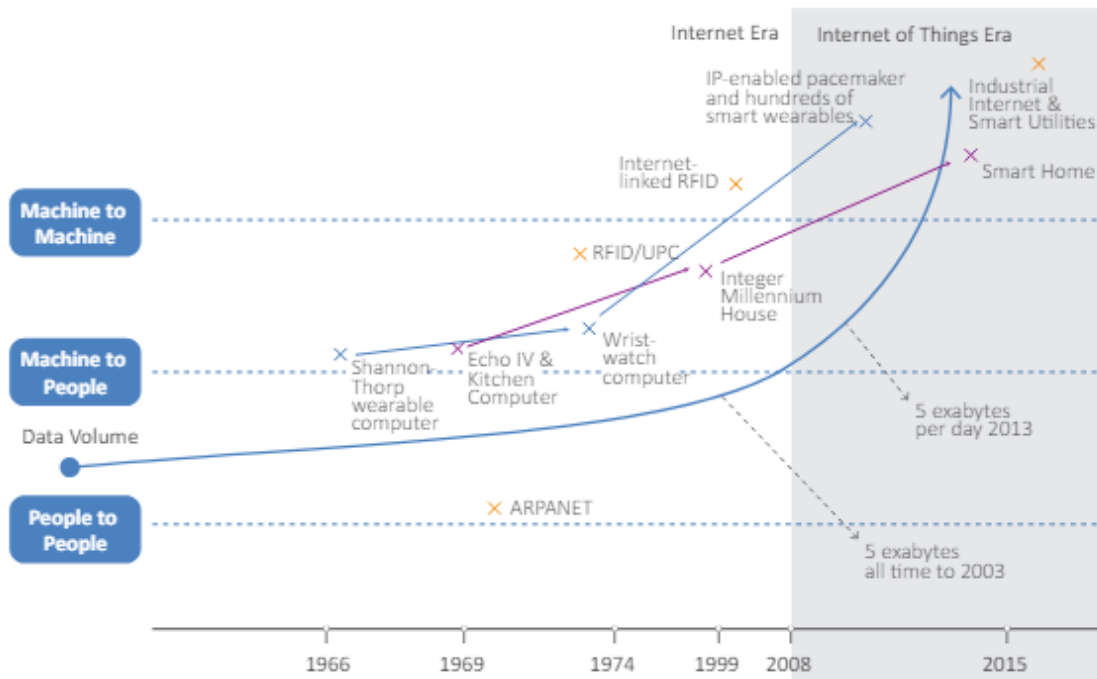
Figure 1.3: Path to IoT from people-to-people to machine-to-machine (M2M) communication[8]

1.7   In India, the Department of Telecommunications (DoT), Ministry of Communications, Government of India issued the National Telecom M2M Roadmap[9] in May 2015. As per the roadmap, "*IoT is connected network of embedded devices capable of having M2M communication without human intervention*".

1.8   In October 2023, the Telecommunication Engineering Centre (TEC), a technical body of the DoT, defined M2M, in its technical paper, as below:

"*M2M refers to the technologies that allow wired/ and wireless system to communicate with devices of the same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, meter reading, temperature, etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information*".[10]

---

[8] Source: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf
[9] Source: https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf
[10] Source: https://www.tec.gov.in/pdf/M2M/Report%20on%20TEC%20initiatives%20in%20IoT%20domain_Oct%202023.pdf

1.9   The network of physical objects connected to the Internet that are embedded
        with sensors, software, thermostats, cameras, speakers, and other related
        technologies have found various applications in day-to-day life, allowing for
        governments, businesses, and individuals to digitize the physical world into
        harmonious connectivity[11]. From bolstering the resilience of services such as
        healthcare, energy distribution, and transportation to optimizing sectors like
        retail, agriculture, and smart homes, IoT and M2M have the potential to
        transcend traditional boundaries to redefine the way we live, work, and interact
        with our environment.

1.10   While the potential market opportunities for IoT and M2M are immense, the
        adoption of IoT and M2M has not fully met the expectations[12], particularly in the
        developing countries[13]. In the year 2023, the global M2M market of US$ 21.2
        Billion[14] contributed less than 1% to the global telecommunication market of
        US$2970.7 Billion[15]. For IoT and M2M to become technologically ubiquitous (in
        the words of Mark Weiser), much is yet to done by the stakeholders of the IoT
        ecosystem as well as the governments, and regulators.

**B.   Policy and Regulatory Developments w.r.t. M2M Communications in
         India**

1.11   In May 2015, the DoT published the National Telecom M2M Roadmap[16] to outline
        the broad policy and regulatory approach to facilitate the M2M ecosystem in the
        country.

---

[11] Source: https://www3.weforum.org/docs/WEF_State_of_the_Connected_World_2023_Edition.pdf
[12] Source: https://www.forbes.com/sites/forbestechcouncil/2019/05/02/the-iot-yesterdays-predictions-vs-todays-reality/?sh=3a5b2dd7512b
[13] Source: https://www.conf.cmi.aau.dk/digitalAssets/99/99461_martinez---m2m-communications.pdf
[14] Source: https://www.imarcgroup.com/machine-to-machine-connections-market
[15] Source: https://www.thebusinessresearchcompany.com/report/telecom-global-market-report
[16] Source:https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap_0.pdf

1.12   In September 2017, the Telecom Regulatory Authority of India (hereinafter, also referred to as "TRAI", or "the Authority"), in response to a reference from the DoT, sent its recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications'[17] to the DoT.

1.13   In May 2018, the Government of India, through the National Digital Communication Policy-2018[18] (NDCP-2018), outlined, *inter-alia*, the following strategies for the growth of M2M communication in the country:

(a) Synergising deployment and adoption of new and emerging technologies by:

       i. Creating a roadmap for emerging technologies and its use in the communications sector, such as 5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M.

      ii. Simplifying licensing and regulatory frameworks whilst ensuring appropriate security frameworks for IoT/ M2M/ future services and network elements incorporating international best practices.

      iii. Earmarking adequate licensed and unlicensed spectrum for IoT/ M2M services.

      iv. Encourage use of Open APIs for emerging technologies.

1.14   Based on TRAI's recommendations of 2017, the DoT introduced a separate authorization on Machine-to-Machine (M2M) under Unified License Agreement[19] in January 2022 and issued 'Guidelines for Registration process of M2M Service

---

[17] https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf
[18] https://dot.gov.in/sites/default/files/Final%20NDCP-2018.pdf?download=1
[19] As per the Unified License, the M2M authorization covers the following:

"2(i) The Licensee shall own the underlying network to provide connectivity and related services for M2M Service Providers.
2(ii) The Licensee can perform functions such as:
(a) access and integration of resources provided by other providers;
(b) support and control of the M2M/IoT capable infrastructure;
(c) offering of M2M/IoT capabilities, including network capabilities and resource exposure to other providers.
2(iii) The Licensee intending to provide services exclusively through the LPWAN or equivalent technologies using unlicensed spectrum shall be covered under this authorization. Such licensees may also obtain licensed spectrum to provide M2M services exclusively, if they desire to provide M2M services in the licensed band.
2(iv) Except those services permitted under the scope of this authorization, the Licensee shall not provide any service / services which require a separate service authorization / license.
2(v) The Unified Licensees having Access Service authorization and Unified Access Services (UAS) licensees can provide the M2M services covered under this authorization and need not to obtain this authorization separately."
Source:https://dot.gov.in/sites/default/files/UL%20AGREEMENT%20with%20Audiotex%20M2M%20without%20INSAT%20MSSR%2017012022_0.pdf?download=1

Providers (M2MSP) & WPAN/ WLAN Connectivity Providers for M2M Services'[20] in February 2022.

C.   The DoT's Reference dated 01.01.2024

1.15   The DoT, through its letter No. 4-31/ M2M Critical Services/ 2019-NT dated 01.01.2024 **(Annexure-I)**, sent a reference to TRAI under the terms of section 11 of TRAI Act, 1997 (as amended). The reference is reproduced below:

"This has reference to the TRAI recommendation dated 05.09.2017 on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" which were accepted by the Government and same was conveyed vide letter No.4-16/2015-NT of March '20. (copy enclosed as Annexure-I).

1.1. One of the recommendations of TRAI (Para 5.1 (g)) was with respect to identification of Critical Services in M2M sector. The same is reproduced here in under-
"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.

1.2   Government accepted the above recommendation with the following remarks:
The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services this regard.

Considering the specific and critical needs of such services and taking into consideration of evolving technologies and needs, as the case may be, government shall declare any such service as critical from time to time.

1.3   In order to have a wider understanding of sectoral 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. The aforesaid Working Group 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. (Relevant excerpt of the IMWG Report is attached as Annexure-II).

1.4   Subsequently, the guidelines for M2M Authorisations under UL and UL-VNO, M2M Service Provider Registration and Captive Non-Public Network (CNPN) License were issued by DoT in Jan, Feb, and June 2022 respectively.

1.5   Considering the introduction of aforesaid new license (UL-M2M) and registration policy, comments were solicited from all relevant stakeholders in the M2M/ IoT ecosystem (including keyline ministries, registered M2M Service Providers and other stakeholders) on the IMWG Report and SLA required for Critical Services. The list of stakeholders who have provided comments, is placed at Annexure-III.

2. Following points have emerged based on the comments received from various stakeholders necessitating a need to revisit and examine afresh the abovesaid recommendation-

I.   Use of licensed spectrum may not be made mandatory for critical services/ sector, if the requisite Service Level Agreements (SLAs)/ Quality of Service (QoS) can be met through unlicensed spectrum. Many Startups/ companies are

designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.

II. 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.

III. A balanced approach of utilizing both licensed and unlicensed bands may be the way forward to improve customer experience, drive innovation and increase affordability. Connectivity may be left to the discretion of the customer/ministries based on service parameters required for an application and not be enforced.

IV. 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.

3. Secondly, as per extant instructions, SIMs are non-transferable. A provision was introduced vide DoT instructions dated 16.05.18 to update the details of person to whom device is transferred in the database of the licensee (as intimated by M2MSP to the licensee) in case the devices with M2M SIM(s) are sold or transferred, However, there is no provision for change in the name of the owner of the M2M SIM.

3.1 Industry has requested to allow the transfer of ownership of M2M SIMs for the following scenarios:

i.   Involving mergers, acquisitions, takeover of companies.

ii. For cases where companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versa and between its subsidiaries/ group companies.

iii. For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/ deployed.

3.2 It is therefore necessary to examine the issue related to Transfer of ownership in case of M2M SIMs in view of situations narrated at 3.1 above.

4.   Accordingly, TRAI is requested to provide reconsidered recommendations, as per provisions of Section 11 of the TRAI Act 1997 as amended from time to time on-

i.   Identification of Critical Services in the M2M Sector

ii. Transfer of Ownership of M2M SIMs"

D.   Additional Information Sought from DoT

1.16   Through a letter dated 12.01.2024, TRAI requested the DoT to provide certain information with respect to the DoT's reference dated 01.01.2024 including a

clarification as to whether the list of 20 services, identified as critical by the IMWG, has been approved. 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*".

E.   The Present Consultation Paper

1.17   In this background, this Consultation Paper has been prepared to solicit comments of stakeholders on specific issues related to critical services in the M2M sector and the transfer of ownership of M2M SIMs. The Chapter I provides introduction and background information. The Chapter II examines the issues. The Chapter III summarizes the issues for consultation.

CHAPTER II: EXAMINATION OF ISSUES

2.1   This chapter outlines the important aspects of M2M communications, and then proceeds to examine the issues on which the DoT has sought recommendations from TRAI.

A.   The M2M Ecosystem

2.2   The M2M ecosystem is entirely different from the standard telecommunication ecosystem. It is more diverse and involves multiple stakeholders. The oneM2M[21], which develops standards for IoT and M2M, has identified the following functional roles in the M2M ecosystem:

(a)   <u>The User</u> (individual or company – aka: end-user): Uses an M2M solution.

(b)   <u>The Application Service Provider</u>: Provides an M2M Application Service and operates M2M Applications.

(c)   <u>The M2M Service Provider</u>: Provides M2M Services to Application Service Providers and operates M2M Common Services.

(d)   <u>The Network Operator</u>: Provides Connectivity and related services for M2M Service Providers and operates an Underlying Network.

---

[21] oneM2M is a global partnership initiative between eight of the world's preeminent standards development organizations: ARIB (Japan), ATIS (U.S.), CCSA (China), ETSI (Europe), TIA (U.S.), TSDSI (India), TTA (Korea), and TTC (Japan) together with industry fora and consortia (Global Platform) to develop specifications that ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT). Source: https://www.onem2m.org/harmonization-m2m

B.   Use cases of M2M

2.3   M2M can enable applications and services across a broad range of vertical markets. To illustrate, a few verticals and related M2M applications are given below:

Industry verticals	M2M applications
Automotive	Vehicle tracking, e-call, V2V & V2I applications, Traffic control, Navigation, Infotainment, Fleet management, Asset tracking, Manufacturing, Logistics, etc.
Utilities	Smart metering, Smart grid, Electric line monitoring, Gas/ Oil/ Water pipeline monitoring, etc.
Healthcare	e-health, Remote diagnostics, Medication reminders, Tele-medicine, wearable health devices, etc.
Safety and Surveillance	Women Safety Bands, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police/medical alert, etc.
Financial	Point of sale (POS), ATM, Kiosk, Vending machines, Digital signage, and Handheld terminals, etc.
Public Safety	Highway, Bridge, Traffic management, Homeland security, Police, Fire, and Emergency services, etc.
Smart City	Intelligent transport System, Waste management, Street Light control system, Water distribution, Smart Parking, etc.
Agriculture	Remotely controlled irrigation pump, Remote Monitoring of Soil Data, etc.

Table 2.1: Examples of M2M applications

C. M2M Communication Technologies

2.4 Many communication technologies are used in the M2M/ IoT domain depending upon the requirements of applications such as coverage, power, quality of service (QoS) etc. The Telecom Engineering Center (TEC), in its technical report on 'Communication Technologies in M2M/ IoT Domain' (2017)[22], identified the wireless technologies for M2M communication as below:
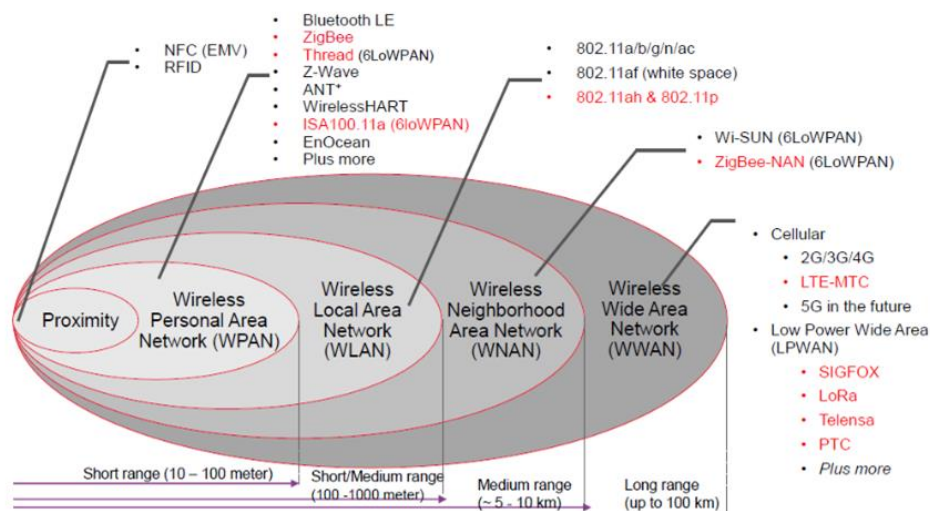
Figure 2.1: Key wireless technologies for M2M communication

2.5 In the afore-mentioned technical report, the TEC mentioned that the wide area network (WAN) may also have wired technologies such as fixed line broadband, Fiber to the home (FTTH) and Power line communication (PLC).

2.6 In November 2021, the TEC issued another technical report on 'Emerging Communication Technologies and Use cases in IoT Domain'[23]. In the technical report, the TEC also included 5G, Wi-Fi 6, Wi-Fi 6E, Wi-Fi HaLow[24], and Bluetooth Mesh[25] as key technologies for M2M communication.

---

[22] Source: https://www.tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf
[23] Source: https://www.tec.gov.in/pdf/M2M/Emerging%20Communication%20Technologies%20&%20Use%20Cases%20in%20 IoT% 20domain.pdf
[24] Wi-Fi HaLow operates in spectrum below 1GHz with a typical range of 1 km. It is part of the Wi-Fi stack developed by Wi-Fi Alliance. Source: https://www.quectel.com/what-is-wi-fi-halow-iot
[25] Bluetooth Mesh is a computer mesh networking standard based on Bluetooth Low Energy that allows for many-to-many communication over Bluetooth radio.

2.7   Essentially, the TEC, in its technical reports, has classified M2M communication technologies based on <u>the range of communication</u>. Typical ranges and typical M2M communication technologies for various types of networks are given below:

S. No.	Type of network	Typical range of communication	Examples of M2M communication technologies
1	Proximity	~ 1 m	NFC, RFID
2	Personal Area Network (PAN)	10 - 100 meter	Bluetooth, Zigbee, Thread, Z-wave, ANT, Wireless HART, ISA100.11a, EnOcean
3	Local Area Network (LAN)	100 - 1000 meter	802.11a/b/g/n/ac, 802.11af 802.11ah and 802.11p
4	Neighborhood Area Network (NAN)	5 - 10 km	Wi-SUN ZigBee-NAN
5	Wide Area Network (WAN)	Upto 100 km	Cellular (2G/ 3G/ 4G/ 5G) Wired technologies such as fixed line Broadband, FTTH and powerline communication Low Power Wide Area Network (LPWAN) technologies such as SIGFOX, LoRa, Telensa, PTC

Table 2.2: Features of typical networks for M2M

2.8   A brief description of the technologies used for providing M2M communication services is given in the **Annexure-II** of this Consultation Paper.

D.   The existing regulatory framework for M2M communication services in the country

2.9   Based on TRAI's recommendations of 2017, the DoT has devised a three-tiered regulatory framework for M2M communication services in the country, as outlined below:

S. No.	Type(s) of networks for provisioning M2M communication services	License/ Registration required for operating the network(s)	Type of frequency spectrum
1	Wireless Personal Area Network (WPAN), and Wireless Local Area Network (WLAN)[26]	Registration of M2M Service Provider (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services	Unlicensed
2	Low Power Wide Area Network (LPWAN)[27]	M2M Authorization under Unified License	Unlicensed
3	Access network within a telecom circle/ Metro area[28] – cellular networks as well wireline networks	Access Service Authorization under Unified License and Unified Access Service License	Licensed

Table 2.3: The regulatory framework for M2M communication services in India

---

[26] The Guidelines for Registration Process of M2M Service Providers(M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services define WPAN and WLAN as below:

*"**WPAN**": A Personal Area Network (PAN) is a network used for data transmission among personal devices such as computers, phones, personal digital assistants, wearables, etc. Wireless PAN or WPANs can be used for communication among the personal devices (intra-personal communication), or for connecting to a higher-level network and the Internet (an uplink). Technologies used in PAN are Bluetooth, Z-Wave, ZigBee, RFID etc.*

*"**WLAN**" means a wireless network whereby a user can connect to a local area network (LAN) through a wireless (radio) connection, as an alternative to a wired local area network. An example of a Wireless LAN is Wi-Fi.*

[27] As per the Unified License Agreement, "*LPWAN is type of WAN which provide wireless connectivity to low-power devices over large distance that is suited for M2M communication*". Source: https://dot.gov.in/sites/default/files/Compendium-UL-AGREEMENT%20updated%20up%20to%2031032024.pdf?download=1

[28] As per the Unified License Agreement, "*[t]he Access Service under Access Service authorization covers collection, carriage, transmission and delivery of voice and/or non-voice MESSAGES over Licensee's network in the designated Service Area. … The Licensee may provide access service, which could be on wireline and / or wireless media with full mobility, limited mobility and fixed wireless access*". The service areas for access service are telecom circles/ metro areas.

2.10   The present regulatory framework for the use of licensed and unlicensed spectrum for providing M2M communication services, is summarized below:

(a)   <u>M2M communication services using the unlicensed spectrum</u>: The entities holding the 'M2M authorization under Unified License' may provide M2M communication services through the LPWAN or equivalent technologies using unlicensed spectrum[29]. The entities holding the 'Registration of M2M Service Provider (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services' are authorized to use WPAN/ WLAN technologies in unlicensed spectrum/ frequency exempt bands to provide M2M communication services.

(b)   <u>M2M communication services using the licensed spectrum</u>: The entities holding Access Service Authorization under Unified License and Unified Access Service License can obtain the licensed access spectrum from the DoT to provide wireless access services including M2M communication services. Various licensees holding the Access Service Authorization under the Unified License have obtained access spectrum in the 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 3300 MHz, and 26 GHz bands to provide wireless access services using GSM/ WCDMA/ LTE/ CDMA/ IMT-2020 technologies. They are permitted to use other technologies based on the standards approved by ITU/ TEC or any other International Standards Organization/ bodies[30].

2.11   The Unified Licensees having the Access Service authorization and the Unified Access Services (UAS) licensees can also provide M2M services through the LPWAN or equivalent technologies using unlicensed spectrum. They can also provide WPAN/ WLAN connectivity in the unlicensed bands.

---

[29] Source: https://dot.gov.in/sites/default/files/Compendium-UL AGREEMENT%20updated%20up%20to%2031032024.pdf?download=1
[30] Source: https://dot.gov.in/sites/default/files/Notice%20Inviting%20Applications%202023-24.pdf

E.   Critical services in the M2M sector

(1) The TRAI's recommendation on critical services in the M2M sector

2.12   As mentioned in the Chapter-I of this Consultation Paper, the Authority sent its recommendations on 'Spectrum, Roaming and QoS Related Requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017 (hereinafter, also referred to as, "the M2M Recommendations of 2017") to the DoT after following a consultation with stakeholders. The matter related to the provision of critical services in the M2M sector also came up for examination at the time of stakeholders' consultation. The Authority made the following observations with respect to the critical services in the M2M Recommendations of 2017:

"2.46   M2M services and applications can be differentiated based on its nature as critical and non-critical. A large number of devices and applications in M2M/ IoT ecosystem will be non-critical in nature. These devices may be either connected through Personal Area Network (PAN) to a local gateway or there may be SIM based standalone connectivity using cellular network. However, there would be some critical M2M applications that would 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 and accountability. If there is any variation in QoS, latency or availability, it can cause substantial damage to customers. It is pertinent that such throughput and latency sensitive application should run only on robust wired optical fiber, copper network or LTE capable access networks.

2.47   As stated earlier, operation in licensed spectrum has certain exclusive rights in terms of usage and is also shielded for any interference. Also, the QoS parameters are measurable and enforceable. Moreover, the government has

administrative control over the licensed connectivity providers. So, critical services should be identified and mandated to be provided by connectivity provider using licensed spectrum. Hence there is a need to identify critical services in which, quality of service, if deficient, could result in serious consequences. Also, the telecom networks should be able to differentiate the critical services from the non-critical services and prioritize the carriage of information on their network based on the critical nature of information."

2.13 Based on the above observations, the Authority, through the M2M Recommendations of 2017, recommended that "*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.*"

(2) The DoT's observations on the TRAI's recommendation on critical services in the M2M sector

2.14 With respect to the afore-mentioned recommendation on critical services in the M2M sector, the DoT has, through the reference dated 01.01.2024, conveyed the following to TRAI:

"1.2 Government accepted the above recommendation with the following remarks:

The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services in this regard.

Considering the specific and critical needs of such services and taking into consideration of evolving technologies and needs, as the case may be, government shall declare any such service as critical from time to time. "

(3) The report of an Inter-Ministerial Working Group (IMWG) constituted to identify critical services in the M2M sector

2.15 In November 2019, the Government constituted an Inter-Ministerial Working Group (IMWG) in order to have a wider understanding of the sectoral requirements of critical M2M applications. The IMWG furnished its report in March 2021 with the following key observations:
"

(a) *Critical Internet of Things (IoT) is an emerging concept in IoT development that enables more efficient and innovative services across a wide range of industries by reliably meeting time-critical communication needs.*

(b) *Critical IoT addresses the time critical communication needs of individuals, enterprises, and public institutions. It is intended for time-critical applications that demand data delivery within a specified time duration with required guarantee (reliability) levels.*

(c) *Failure in a critical IoT system unlike with massive IoT, could lead to widespread systematic issues within a smart city, business, or infrastructure setting. Critical services thus require high QoS, ultra reliability, very low latency, very high availability alongwith accountability with requisite security."*

2.16 In its report, the IMWG recommended that the following services should be classified as critical M2M/ IoT services:
"
i. *Connected and Autonomous Cars/ three wheelers and two wheelers.*

ii. *Remote Surgery - Mission Critical remote surgery and other health related applications.*

iii.   *Trauma and Burn patients handling and care leading to National Injury Surveillance.*

iv.   *Remote Patient Tracking and Monitoring (Home/ In-patient).*

v.   *Remote Diagnostics.*

vi.   *Drug Management.*

vii.   *Remote control in mining, Oil and Gas.*

viii.   *Safety & Surveillance: State, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police.*

ix.   *Defense Networks.*

x.   *Financial Transactions.*

xi.   *Remote early warning sensors – for weather alert and disaster management.*

xii.   *Energy Smart Grids.*

xiii.   *Utilities distribution networks including Power, Water and Cooking Gas.*

xiv.   *Distribution Network of inflammable/ explosive articles.*

xv.   *Chemical and Nuclear Industry.*

xvi.   *Food Industry including Smart Cultivation, Storage and Public Distribution Systems.*

xvii.   *Aviation - Remote radar systems.*

xviii.   *Drone Communications including UAV-UAV, UAV-GCS and UAV- Network.*

xix.   *Space and Research.*

xx.   *Control network of Smart Cities."*

2.17   In its report, the IMWG also made the following recommendations with respect to the regulatory requirements for critical M2M/ IoT services:

"The regulatory requirements for above-identified critical services covers broad range and is to be defined by respective ministries as being done by ARAI and BIS. However, broad recommendations of the working group are:

i. *The critical services should be provided only using connectivity from the licensed telecom operators from DoT.*

ii. *These services shall use connectivity being offered on licensed spectrum bands.*

iii. *Details regulatory requirements for these critical services shall be issued by respective ministries/ regulatory bodies."*

(4) The DoT's consultation with stakeholders on the IMWG Report and the SLA required for critical services in the M2M sector

2.18 Through the reference dated 01.01.2024, the DoT has informed that it solicited comments from all relevant stakeholders in the M2M/ IoT ecosystem including key line ministries, registered M2M Service Providers, and other stakeholders on the IMWG Report and SLA required for critical services. The DoT has stated that based on the comments received from various stakeholders, the following points have emerged which necessitate a need to revisit and examine afresh the TRAI's recommendation relating to critical services in M2M sector:
"

I. *Use of licensed spectrum may not be made mandatory for critical services/ sector, if the requisite Service Level Agreements (SLAs)/ Quality of Service (QoS) can be met through unlicensed spectrum. Many Startups/ companies are designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.*

II. *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.

III. *A balanced approach of utilizing both licensed and unlicensed bands may be the way forward to improve customer experience, drive innovation and increase affordability. Connectivity may be left to the discretion of the customer/ ministries based on service parameters required for an application and not be enforced.*

IV. *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 trustworthiness 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."*

(5) Examination of the issues related to critical services in the M2M sector

2.19 As mentioned earlier, the Authority through the M2M Recommendations of 2017 recommended, *inter-alia*, that *"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".*

2.20   The afore-mentioned recommendation has two operative parts, viz.-

(a)   The Government should identify critical services in the M2M sector; and

(b)   The Government should mandate that the critical services in the M2M sector should be provided only by connectivity providers using licensed spectrum.

2.21   With respect to the part (a) of the afore-mentioned recommendation, the DoT has taken steps towards identifying critical services in the M2M sector through the IMWG. On this aspect, stakeholders have conveyed to the DoT that instead of classifying entire domain/ sector as critical, specific applications within a domain/ sector should be identified as critical based on the market requirement.

2.22   With respect to the part (b) of the afore-mentioned recommendation, stakeholders have expressed their concern to the DoT against mandating the critical M2M/ IoT services to be provided only by connectivity providers using the licensed spectrum.

2.23   In this background, through the reference dated 01.01.2024, the DoT has conveyed that there is a need to revisit and examine afresh the afore-mentioned recommendation and has requested TRAI to provide reconsidered recommendation on the matter.

2.24   The Authority took note that Ericsson, in its white paper on the Cellular Networks for Massive IoT (January 2016), made a distinction of massive IoT and critical IoT. In the white paper, Ericsson stated that "*[a]t one end of the scale, in Massive IoT applications – typically sensors that report to the cloud on a regular basis – the end-to-end cost must be low enough for the business case to make sense. Here, the requirement is for low-cost devices with low energy consumption and good coverage. At the other end of the scale, Critical IoT applications will have very high demands for reliability, availability and low latency.*"

2.25 In its white paper, Ericsson also depicted different regulatory requirements for massive IoT and critical IoT as below:
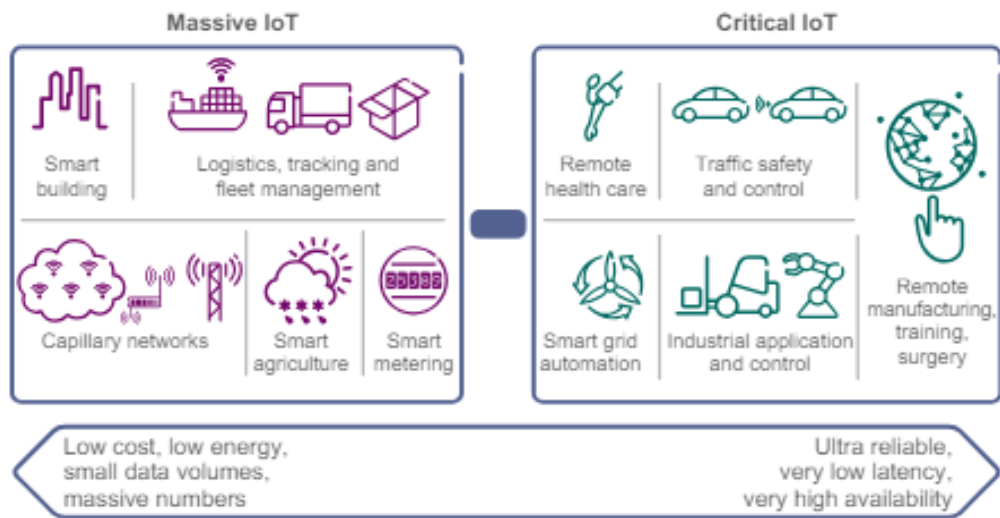
Figure 2.2: Different requirements for massive IoT and critical IoT applications

2.26 With respect to the provision of critical IoT applications, the following aspects are noteworthy:

(a) The IMWG, in its report of March 2021, observed that critical IoT "*is intended for <u>time-critical applications</u> that demand data delivery within a specified time duration with required guarantee (reliability) levels*" and "*[c]ritical services thus require high QoS, ultra reliability, very low latency, very high availability alongwith accountability with requisite security.*"

(b) In the recommended list of 20 services to be classified as critical M2M/ IoT services, the IMWG included, *inter-alia*, domains/ sectors such as <u>drug management</u> and <u>food industry</u> including smart cultivation, storage and public distribution systems. The IMWG recommended that the services included in the list "*shall use connectivity being offered on licensed spectrum bands.*"

(c)   In the DoT's consultation, stakeholders contended, *inter-alia*, as below:

(i)   <u>Entire domain/ sector</u> should not be classified as critical; instead, specific applications within a domain/ sector should be identified as critical based on the use cases.

(ii)   Use of licensed spectrum should not be made mandatory for critical M2M/ IoT services. 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.

(iii)   IoT/ M2M devices for critical infrastructure sectors should also be brought under the Trusted Source/ Trusted Product regulation.

2.27   With respect to the issue related to security and trustworthiness of M2M/ IoT devices, it is worth mentioning that through the M2M Recommendations of 2017, the Authority had recommended, *inter-alia*, as below:

"a) Device manufacturers should be mandated to implement "Security by design" principle in M2M device manufacturing so that end-to-end encryption can be achieved.

b) The government should provide comprehensive guidelines for manufacturing/ importing of M2M devices in India.

c) A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software)."

[The above recommendation has been accepted by the Government.]

2.28   With respect to the demand of stakeholders to bring IoT/ M2M devices for critical infrastructure sectors under the Trusted Source/ Trusted Product regulation, it is

noteworthy that the DoT has stipulated, *inter-alia*, the following provision in the Unified License:

"*39.7.1. The Government through the Designated Authority will have the right to impose conditions for procurement of Telecommunication Equipment on grounds of Defence of India, or matters directly or indirectly related thereto, for national security. Designated Authority for this purpose shall be National Cyber Security Coordinator. In this regard, the licensee shall provide any information as and when sought by the Designated Authority.*

Designated Authority shall notify the categories of equipment for which the security requirement related to Trusted Sources are applicable. For the said categories of equipment, Designated Authority shall notify the Trusted Sources along with the associated Telecommunication Equipment (Trusted Products). The Designated Authority may also notify a list of Designated Sources from whom no procurement can be done. Procedure for inclusion of Telecommunication Equipment in the list of Trusted Sources will be issued by the Designated Authority.

With effect from 15th June 2021, the licensee, shall only connect Trusted Products in its network and also seek permission from Designated Authority for upgradation of existing Network utilizing the Telecommunication Equipment not designated as Trusted Products. However, these directions will not affect ongoing Annual Maintenance Contracts (AMC) or updates to existing equipment already inducted in the network as on date of effect.

The licensees shall comply with the Guidance for Enhanced Supervision and Effective Control of Telecommunication Networks, as per guidelines to be issued by the licensor."

2.29 In this background, the authority solicits comments of stakeholders on the following set of questions:

Issues for consultation:

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.

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.

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.

F.   The transfer of ownership of M2M SIMs

2.30   Through the reference dated 01.01.2024, the DoT has requested TRAI to provide recommendation on "*Transfer of Ownership of M2M SIMs*". The relevant extract of the reference dated 01.01.2024 is reproduced below:

"3. … as per extant instructions, SIMs are non-transferable. A provision was introduced vide DoT instructions dated 16.05.18 to update the details of person to whom device is transferred in the database of the licensee (as intimated by M2M SP to the licensee) in case the devices with M2M SIM(s) are sold or transferred, However, there is no provision for change in the name of the owner of the M2M SIM.

3.1   Industry has requested to allow the transfer of ownership of M2M SIMs for the following scenarios:

   i.   Involving mergers, acquisitions, takeover of companies.
   ii.   For cases where companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versal and between its subsidiaries/ group companies.
   iii.   For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/deployed.

3.2   It is therefore necessary to examine the issue related to Transfer of ownership in case of M2M SIMs in view of situations narrated at 3.1 above."

2.31   Subscriber Identity Modules (SIMs) are used for providing telecommunication services using 3GPP[31] standards. A subscriber obtains a SIM from its access service provider when a new cellular mobile connection is activated in his name.

---

[31] Source: https://www.3gpp.org/

SIMs contain communication profiles that uniquely identify cellular mobile subscriptions. A communications profile includes Mobile Station International Subscriber Directory Number (MSISDN) and International Mobile Subscriber Identity (IMSI). Generally, the SIMs, which are used for People-to-People (P2P) mobile communication, are referred to as 'consumer SIMs'. On the other hand, the SIMs, which are used for Machine-to-Machine (M2M) mobile communication, are referred to as 'M2M SIMs'.

2.32   As per the extant licensing framework in the country, the change in the name of subscriber, in the case of <u>consumer mobile connections</u>, is permitted only between the blood relations/ legal heirs. The relevant extract of the DoT's instructions dated 09.08.2012[32] in this regard is reproduced below:

"*7. Change in the name of subscriber*

(i) The change of name of subscriber is not permitted as the SIM card in user terminal is not transferable. <u>The change in name between the blood relations/ legal heirs is permitted</u> provided new CAF and all the procedure as for registering a new subscriber is followed and new SIM Card is issued. However, after the change in name the connection shall be treated as new connection. In such case, change in address is not permitted. Further, No Objection Certificate from the original user shall also be taken. In case of death of the original user, death certificate will suffice instead of No Objection Certificate."

2.33   As per the DoT's instructions[33] dated 16.05.2018 read with the DoT's Guidelines[34] for Registration Process of M2M Service Providers (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services dated 08.02.2022 (hereinafter, referred to as, "the M2MSP Guidelines"), an access service provider may grant <u>M2M mobile connections</u> to M2MSP registrants only. As per the M2MSP Guidelines, the

---

[32]Source:https://dot.gov.in/sites/default/files/Instructions%20on%20Verification%20of%20New%20Mobile%20Subscribers%20%281%29.PDF?download=1

[33] Source: https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

[34] Source: https://dot.gov.in/sites/default/files/M2SP%20Guidelines%20.pdf?download=1

M2MSP registrants are authorized to "*provides M2M services to third parties using telecom resources. Provided that (a) such third parties utilising M2M services from registered M2MSP in connection with its products or as part of its offerings to its end customers as a product or service, and (b) any organization which intends to provide M2M services for its own use (captive use) and not for commercial purpose, shall also be covered under this definition.*"[35]

2.34   The M2MSP Guidelines also provides that "*[t]he details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Updated information regarding (a) details of M2M end device i.e., IMEI, ESN etc., (b) Make, Model, Registration number etc. of the machines (i.e. Cars, Utility Meters, POS, etc.) & (c) corresponding physical custodian's name and address shall be made available to Authorized Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated.*"

2.35   While the change in the name of customers of M2M services (custodians of the machines fitted with M2M SIMs) is permitted, there is no provision in the M2MSP Guidelines for the change in the name of the owner of the M2M SIMs i.e. M2MSPs.

2.36   In summary, the extant regulatory framework applicable for the change of ownership of SIMs in the country is tabulated below:

---

[35] Source: https://dot.gov.in/sites/default/files/M2MSP%20Guidelines%20.pdf?download=1

Type of mobile connections	Who owns the SIM(s)	Provision relating to the change of the owner of the SIM(s)
Consumer connection	Subscribers	The change of ownership of SIM is permitted only between the blood relations and legal heirs.
M2M connection	M2MSP registrants	There is no provision for the change in the name of the owner of the M2M SIM.

Table 2.4: The regulatory framework for the change of ownership of SIMs in the country

2.37 In this background, the DoT, through the reference dated 01.01.2024, has stated that the industry has requested to allow the transfer of ownership of M2M SIMs in the following scenarios:

(a) Involving mergers, acquisitions, takeovers of companies.

(b) For cases where companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versa and between its subsidiaries/ group companies.

(c) For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/deployed.

2.38 As per the M2MSP Guidelines, in case an M2MSP registration merges with (or gets acquired by) another entity, the M2MSP registration does not get transferred to the resultant entity. The relevant extract of the M2MSP Guidelines is reproduced below:

"10. In case of merger/acquisition, the registration granted cease to exist and the new entity has to re-register."

2.39 It is noteworthy that the transfer of the Unified License is permitted with a prior written consent of the Licensor (i.e., the DoT) in certain circumstances subject to the guidelines issued by the DoT on the subject. The relevant extract of the Unified License Agreement is given below:

"6. Restrictions on 'Transfer of License':

6.1 The Licensee shall not, without a prior written consent of the Licensor as described below, either directly or indirectly, assign or transfer this License in any manner whatsoever to a third party or enter into any agreement for sub-License and/or partnership relating to any subject matter of the License to any third party either in whole or in part i.e. no sub-leasing/ partnership/ third party interest shall be created. For provision of the service by the Licensee, the Licensee may appoint or employ franchisee, agents, distributors and employees.

6.2 The Licensor shall have the right to direct the Licensee to warn, penalize or terminate the services of the franchisee or agent or distributor or employee (servant), after considering any report of conduct or antecedents detrimental to the security of the nation. The decision of the Licensor in this regard shall be final and binding and in any case the Licensee shall bear all liabilities in the matter and keep the Licensor indemnified for all claims, cost, charges or damages in this respect.

6.3 Intra service area mergers and acquisitions as well as transfer of licenses shall be subject to the guidelines issued on the subject from time to time by the Licensor.

6.4 Further, the Licensee may transfer or assign the License Agreement with prior written approval of the Licensor, in the following circumstances, and if otherwise, no compromise in competition occurs in the provisions of Telecom Services:-

(i)(a) When transfer or assignment is requested in accordance with the terms and conditions on fulfillment of procedures of Tripartite Agreement if already executed amongst the Licensor, Licensee and Lenders; or

(i)(b) Whenever amalgamation or restructuring i.e., merger or demerger is sanctioned and approved by the High Court or Tribunal as per the law in force; in accordance with the provisions; more particularly Sections 230 to 233 of Companies Act, 2013; provided that scheme of amalgamation or restructuring is formulated in such a manner that it shall be effective only after the written approval of the Licensor for transfer/merger of Licenses,

and

(ii) Prior written consent/ No Objection of the Licensor has been obtained for transfer or merger of Licenses as per applicable guidelines issued from time to time. Further, the transferee/ assignee is fully eligible in accordance with eligibility criteria as applicable for grant of fresh License in that area and show its willingness in writing to comply with the terms and conditions of the License agreement including past and future roll out obligations as well as to comply with guidelines for transfer/merger of Licenses including for charges as applicable; and

(iii) All the past dues are fully paid till the date of transfer/ assignment by the Transferor Company and Transferee Company; and thereafter the transferee company undertakes to pay all future dues inclusive of anything remained unpaid of the past period by the outgoing company."

2.40   Further, the newly enacted Telecommunications Act, 2023 provides that any authorised entity may undertake any merger, demerger or acquisition, or other forms of restructuring subject to the extant laws. The relevant provision of Telecommunications Act, 2023 is reproduced below:

"3. (1) Any person intending to—
(a) provide telecommunication services;
(b) establish, operate, maintain or expand telecommunication network; or
(c) possess radio equipment,
shall obtain an authorisation from the Central Government, subject to such terms and conditions, including fees or charges, as may be prescribed.

(5) <u>Any authorised entity may undertake any merger, demerger or acquisition, or other forms of restructuring</u>, subject to any law for the time being in force and any authorised entity that emerges pursuant to such process, shall comply with the terms and conditions, including fees and charges, applicable to the original authorised entity, and such other terms and conditions, as may be prescribed."

[The appointed date of the Telecommunications Act, 2023 is yet to be notified.]

2.41   Any entity holding M2MSP registration may have to undergo through merger/ acquisition, closure of business, or reorganization of business within the business group. One may contend that under such situations, the subscribers should not be inconvenienced and the M2M services should remain available to them seamlessly. Keeping the above in view, *prima facie*, there is a need for establishing a framework for the transfer of ownership of M2M SIMs to avoid service disruptions and inconvenience to users.

2.42   In this background, the Authority solicits comments of stakeholders on the following sets of questions:

Issues for consultation:

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 the new M2MSP for providing connectivity to the existing customers?

    Please provide a detailed response with justifications.

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.

2.43   The following chapter lists the issues for consultation.

CHAPTER-III: ISSUES FOR CONSULTATION

Stakeholders are requested to provides detailed responses to the following questions:

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.**

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.**

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.

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.

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.**

DoT's reference dated 01.01.2024

Government of India
Ministry of Communications
Department of Telecommunications
Networks & Technologies Wing (NT Wing)

No. : 4-31/M2MCriticalServices/2019-NT   Dated: 01.01.2024

Sub: Reference to TRAI for issues involved in M2M Communications -reg

This has reference to the TRAI recommendation dated 05.09.2017 on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" which were accepted by the Government and same was conveyed vide letter No.4-16/2015-NT of March '20. **(copy enclosed as Annexure-I)**

1.1. One of the recommendations of TRAI (Para 5.1 (g)) was with respect to identification of Critical Services in M2M sector. The same is reproduced here in under-

"*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.*"

1.2 Government accepted the above recommendation with the following remarks:

The deliberations converged into an agreement that critical services do require SLAs for effective delivery of services at a certain QoS as may be intended. Considering the scope and breadth of this potential issue, DoT will take up a detailed consultation with all stakeholders to comprehensively examine and identify critical services in this regard.

Considering the specific and critical needs of such services and taking into consideration of evolving technologies and needs, as the case may be, government shall declare any such service as critical from time to time.

1.3 In order to have a wider understanding of sectoral 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. The aforesaid Working Group 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. (Relevant excerpt of the IMWG Report is attached as **Annexure-II).**

1.4 Subsequently, the guidelines for M2M Authorisations under UL and UL-VNO, M2M Service Provider Registration and Captive Non-Public Network (CNPN) License were issued by DoT in Jan, Feb and June 2022 respectively.

1.5   Considering the introduction of aforesaid new license (UL-M2M) and registration policy, comments were solicited from all relevant stakeholders in the M2M/IoT ecosystem (including key line ministries, registered M2M Service Providers and other stakeholders) on the IMWG Report and SLA required for Critical Services. The list of stakeholders who have provided comments, is placed at **Annexure-III**.

2.   Following points have emerged based on the comments received from various stakeholders necessitating a need to revisit and examine afresh the abovesaid recommendation-

I.   **Use of licensed spectrum may not be made mandatory for critical services/sector, if the requisite Service Level Agreements (SLAs)/Quality of Service (QoS) can be met through unlicensed spectrum.** Many Start-ups/companies are designing their model to operate in license-free band. 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. Further, the relationship between security of M2M services and these services operating on licensed spectrum was not cogent.

II.   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.

III.   **A balanced approach of utilizing both licensed and unlicensed bands may be the way forward to improve customer experience, drive innovation and increase affordability.** Connectivity may be left to the discretion of the customer/ministries based on service parameters required for an application and not be enforced.

IV.   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 trustworthiness 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.*

3. Secondly, as per extant instructions, SIMs are non-transferable. A provision was introduced vide DoT instructions dated 16.05.18 to update the details of person to whom device is transferred in the database of the licensee (as intimated by M2M SP to the licensee) in case the devices with M2M SIM(s) are sold or transferred, However, there is no provision for change in the name of the owner of the M2M SIM.

3.1 Industry has requested to allow the transfer of ownership of M2M SIMs for the following scenarios:

i. Involving mergers, acquisitions, takeover of companies.

ii. For cases where companies wish to transfer the ownership from the parent company to its subsidiaries/ other group companies or vice versa/ and between its subsidiaries/ group companies.

iii. For cases where M2MSP is ceasing its operations or is filing for bankruptcy, etc. and the M2M SIMs are required to be either transferred to the new M2MSP or directly to the company where M2M SIMs are used/deployed.

3.2 It is therefore necessary to examine the issue related to Transfer of ownership in case of M2M SIMs in view of situations narrated at 3.1 above.

4. Accordingly, TRAI is requested to provide reconsidered recommendations, as per provisions of Section 11 of the TRAI Act 1997 as amended from time to time on

i. Identification of Critical Services in the M2M Sector

ii. Transfer of Ownership of M2M SIMs

Enclosure: As above

(Dindayal Tosniwal)
DDG-NT, DoT HQ
011-23232348

To
The Secretary,
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi-110 002

No. 4-16/2015-NT   Dated: March, 2020

To
Secretary,
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi-110 002

Sub: Acceptance of Recommendations of TRAI on Quality of Services (QoS),
       Spectrum and Roaming related requirements in M2M communications –
       regarding

Ref: D.O. no. 103-3/2015-NSL-II dated 5th September 2017

        Kindly refer TRAI letter no. 103-3/2015-NSL-II dated 5th September 2017
vide which TRAI recommendations on Quality of Services (QoS), Spectrum and
Roaming related requirements in M2M communications was conveyed.

2.   In this regard, it is to intimate that government has considered and accepted the
TRAI recommendations related to M2M.

3.   This is for your kind information, please.

                                                           02.03.2020
                                                        (Surendra Rai)
                                                         DDG (NT)

<u>**Extracts of the report of the Inter-Ministerial Working Group constituted to identify Critical Services in M2M sector**</u>

In order to have wider understanding of the sectorial requirements of critical M2M applications, an Inter-Ministerial Working Group was constituted.

Observations of the Inter-Ministerial Working Group are as below:

a) Critical Internet of Things (IoT) is an emerging concept in IoT development that enables more efficient and innovative services across a wide range of industries by reliably meeting time-critical communication needs.

b) Critical IoT addresses the time-critical communication needs of individuals, enterprises and public institutions. It is intended for time-critical applications that demand data delivery within a specified time duration with required guarantee (reliability) levels.

c) *Failure in a critical IoT system, unlike with massive IoT, could lead to widespread systematic issues within a smart city, business, or infrastructure setting. Critical services thus require high QoS, ultra-reliability, very low latency, very high availability along with accountability with requisite security.*

Recommendations of the Inter-Ministerial Working Group:

The Inter-Ministerial Working Group recommends following services to be classified as Critical M2M/ IoT Services:

i. Connected and Autonomous Cars/ three wheelers and two wheelers

ii. Remote Surgery - Mission Critical remote surgery and other health related applications.

iii. Trauma and Burn patients handling and care leading to National Injury Surveillance

iv. Remote Patient Tracking and Monitoring (Home/ In-patient)

v. Remote Diagnostics

vi. Drug Management

vii. Remote control in mining, Oil and Gas

viii. Safety & Surveillance; State, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police

ix. Defense Networks

x. Financial Transactions

xi. Remote early warning sensors – for weather alert and disaster management.

xii. Energy Smart Grids

xiii. Utilities distribution networks including Power, Water and Cooking Gas

xiv. Distribution Network of inflammable/ explosive articles

xv. Chemical and Nuclear Industry

xvi. Food Industry including Smart Cultivation, Storage and Public Distribution Systems

xvii. Aviation - Remote radar systems

xviii. Drone Communications including UAV-UAV, UAV-GCS and UAV-Network.

xix. Space and Research

xx. Control network of Smart Cities

The regulatory requirements for above identified critical services covers broad range and is to be defined by respective ministries as being done by ARAI and BIS. However broad recommendations of the working group are:

i. The critical services should be provided only using connectivity from the licensed telecom operators from DoT.

ii. These services shall use connectivity being offered on licensed spectrum bands.

iii. Detailed regulatory requirements for these critical services shall be issued by respective ministries/ regulatory bodies.

****

The Technologies Used for Providing M2M Communication Services

1. A brief description of the main technologies, which are used for providing M2M Communication services, is given below:

A.   RFID

2. A radio-frequency identification (RFID) system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running the RFID software. The RFID works in the unlicensed 120–150 kHz (LF), 13.56 MHz (HF), 433 MHz (UHF), 865-868 MHz (Europe) 902-928 MHz (North America) UHF, 2450-5800 MHz (microwave), 3.1–10 GHz (microwave) frequency band and works within the range of 10 cm to 200 m.

B.   Bluetooth

3. Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances and building personal area networks. The Bluetooth system operates in the 2.4 GHz ISM band. Bluetooth is often used to allow two different types of devices to communicate with each other. Bluetooth devices are classified as Class 1, 2 or 3 and the maximum output power is 20 dBm.

C.   Zigbee

4.   ZigBee is a low-cost, low-power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. ZigBee devices have low latency that further reduces average current. ZigBee operates in the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary from 20 Kbit/s (868 MHz band) to 250 Kbit/s (2.4 GHz band). ZigBee works within the range of 10-100 meters line-of-sight.

D.   Thread

5.   Thread is an IPv6 based networking protocol for Internet of Things (IoT) "smart" home automation devices to communicate on a local wireless mesh network. Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as does ZigBee and other systems. Thread, however, is IP-addressable, with cloud access and AES encryption. It currently supports up to 250 devices in one local network mesh. Thread uses IEEE 802.15.4 radio technology on the unlicensed 2.4 GHz spectrum, which can be deployed worldwide. Thread works within the range of 10 meters.

E.   Z Wave

6.   An IoT Hub or Gateway is a key component of any Z-Wave based IoT deployment. The hub communicates with the smartphone and/ or the communication router to allow access to the home automation devices remotely. A typical deployment may consist of scores or even hundreds of sensors, devices and actuators, which need to send data to a server and/ or receive commands for configuration changes or action. Some hubs have multiple smart home radios

in them (Z-Wave, Bluetooth, etc.) so that they can perform different functions and support different products. The Z-Wave IoT Hub provides a bridge between these sensors, devices and the application server.

F.   ANT/ANT+

7.   ANT represents another ultra-low-power, short-range wireless technology designed for sensor networks and similar applications. This protocol is developed and sold by Canadian company Dyna stream Innovations Inc., a subsidiary of GPS personal navigation firm Garmin. It is conceptually similar to Bluetooth low energy but is oriented towards usage with sensors. ANT also uses the very short duty-cycle technique and deep -sleep modes to ensure very low power consumption. The ANT protocol is set up to use a single 1 MHz channel for multiple nodes due to a time-division multiplex technique. Each node transmits in its own time slot. Modulation is GFSK. It uses the unlicensed 2.4 GHz ISM band.

G.   6LoWPAN

8.   6LoWPAN stands for IPv6 over Low Power Wireless Personal Area Networks. A key IP (Internet Protocol) based technology is 6LowPAN. Rather than being an IoT application protocol technology like Bluetooth or ZigBee, 6LowPAN is a network protocol that defines encapsulation and header compression mechanisms. The standard has the freedom of frequency band and physical layer and can also be used across multiple communications platforms, including Ethernet, Wi-Fi, 802.15.4 and sub-1GHz ISM.

H.   IEEE 802.11p

9.   This technology has been developed as amendment to IEEE 802.11 standard specifications in order to support ad-hoc communication between vehicles and between vehicle and infrastructure network. There are changes made to PHY (Physical) and MAC layers for the same. IEEE 802.11p is also known by names such as Wireless Access for Vehicular Environments (WAVE) and Dedicated Short-Range Communication (DSRC).

I.   802.11af (TVHT)

10.   IEEE 802.11af is a wireless networking standard that is designed for low-power, long-range wireless local area network (WLAN) operation for smart homes and IoT devices. It operates in the TV white space (TVWS) frequency range, employing unused TV spectrum at frequencies between 54 to 790 MHz for short periods of time. 802.11af utilizes cognitive radio techniques to provide an indoor range of a few hundred Meters and an outdoor range up to and beyond one Kilometer.

J.   Wi-SUN (Wi-SUN Alliance)

11.   Wi-SUN Alliance provides wireless mesh solutions for Field Area Networks for applications such as Advanced Metering Infrastructure and Distribution Automation, and for Home Energy Management. Wi-SUN has a range of around 0.7 km in city areas and 2-3 km in rural areas.

K.   Wi-Fi

12.   Wi-Fi is based on the IEEE 802.11 standards and is a trademark of the Wi-Fi Alliance. Wi-Fi operates at 2.4 GHz (12 cm) UHF and 5 GHz (6 cm) SHF ISM radio

bands. A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom.

13.   In Europe and Japan, channels 1, 5, 9, and 13 for 802.11g and 802.11n are used. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap. The 802.11a, 802.11b and 802.11g standards, called "physical standards" are amendments to the 802.11 standard and offer different modes of operation, which lets them reach different data transfer speeds depending on their range.

L.   LoRa

14.   LoRa is the physical layer or the wireless modulation utilized to create the long range communication link. LoRa is based on chirp spread spectrum modulation, which maintains the same low power characteristics as FSK modulation but significantly increases the communication range enabling a low cost commercial deployment. Chirp spread spectrum has been used in military and space communication for decades due to the long communication distances that can be achieved and robustness to interference and Doppler.

M.   SIGFOX

15.   In Sigfox system, low throughput transmissions combined with advanced signal processing techniques provide high link budget and highly effective protection against interference. Because of these characteristics, Sigfox system is particularly well adapted for low throughput IoT traffic. Sigfox LPWAN autonomous battery-operated devices send only a few bytes per day, week or

month in an asynchronous manner and without the needed for central coordination, which allows them to remain on a single battery for up to 10-15 years. Sigfox service operates in the ISM and SRD bands worldwide from 862 to 928 MHz.

N.   3GPP: Cellular technologies[36]

16.   3GPP introduced technologies like NB-IoT and LTE-M to address requirements of IoT applications, specifically focusing on long-battery life, low complexity since. NB-IoT and LTE-M have already been designed to address the requirements of the use cases, including requirements on support of large numbers of devices, low device cost, ultra-long battery life, and coverage in challenging locations, and these requirements still apply for Massive IoT in the 5G context. These technologies operate on licensed spectrum and historically have primarily targeted high-quality mobile voice and data services. Mobile network operators should be able to offer massive IoT applications in combination with enhanced mobile broadband (eMBB) and Critical-IoT services.

---

[36] https://tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf

LIST OF ACRONYMS

Acronyms	Description
ANT	Advanced Network Technology
AMC	Annual Maintenance Contract
API	Application Programming Interface
ARAI	Automotive Research Association of India
ATM	Automated Teller Machine
BIS	Bureau of Indian Standards
CAF	Customer Agreement Form
CDMA	Code-Division Multiple Access
CNPN	Captive Non-Public Network
3GPP	3rd Generation Partnership Project
5G	Fifth generation
DoT	Department of Telecom
E-KYC	Electronic- Know Your Customer
eMTC	Enhanced Machine-type communication
ESN	Electronic Serial Number
FTTH	Fiber to the Home
GCS	Group Communication Service
GSM	Global System for Mobile Communications
ICT	Information and Communication Technologies
IMARC	International Market Analysis Research and Consulting Group
IMEI	International Mobile Equipment Identity
IMT	International Mobile Telecommunications

IMWG	Inter-Ministerial Working Group
IoT	Internet of Things
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector
KYC	Know Your Customer
LAN	Local Area Network
LLP	Limited Liability Protection
LPWAN	Low Power Wide Area Network
LoRaWAN	Long Range Wide Area Network
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines
M2M	Machine To Machine
M2MSP	M2M Service Provider
MTCTE	Mandatory Testing and Certification of Telecom Equipment
NAN	Neighbourhood Area Network
NB-IoT	Narrowband IoT
NCIIPC	National Critical Information Infrastructure Protection Centre
NDCP	National Digital Communication Policy
NFC	Near Field Communication
NTC	National Trust Centre
OEM	Original Equipment Manufacturer
PAN	Personal Arae Network
PLC	Power Line Communication

POI	Point of Interest
POS	Point of Sale
QoS	Quality of Service
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TAN	Tiny Area Network
TEC	Telecommunication Engineering Center
TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UAS	Universal Access Service
UAV	Unmanned Arial Vehicle
UL	Unified License
UL-VNO	Unified License – Virtual Network Operator
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WAN	Wide Area network
WCDMA	Wideband Code-Division Multiple Access
Wi-Fi	Wireless Fidelity
Wireless HART	Wireless Highway Addressable Remote Transducer Protocol
Wi-SUN	Wireless Smart Utility Network
WLAN	Wireless-Local Area Network
WPAN	Wireless Personal Area Network