ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(03/2023)

DSTR-IoTM2M-Roaming

Roaming aspects of IoT and M2M including any related development and tariff principles

Technical Report ITU-T DSTR-IoTM2M-Roaming

Roaming aspects of IoT and M2M including any related development and tariff principles

Summary

This Technical Report addresses roaming aspects of the Internet of things (IoT) and machine-to-machine (M2M) communications. Following an overview of IoT/M2M communications, it discusses business models and policy challenges. The report also includes illustrative case studies from the European Union (EU), Republic of Korea, and India. This report encourages policymakers to support clear, harmonized light-touch regulatory frameworks that enable investments by the private sector.

By using the information in this report, Member States may consider various roaming business models in order to adopt an approach that suits them best and supports innovation and technology development in their respective jurisdictions.

Keywords

IoT, M2M, roaming.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1 of the ITU-T Technical Report on "Roaming aspects of Internet of Things (IoT) and machine-to-machine (M2M) communications" approved at the ITU-T Study Group 3 meeting held in Geneva, 1-10 March 2023.

Editor: Ena Dekanic
Federal Communications Commission
United States
Tel: +1 (202) 418 3628
Email: Ena.Dekanic@fcc.gov

Table of Contents

Technical Report ITU-T DSTR-IoTM2M-Roaming

Roaming aspects of IoT and M2M including any related development and tariff principles

1 Scope

This Technical Report addresses roaming aspects of Internet of things (IoT) and machine-to-machine (M2M) communications.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 Internet of things (IoT) [b-ITU-T Y.4000]: 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.

3.1.2 M2M communications [b-ETSI TR 102 725]: Refer to physical telecommunication based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

API	Application Programming Interface
ARPU	Average Revenue Per User
B2B	Business-to-Business
B2C	Business-to-Consumer
B2B2B	Business-to-Business-to-Business
B2B2C	Business-to-Business-to-Consumer
DOT	Department of Telecommunications
EC	European Commission
eSIM	embedded SIM
ETSI	European Telecommunications Standards Institute
eUICC	embedded Universal Integrated Circuit Card
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
KYC	Know Your Customer
LPWA	Low Power Wide Area
LTE	Long Term Evolution

LTE-M	Long-Term Evolution Machine-Type Communication
M2M	Machine-to-Machine
M2MSP	M2M Service Providers
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NB-IoT	Narrowband Internet of Things
OEM	Original Equipment Manufacturer
OTT	Over The Top
TEC	Telecom Engineering Center
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

5 Introduction

Over the last three decades, the Internet has had a significant impact throughout the world. Major changes have happened due to the increased usage of smart phones and devices and fast connectivity (e.g., use of Wi-Fi, LTE, 2G to 5G). Internet of things (IoT)/machine to machine (M2M) services are the next big leap in the world of the Internet that keeps the world connected with "things," i.e., any physical devices, vehicles, etc. which can be connected through sensors, embedded software, and network connectivity. The usage of these services is increasing at a lightning speed, contributing to the growth of businesses in various sectors such as healthcare, the automotive industry, and other industrial and consumer-based sectors.

Huge investments are being announced to develop these IoT/M2M based services in both developed and developing countries; according to some projections, there will be 4.3 billion IoT devices connected to cellular networks globally by 2026.

Looking at the demand and the need to create a global village driven by IoT/M2M, there is a need for global partnership in aligning the standards and regulatory requirements and cooperating in building efficient network-based infrastructure.

Supportive IoT policies must be based on the premise that the new business models for IoT and M2M differ greatly from the traditional business models that have supported the mobile phone and tablet industry segments in the past. Because of the diversity of solutions and potential providers of IoT and M2M applications, the best path forward is to encourage market entry and investment. Policymakers therefore are encouraged to support a clear, harmonized light-touch regulatory framework that would encourage investments by the private sector.

6 Overview of IoT and M2M communications

6.1 Common definitions of IoT and M2M (existing definitions)

As per [b-ITU-T Y.4000], IoT is defined 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." Through the exploitation of identification, data capture processing and communication capabilities, IoT makes full use of things to offer services to all kinds of applications while taking into account the need to comply with all applicable security and privacy requirements. M2M and IoT are usually interchangeable terms. However, M2M is only a subset of IoT and, as per [b-ETSI TR 102 725], M2M communications "refer to physical telecommunication-based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure."

IoT is therefore a network of physical devices embedded with sensors, software and other hardware, enabling devices to communicate with each other and to exchange the data over the network, while, M2M is a direct communication between devices either using wired or wireless communication channels. Hence, IoT is all encompassing because it not only includes the machine-to-machine communication but also human to machine communication, radio frequency identification, lab on a chip (LoC), etc.

6.2 Differences between IoT and M2M vs. traditional telecommunications services

Telecommunications has witnessed a sea change of transformation over the decades. Telecommunication services have aimed to break the barriers of distance/geography to connect people. This started with analogue communication services for voice services, followed by the sharing of data packets, followed by video. The present era is now moving from human-to-human communications towards machine to machine and machine to human communications.

Traditional telecommunication services differ from IoT/M2M services with respect to the following dimensions:

Connected elements and connections: Traditional telecommunications services connect people through phones and the connections are correlated with the number of people involved. However, in the case of IoT/M2M services, the devices play the major role as the connected elements and connections are established depending on the number of devices connected in the network.

Core service: The core purpose of traditional telecommunication services is focused upon the connectivity aspect (how well is it connected, and issues/concerns related to the same). Conversely, the core for IoT/M2M services is the connecting of applications and devices and their interconnections for the seamless functioning of said service.

Connectivity ARPU: Average revenue per user (ARPU) is the measure used in the telecommunications sector to track the amount of revenue generated per mobile phone user/customer. In terms of this measurement, the connectivity ARPU stands lower for IoT/M2M services than for traditional telecommunications services.

Business models: The business model for traditional services is business-to-business (B2B) or business-to-consumer (B2C), while for IoT/M2M services it also includes business-to-business-to-consumer (B2B2C) or business-to-business-to-business (B2B2B).

6.3 Different types of communications networks used

Diverse technologies are used to support the delivery of IoT, including mobile services and fixed-line communications. These technologies are used to offer both traditional telecommunications services (smartphones, tablets, etc.), as well as IoT services. Additionally, technologies such as long-term evolution machine-type communication (LTE-M) and narrowband Internet of things (NB-IoT) which are jointly termed low power wide area (LPWA) are used specifically to support the diverse functionalities required by IoT use cases. Cellular technologies have the advantage of ubiquities coverage at a relative low cost. In most countries, the vast majority of the country is covered with multiple cellular operators and, with the well-established roaming infrastructure in place, global IoT coverage can be enabled by mobile network operators (MNOs) with IoT roaming.

6.3.1 Cellular technologies (mobile services)

2G & 3G: 2G and 3G currently support nearly a billion connected devices. However, many mobile network operators have begun the process of sunsetting of either 2G or 3G (and sometimes both) to repurpose the spectrum for newer technology.

LTE/4G: LTE is the generation of cellular standard that followed 3G and it is what most people use today for mobile cellular data. IoT LTE devices are capable of faster speeds but typically require a constant power source or must be able to be recharged regularly.

LPWA: LTE-M and NB-IoT are two newer cellular technologies collectively referred to as low power wide area or LPWA. These technologies build upon LTE to meet the essential IoT requirements of battery life, reliable coverage, high network capacity and low operating cost. The main differences between the two are latency (the time it takes to get on a network and send a message) and speed (the amount of data transferred per second). NB-IoT, the slower of the two, is designed for things like static sensors, which have low data needs and do not need to be connected all the time. LTE-M exceeds the speed and latency of 2G but may not match 3G for speed. LTE-M is a good choice for fixed and mobile applications that benefit from lower latency and over-the-air updates.

5G: 5G networks are optimized to process huge volumes of changing data in real-time, a capability not possible with other technologies. Reliability and low-latency connectivity are key to enable critical IoT uses cases such as industrial devices and autonomous vehicles.

6.3.2 Other wireless technologies

Other non-cellular IoT communication technologies are used including satellite, Bluetooth, and Wi-Fi. Wi-Fi and Bluetooth have a role in consumer electronics, however, do not provide the ubiquitous coverage needed for many IoT use cases. Satellite can be used for IoT, however the terminal size cost and the relatively high service cost make it suitable only for specific applications. Satellite may also be used in the backhaul of a cellular network that is supporting IoT; for example, a cargo ship may use satellite connected cell sites on the ship to enable the tracking of shipping containers at sea. In this case the satellite is transparent to the IoT application.

6.3.3 Fixed-line technologies

Fibre and copper connectivity are also used for IoT applications where mobility of the IoT device is not required. Fibre connectivity provides large bandwidth, low latency, and low losses. It is also less prone to hacking and intrusion as compared to wireless technologies. Fixed connectivity is also suitable where electromagnetic interference could be an issue. In many applications, the fibre or the copper networks provide the backhaul up to the customer premises and connect to the IoT devices through Wi-Fi or ethernet interfaces. Smart homes, smart television, closed-circuit TV, and street lights in smart cities often use fibre connectivity. Fibre to the home, fibre to the machine/mast, fibre to the factory, fibre to the building, fibre to the office, and other similar configurations are increasingly being used for IoT applications with limited mobility requirements.

6.4 The drivers, inhibitors and challenges of IoT/M2M

IoT/M2M services are driven by technology advancements, decreasing costs and demands for efficiency. This could be facilitated by appropriate government policies promoting IoT/M2M, cost savings and new revenue opportunities.

Drivers affecting the growth of the technologies include evolving technological standards and enhancing network coverage, international commercial arrangements, and capacity of devices reconfiguration.

Inhibitors include policy and regulatory barriers.

Finally, challenges include privacy and security concerns, business models and investments, extraterritorial connectivity continuity and standards applied to the IoT environment.

6.5 Ecosystem including forecasts and an understanding of the delivery models for IoT/M2M

With the technological advancements fuelling the growth of IoT, the ecosystem for IoT/M2M keeps expanding with the addition and enabling of new "things" to be connected and used to provide services. The IoT ecosystem enables entities to connect and control their devices. According to researchers on this topic, "The conceptual model of Simon Fabri proposed in January, 2015 divides the connected ecosystem of things into industrial verticals and horizontal enablers. This denotes that there are essentially two types of players in this field: companies who provide the technology, services, infrastructure and other capabilities to allow a company to create a 'smart' experience; and new or established companies using these enablers to create new products or enhance in some way existing products or operations" [b-IoT Study].

Industry verticals: The industry verticals comprise all services and products offered to an end-user, and the whole bundle of industries that can benefit from IoT technologies [b-IoT Study].

Horizontal enablers: The horizontal enablers comprise all those technology and service elements required to make a smart connected system. They consist of key building blocks where smart systems connect physical devices to centralized computing centres. The sensors and devices interact with the physical world (e.g., fitness bands with heart monitors, motion sensors, proximity sensors, drones and robots) [b-IoT Study].

6.6 Value chain and the technology of IoT networks

The IoT value chain components fall under five broad categories: (1) hardware, (2) connectivity, (3) backend, (4) applications, and (5) users.

Hardware includes sensors, embedded chips, SIM cards, and similar devices. They capture the IoT data such as environmental parameters, industrial data, videos, etc. The data is captured either at pre-defined intervals or triggered by events such as outlier detection.

Connectivity components include the network terminal equipment, telecom or Internet network, and network service providers, etc. Connectivity is essential for transfer of data from the IoT devices to the backend and for command and control of the devices from remote locations.

Backend components include cloud storage, servers, application programming interfaces (APIs) for sharing data with third parties, data privacy and security components, analytics, etc.

Applications use the IoT data and add value. The data is either processed in real-time as in the case of autonomous vehicles or post-processed as for the training of artificial intelligence models.

Users include individuals, organizations, corporations, and governments that use or benefit from the data. Patients and doctors are users of a health-tracking system, a courier company is a user of a consignment tracking system, and citizens and governments are users of smart-city applications such as smart-traffic signals.

Multiple manufacturers, vendors, and service providers provide different value chain components. The stakeholders may be in various countries following different regulatory environments. Harmonization between all the stakeholders is essential for seamless working and exponential growth of IoT.

7 Business models for IoT and M2M roaming

As previously mentioned, the business model for traditional telecommunications services is B2B or B2C, while for the IoT/M2M services it also includes B2B2C or B2B2B. In the energy sector, smart metering increases business efficiencies and decreases operational expenses for energy companies; transportation tracking solutions improve route optimization and safety for vehicles on the road; and the healthcare industry is also looking into improvement of patient care through near real-time device communications, remote monitoring, and disease management.

Among industry verticals benefitting from the M2M paradigm, the automotive industry has historically been the largest. Other industry verticals employing M2M principles include healthcare, finance, transport, utilities, insurance, retail, security, logistics, construction, government, and education.

8 Policy challenges facing IoT and M2M roaming

Roaming models for IoT will have to accommodate the "things" pertaining not just to the home or domestic ecosystem but also to the global locations where the services are extended. In such scenarios, the regulatory environment consists of multiple entities and authorities. In a traditional telecommunications environment, the connectivity providers such as telecom service providers and Internet service providers function in accordance with applicable telecom rules and regulations. However, for IoT/M2M, the entities/authorities are not just telecom operators, but also non-communications companies providing products and services across differing sectors such as healthcare, automotive industry, energy, transportation, etc. that may be subject to additional or different rules and regulations in those sectors. Hence, the regulations lack uniformity.

This creates barriers to the growth of IoT/M2M and needs to be addressed to convert them into drivers for facilitation of the seamless development and deployment of IoT/M2M services.

Some of the policy issues/challenges that have to be addressed are described below:

Connectivity issues:

- Usage of multiple networks within the territory is essential to connectivity anywhere, but the regulatory positions vary within the countries. Therefore, policy and regulatory approaches towards improvement of connectivity should be encouraged.
- The IoT ecosystem requires streamlining of its devices such as sensors and devices using common language and standards of implementation. This lack of standardization in the common architecture for interoperability needs to be addressed to build an efficient IoT ecosystem.
- IoT/M2M is ever expanding with the inclusion of many devices and applications that have to be uniquely identified, which requires proper and efficient numbering plans.
- To facilitate the growth and development of IoT services, as well as to mitigate unnecessary demand for numbering resources, permanent M2M roaming, commercial agreements with mobile virtual network operators (MVNOs), device reconfiguration and the extraterritorial use of national numbering resources for IoT services constitute connectivity alternatives.

Privacy and security issues:

- IoT/M2M also deals with the transfer of data across the ecosystem. When data comes into the picture, increasingly stringent privacy and security regulations constrain the growth of the IoT/M2M.

Regulatory issues:

- Regulatory issues (e.g., related to subscriber registration and taxation) also impact the growth of IoT/M2M.

8.1 Roaming models

International mobile roaming is essential for the operations of Internet of things (IoT) devices and contributes to the success of machine-to-machine (M2M) platforms [b-Luti1]. With "Internet of everything," the issue of data transmission and consequently the international roaming charges become a problem of paramount importance for billions of varied devices in different economic sectors. High roaming tariffs set barriers in many areas of the regional integration, and in the near future such barriers would hamper growth in promising areas of the digital economy.

In this context, one issue that arises is the regulation of permanent roaming. While there is no common definition of what exactly is understood by "permanent roaming", and views vary, so do interpretations regarding its regulatory standards impact on the operation of the IoT/M2M services.

There is an understanding that constraints on permanent roaming, which affect the use of data internationally, introduces challenges to global device deployment [b-Zervaki]. On the other hand, in the few countries where permanent roaming is prohibited, this may be due to several reasons such as, taxation obligations, local compliance and registration requirements, revenue and commercial aspects, sectoral monitoring, and competition issues. These perspectives are outlined respectively below.

8.1.1 Permanent roaming

The variety, scope and number of IoT applications has been growing exponentially. Central to that growth, on a global basis, is the use of the permanent M2M roaming model, which has been at the forefront of delivering IoT services to corporate enterprise customers. This model is the most efficient method of scaling global connectivity (via roaming agreements) and enables IoT devices to be connected in virtually every country around the globe. Furthermore, permanent roaming allows global customers' services and applications to operate on multiple MNO networks in each country, which creates opportunities to drive down prices and improve coverage. Using the permanent roaming model, a manufacturer in its home country could enter into a telecommunications services agreement with a local MNO, using the local MNO's IoT global platform, international mobile subscriber identity (IMSI), etc. Such a MNO would use its roaming agreements with its roaming partners globally, to deliver the wireless connectivity to its customers' devices around the world. This model drastically streamlines the cost and complexity of a global customer's ability to provide or to use IoT services in nearly every country. Integrating into multiple MNO IoT platforms requires significant costs to be incurred for each platform, but the permanent roaming model, by utilizing the existing roaming integration and having a single IoT platform integration, drastically reduces delivery costs to the original equipment manufacturer (OEM) and its customers and increases IoT applications and services within a country.

Alternatively, in a scenario where permanent roaming is not allowed, manufacturers looking to export their devices to foreign countries would be compelled to enter into separate service relationships with at least one licensed MNO in each country where they wish to sell their devices. That would introduce contracting and compliance complexity by having to enter into such agreements with multiple MNOs (and be required to use multiple IoT platforms) in each country to gain the reach afforded by M2M roaming. In addition, they would be required to anticipate national market demand and identify before or during manufacture, when the IMSI is installed in the device, the specific country where each device would be sold, so that the corresponding MNO IMSI could be activated on the correct IoT platform. This, in turn, would require the maintenance of SIM inventories for multiple countries. For customers who seek to distribute products in 100 or more countries, by requiring several IoT platform integrations, the inability to use the permanent roaming model would increase platform integration costs and jeopardize the business case for the majority of typical IoT global applications. Without the use of permanent M2M roaming a global customer could face a logistics challenge in attempting to wirelessly enable its devices and an increase in operational complexity to manage and collect data in global markets.

8.1.2 Other models

With the understanding that there are not only a wide variety of IoT applications that come with each unique set of challenges and requirements [b-Luti1], but also a large range of connectivity solutions, it can be argued that there is no "one size fits all" solution when it comes to determining an entity's access and availability to connectivity solutions [b-Deloitte]. Some alternatives are:

- *Commercial arrangements:* One of the most popular commercial arrangements for MNOs is a standard roaming bilateral agreement, where the two involved parties determine the terms and conditions of their collaboration [b-Luti1]. Global coverage can be provided through roaming agreements with usage of mobile virtual network operators (MVNOs), which are "specialized service platforms providing worldwide device connectivity by leveraging already existing infrastructure of MNOs", technically deployed using the IP exchange network (IPX) [b-Geissler] [b-Lutu2].
- *Capacity of devices reconfiguration:* Opting for a multiple international mobile subscriber identities (Multi-IMSI) approach, in which the SIM card on the device has multiple profiles from multiple operators, can allow connection in multiple territories [b-Transforma]. One of the most recent solutions is the embedded SIM (eSIM) (subscriber identity module or subscriber identification module, or embedded universal integrated circuit card (eUICC)), that can "proactively update the SIM profile on your device to select a local profile, or other appropriate one, [which] can guarantee connectivity as if it were a local SIM" [b-Deloitte] [b-Transforma] [b-Rimli].

Additionally, other market dynamics and technological improvements related to this topic include:

- Developments that are likely to be relevant to competition in roaming in the medium term, include developments which enable end-users to bypass roaming such as Wi-Fi and over the top (OTT) services, developments which facilitate entry into the roaming segment such as eSIM, and new generation technologies such as 5G, VoLTE and RCS, which affect the nature of roaming products and require renegotiation of existing agreements.
- Traditional mobile network operators are considered likely to continue to play the most significant role in the provision of international roaming connectivity in the medium term. However, new IoT/M2M services and business models alongside entry enablers such as eSIM are expected to increase the scope for new players or types of players to gain a foothold in markets for cross-border data connectivity. The main beneficiaries seem likely to be mobile virtual network operators and aggregators. Device manufacturers and verticals are also likely to play an increasingly important role as they look to bundle connectivity or provide interfaces or options for connectivity into their offers to consumers.

9 Case studies for regulatory frameworks of IoT/M2M communications

Regulations and policies are ever-present in the world of electronic communications and are necessary to ensure fair competition, to protect the end-users, and to sustain the development of technology. With the advent of M2M communications, which can be seen as a basis for building IoT, the question of regulating or not regulating this area becomes inescapable. On one hand, it is argued that, at the moment, there is no need to create specific regulations, since the technology is not yet mature and inappropriate policies could hinder development and innovation and interfere with its natural evolution.

On the other hand, the concept of "everything connected" raises new challenges, in particular regarding data use and sharing, ethics, or privacy and security that might not be addressed by existing legislation. Furthermore, the highly varied nature of M2M and IoT applications makes it difficult to develop a one-size-fits-all framework.

9.1 EU

Based on the findings of a public consultation, another study by the European Commission (EC) made recommendations on potential policy options, which could advance the development of IoT while being consistent with European regulation objectives [b-EC]. In particular, three possible levels for a regulatory framework are evolving:

- No change with respect to the current ICT regulation;

- Soft law to provide guidance by using non-legislative measures; and
- Hard law to enforce regulation policies by explicit legislation.

The "no change" alternative implies that no specific intervention should be made by the EU regarding the M2M market. Such de-regulation would allow the market to define the evolution of the sector, without setting boundaries that could restrain the potential of future applications.

"Soft law" would involve, among other considerations, monitoring M2M development, supporting research and innovation in areas with high socio-economic impact (e.g., health care, smart grids), participating in standardization bodies, and providing active support to industry.

However, some areas may require stricter regulation, beyond "soft law," which lacks accountability or enforcement methods. Notably, with M2M applications, concerns regarding data privacy, security and third-party sharing will be brought outside the virtual world and into everyday life through interaction with "smart" devices.

9.2 Republic of Korea

The IoT ecosystem consists of various operators with different functions and a basic function is to covey signals over a network dedicated to M2M communications. As it is in general regarded as a virtue to keep low regulation at the entry stage for the development of new services, the question naturally arises as to whether the entry regulation for IoT service providers should be applied in the same manner as the traditional telecommunications services. Such a question should be more valid to countries where the definition of IoT services overlap or do not clearly discern with that of traditional telecommunication services.

As reflected in "Article 6 of the Telecommunications Business Act of 2018" shown below, in 2018, Korea amended its Telecommunication Business Act which requires that every facility-based telecommunications service provider register before starting business. However, there exists a proviso which may allow IoT/M2M service providers to start business without delay by simply reporting to the Minister, instead of registration. The proviso requires, amongst other features, the service to use telecommunications services in an ancillary manner; that is, the provision of goods or services must be possible even if the function of using telecommunications services is removed from the goods or services. The proviso further requires the ancillary use of telecommunications services is restricted to transmit or receive data only, excluding videos and voices.

Telecommunications Business Act of 2018, Article 6 (Registration of Facilities-Based Telecommunications Business)

(1) A person who intends to operate the facilities-based telecommunications business shall file for registration (including registration through an information and telecommunications network) with the Minister of Science and ICT after satisfying the following requirements, as prescribed by Presidential Decree: Provided, That where a person uses ancillary facilities-based telecommunications services and imposes fees for use thereof as prescribed by Presidential Decree, while providing his or her own goods or services (the same shall apply where the usage fees are included in the price for such goods or services), he or she shall file a report on the facilities-based telecommunications business; and where a person who has filed a report on the business, provides other facilities-based telecommunications services, he or she shall file for registration under the main sentence:

1. Financial and technical capabilities;
2. Plans for protecting users;
3. Business plans and other matters prescribed by Presidential Decree.

(2) Where completing registration of the facilities-based telecommunications business under clause (1), the Minister of Science and ICT may place necessary conditions to facilitate fair competition, protect users, improve service quality, and efficiently utilize information and telecommunications resources. In such cases, details of such conditions shall be published in the Official Gazette or posted on the website.

(3) Only corporations shall file for registration prescribed in clause (1)

(4) The requirements and procedures for filing for registration under clause (1) or (2) and other necessary matters shall be determined by Presidential Decree.

9.3 India

The Government of India has identified that M2M/IoT is one of the fastest emerging technologies across the globe, providing enormous beneficial opportunities for society, industry, and consumers. It is being used to create smart infrastructure in various verticals such as power, automotive, safety and surveillance, remote health management, agriculture, smart homes, Industry 4.0, Smart Cities, etc. using connected devices. M2M communication is going to play a major role and will contribute significantly towards the Government of India's initiatives in this regard.

In order to strengthen the M2M ecosystem and to facilitate wider proliferation and innovation in the sector, the following actions have been taken recently:

- In February 2022, the Department of Telecommunications issued "Guidelines for Registration Process of M2M Service Providers (M2MSP) and WPAN/WLAN Connectivity Providers for M2M Services" [b-DoTIndia1]. Applicants need to register themselves to provide SIM and WPAN/WLAN-based M2M communication. This will help in addressing concerns like connectivity with telecommunication service providers, "know your customer", traceability, and encryption. Registration will be carried out at DOT field offices spread across the country.
- New licenses for M2M have been introduced and accordingly the licensing guidelines were amended in January 2022. Though the existing access service providers were already enabled to provide connectivity to M2M/IoT networks, through the new licenses, an independent category of service providers has been enabled to create, operate and provide a network for interconnection of M2M/IoT devices. In this license, applicants can apply for

different categories such as Category A (pan-India), Category B (state area) and Category C (district area) [b-DoTIndia2].

- To have additional availability of spectrum for M2M/IoT applications, one megahertz additional spectrum was added in the earlier unlicensed 865-867 MHz band, making it 865-868 MHz. The radiated power, channel bandwidth and duty cycle have also been defined for different use cases.

In addition, the Department of Telecommunications (DOT) of India had taken the following actions in the M2M/IoT domain in the past to facilitate the burgeoning M2M industry:

- Released a 13-digit numbering plan exclusively for M2M/IoT devices connected through mobile networks.
- Defined features of the SIMs used only for M2M communication services and related KYC instructions for issuing M2M SIMs to entity/organizations providing M2M communication under bulk category.
- Permitted use of eSIMs by allowing MNOs to configure them over the air. This has enabled availability of sufficient numbering resources and led to a robust framework for a mobile M2M ecosystem in the country.
- Important parameters for a large-size M2M networks are scalability, interoperability and efficiency. To support such deployments, the Government of India has adopted international standards set by the OneM2M Alliance, and Release 2 standards were adopted in January 2020 as national standards through the Telecom Engineering Center (TEC), the technical wing of the Government of India.
- TEC, India's standard setting organization, also released recommendations on IoT/M2M security in January 2019 [b-DoTIndia3] and a Code of Practice for Securing Consumer IoT in August 2021 [b-TECIndia]. Both these documents suggest ways to have safe and secure IoT deployments.

The Government of India expects the above regulatory enablement for M2M services to reduce cost, enhance productivity, provide faster response time, optimize resource consumption, and increase revenue for businesses leading to ease of living for the common citizens.

10 Challenges and ways forward for IoT/M2M communications

The following suggestions can be identified at this moment:

Connectivity concerns: Standardization in the direction of special handling or optimization of the network for M2M specific services will lead to better support of M2M communications.

Security and privacy concerns: There is the requirement of discovering, filtering, and interpreting relevant information, while maintaining a generic character (e.g., creating a level of abstraction in which data cannot be linked to specific individuals or devices).

Regulatory concerns: A challenge lies within the regulatory domain, particularly in defining what type of data can be shared or brokered by the owners of IoT/M2M applications.

While for commercial services (e.g., consumer electronics, logistics), the owners of the IoT/M2M platform should retain full ownership of data, there are applications where this data becomes of public or national interest (e.g., smart metering, smart cities). These are IoT/M2M service deployments in which a public sector (government) entity is the IoT/M2M customer. In this latter case, the challenge is enforcing separation between commercial data and publicly available data.

11 Concluding remarks

Reflecting on technological advancements and their contribution towards the growth of IoT/M2M services, it can be inferred that IoT/M2M is ever expanding and needs attention to grow to meet the technological advancements in this Internet era. IoT currently comprises partial, overlapping or competing technical solutions and platforms within the various vertical business domains based on existing industry standards. As such, IoT/M2M services face numerous inhibitors in seamless growth with complete utilization of the technological advancements. The modularity of IoT will play a major role in the development of the IoT industry and the ecosystems since IoT links not just the technologies and systems together, but also the various vertical and horizontal applications pertaining to various sectors. From a global perspective, IoT/M2M services are viewed with increasing enthusiasm as the IoT/M2M roaming business models are developed that explore opportunities (e.g., a lowering of costs, an increase in profits, etc.) in the respective sectors.

To conclude, it is essential for every country to share the information on the major drivers and address the inhibitors that are constraining the growth of the IoT/M2M services. Member States may consider various roaming business models in order to adopt an approach that suits them best and supports innovation and technology development in their respective jurisdictions.

Bibliography

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ETSI TR 102 725] ETSI TR 102 725 – V1.1.1 (2013), *Machine-to-Machine communications (M2M); Definitions*.

[b-Deloitte] Deloitte (2018), *The Future of Connectivity in IoT Deployments.* Deloitte Blog: Internet of Things. https://www2.deloitte.com/de/de/blog/internet-of-things-blog/2019/the-future-of-connectivity-in-iot.html.

[b-DoTIndia1] Department of Telecommunications of India (2022). *Guidelines for Registration Process of M2M Service Providers (M2MSP) and WPAN/WLAN Connectivity Providers for M2M Services.* https://dot.gov.in/latestupdates/guidelines-registration-process-m2m-service-providers-m2msp-and-wpanwlan-connectivity.

[b-DoTIndia2] Department of Telecommunications of India (2022), *Guideleines for Grant of Unified License*. https://dot.gov.in/sites/default/files/UL%20guidelines%20with%20M2M%20without%20INSAT%20MSS%20R%20dated%2017012022_0.pdf.

[b-DoTIndia3] Telecom Engineering Center of India (2019), *Technical Repoort: Recommendations for IoT/M2M Security*. https://www.tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20IoT%20M2M%20Security.pdf.

[b-EC] European Commission DG Communications Networks, Content & Technology (2014), *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*.

[b-Geissler] Geissler, S., Wamser, F., Bauer, W., Krolikowski, M., Gebert, S., & Hoßfeld, T. (2021), *Signaling Traffic in Internet-of-Things Mobile Networks*. 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 452–458. https://ieeexplore.ieee.org/abstract/document/9463958.

[b-IoT Study] B. Jekov, E. Shoikova, P. Petkova, and D. Donchev (2017), *Study on the IoT Ecosystem Business Models and the Segment of Startups.*

[b-Luti1] Lutu, A., Jun, B., Finamore, A., Bustamante, F. E., & Perino, D. (2020), Where Things Roam – Uncovering Cellular IoT/M2M Connectivity. *Proceedings of the ACM Internet Measurement Conference*. https://doi.org/10.1145/3419394.3423661.

[b-Lutu2] Lutu, A., Jun, B., Bustamante, F. E., Perino, D., Bagnulo, M., & Bontje, C. G. (2020), *A First Look at the IP Exchange Ecosystem*. ACM SIGCOMM Computer Communication Review, 50(4), 25–34. https://doi.org/10.1145/3431832.3431836.

[b-Rimli] Rimli, P. (2020), *One eSIM (eUICC) for Multiple Countries: How to Expand Your Business with IoT Connectivity eSIM – Use Case: From Switzerland to China*. Swisscom. https://ict.swisscom.ch/2020/12/one-esim-euicc-for-multiple-countries-how-to-expand-your-business-with-iot-connectivity-esim-use-case-from-switzerland-to-china.

[b-TECIndia] Telecom Engineering Center of India (2020), *Code of Practice for Securing Consumer Internet of Things (IoT)*. https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf.

[b-Transforma] Transforma Insights (2021), *Position Paper: Using Permanent Roaming for Your Internet of Things Deployment Risks Huge Costs and Continuity of Service Problems*. Transforma Insights. https://transformainsights.com/blog/permanent-roaming-headache.

[b-Zervaki] Zervaki, M. (2020), *Tech Policy Trends 2020 | What is Next for IoT Regulation?* Access Partnership. https://www.accesspartnership.com/tech-policy-trends-2020-what-is-next-for-iot-regulation.