Consultation Paper No. 9/2022

Telecom Regulatory Authority of India

Consultation Paper

on

Embedded SIM for M2M Communications

New Delhi, India

25th July 2022

Mahanagar Doorsanchar Bhawan

Jawahar Lal Nehru Marg

New Delhi – 110 002

Written Comments on the Consultation Paper are invited from the stakeholders by 22nd August 2022 and counter-comments by 05th September 2022. Comments and counter-comments will be posted on TRAI's website. 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.

For any clarification/information, Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), TRAI, may be contacted at Telephone No. +91-11-23210481.

CONTENTS

Chapter	Topic	Page No.
Chapter 1	Introduction	**1**
Chapter 2	Policy, technical aspects, and issues of Embedded SIM for M2M communications	**19**
Chapter 3	Issues for Consultation	**45**

ANNEXURES

Annexure I	Reference from DoT	**47**
Annexure II	Global Scenario for M2M/Consumer eSIM Subscription Models	**52**

CHAPTER 1
INTRODUCTION

1.1 The Department of Telecommunications (DoT), through its letter dated 9th November 2021 **(Annexure-1)**, has informed the following to the Telecom Regulatory Authority of India (TRAI):

- *SIMs for the purposes of M2M communication are embedded (integrated/ soldered) at the point of manufacturing in order to achieve the standard physical and environmental requirements and are deployed in domestic or international market. Today, there are different solutions (proprietary and GSMA) in the market to allow a SIM Card to be re-provisioned over-the-air with a new Service Provider, avoiding the MSP lock-in.*
- *DoT had issued instructions dated 16th May 2018 permitting the use of eSIM with both single and multiple profile configurations with Over-the-Air (OTA) subscription update facility, as per prevailing global specifications and standards (GSMA).*
- *There are various issues involved in deployment of embedded SIM.*

DoT has also attached a brief, consisting of background of eSIM and issues involved, along with its reference letter dated 9th November 2021.

1.2 In view of the above, DoT through its afore-mentioned letter dated 9th November 2021, under the terms of clause 11 (1)(a) of TRAI Act, 1997 as amended by TRAI Amendment Act 2000, has requested TRAI to provide its recommendations for holistic deployment of eSIM in Indian Telecom Network including implementation mechanism under different profile configurations and switchover of profiles by TSP's.

1.3 As a background, it needs to be mentioned that the eSIM is an eUICC (Embedded Universal Integrated Circuit Card) chip on the circuit board of an electronic device with a cellular connection. Two eSIM models, based

on two different types of use cases, have been standardized by the GSMA: the first is for M2M/Internet of Things devices, which is called Machine to Machine eSIM and the second is for end-user consumer devices. Machine-to-Machine (M2M) communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. This technology permits billions of devices to connect over the internet giving rise to an unprecedented number of new applications, services, and business opportunities in various verticals.

1.4 The International Telecommunication Union (ITU-T)[1] has defined Internet of things (IoT) as "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, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled".

1.5 M2M technology is creating significant opportunities and has a proven potential of revolutionizing the performance of various verticals of different sectors, businesses, and services, by providing automation and intelligence to the end devices. With the ability to tap into a device's data stream on an ongoing basis, it is possible to track and service a device throughout its entire lifecycle from the assembly line to the recycling heap, leading to a redefinition of customer relationships and business operations. Further, these devices have the feature of Over-the-Air Profile Management resulting in overall cost cutting by upgrading software and features of these devices remotely. In all, M2M technology has the potential to unleash significant productivity gains and economic growth, unlike any previous technology wave.

[1] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items

M2M Ecosystem

1.6 The M2M Ecosystem broadly consists of the following entities:

1.6.1 **Device Manufacturer/Provider:** The device provider is responsible for devices providing raw data to the network provider and application provider according to the business model. This category will encompass the M2M chip-set manufacturer, the M2M module manufacturer and the end device manufacturer (e.g., a Car or an Air Conditioning manufacturer) who integrates the M2M module in his device).

1.6.2 **Connectivity/ Network Provider:** The network provider/ operators are the connectivity providers who own the underlying network to provide connectivity and related services for M2M Service providers.

1.6.3 **M2M Service Provider (MSP):** M2M SP provides M2M services to third parties using telecom resources. DoT has issued guidelines on 8th February 2022 for the 'Registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services'[2].

1.6.4 **M2M Application Provider:** It is an entity that realizes the service logic of an M2M Application and utilizes capabilities/resources provided by the network provider, device provider and M2M service provider, to provide M2M applications to end users.

1.6.5 **End user:** Individual or company who uses an M2M solution.

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

M2M Applications and Examples

1.7 Some of the verticals and related M2M applications as per industry are given in the table below:

Industry/ Vertical	M2M Applications
Automotive/ Transportation	Vehicle tracking, e-call, V2V & V2I applications, Traffic control, Navigation, Infotainment, Fleet management, Asset tracking, Manufacturing, Logistics, etc.
Utilities/Energy	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 & Surveillance	Women Safety Bands, Commercial and home security monitoring, Surveillance applications, Fire alarm, Police/medical alert, etc.
Financial/ Retail	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.

M2M Communication Technologies

1.8 M2M communications refers to the technologies that allow wired/wireless systems 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.

1.9 Based on communication networks, the communication technologies used for M2M Communications can broadly be classified into:

1.9.1 Fixed & Short-Range Technologies (RFID, Bluetooth, Zigbee & Wi-Fi)

1.9.2 Long Range Technologies:

- Non-3GPP Standards (LPWAN): LoRaWAN, Sigfox etc.
- 3GPP Standards: LTE-M, NB-IoT, 5G.

1.10 **Fixed & Short-Range Technologies**

1.10.1 **RFID:** RFID sensors are Radio Frequency Identifiers embedded in the device. According to the RFID Journal the technology is "any method of identifying unique items using radio waves. Typically, a reader communicates with a transponder that holds digital information in a microchip". This technology relies on being within a close range. Warehousing inventories depend heavily on RFID to keep internal stock control for example.

1.10.2 **Bluetooth:** The very popular Bluetooth technology is a global wireless standard enabling convenient and secure connectivity for an expanding range of devices and services. It was designed to enable communication between devices and not the networking between many devices as other technologies (like Wi-Fi) aim to do. Bluetooth mostly serves as a substitute for data cables. It is available in most of the current devices. It is used to establish point to point connection. The IoT/ M2M has embraced Bluetooth 4.0 (also called Smart, LE or Low Energy) as it ~~is~~ has greatly improved in power consumption over the classic Bluetooth technology while maintaining a similar communication range. The Bluetooth Special Interest Group (SIG), the standards organization that oversees the development of Bluetooth standards and the licensing of the Bluetooth technologies,

explains its main advantage by stating that it "collects data and runs for months or years on a tiny battery". Many modern wearable and other connected devices use Bluetooth LE to connect to data hubs, mobile devices, or computers.

1.10.3 **Zigbee:** ZigBee is a wireless mesh technology developed as an open standard to address the unique needs of low-cost and low-power wireless M2M networks. It uses digital radios based on IEEE 802 standard for home area network with a focus on monitoring, control, and sensor application. It is targeted at applications that require a low data rate, long battery life, and secure networking – for example in wireless switches, electrical meters, lighting control, smart energy, HVAC control, health monitoring and so on.

1.10.4 **Wi-Fi:** Wi-Fi proliferation is on the rise in India. Home networking devices may also use Wi-Fi wireless LAN connections by using technology under 802.11 IEEE standards. A wireless network can be used for communication among many electronic devices, to connect to the Internet or to the wired networks that use Ethernet technology.

1.11 Long Range Technologies: Non-3GPP Standards

1.11.1 **RF Module Based (LPWA) Communication:** LPWAN technologies have been designed to transmit very low amounts of data (such as meter readings, sensor data from pollution devices etc.) to large distances. LoRa and SIGFOX technologies have been developed and are being deployed globally. Their range can go beyond 10 km in open area and devices can have a battery life of up to 10 years. LoRa and SIGFOX usually use unlicensed frequency bands worldwide in Sub-GHz.

1.11.1.1 **LoRa:** LoRa is the physical layer, or the wireless modulation utilized to create the long-range

communication link. LoRa is based on CHIRP (Compressed High Intensity Radar Pulse) spread spectrum modulation, which maintains the low power characteristics but significantly increases the communication range enabling a low-cost commercial deployment.

1.11.1.2 **SIGFOX:** In the Sigfox system, low transmissions combined with advanced signal processing techniques provide a high link budget and highly effective protection against interference. Sigfox is based on Ultra Narrow band modulation. Sigfox devices send only a few bytes per day, week, or month in an asynchronous manner and without the need for central coordination, which allows them to remain on a single battery for up to 10-15 years.

1.12 Long Range Technologies: 3GPP Standards: LTE-M, NB-IoT, 5G

1.12.1 **LTE-M:** LTE-M is the simplified industry term for the LTE-MTC low power wide area (LPWA) technology standard published by 3GPP in the Release 13 specification. It specifically refers to LTE CatM1, suitable for the IoT. LTE-M is a low power wide area technology which supports IoT through lower device complexity and provides extended coverage, while allowing ~~the~~ reuse of the LTE installed base. This allows the battery life to last as long as 10 years or more for a wide range of use cases.

1.12.2 **NB-IoT:** Narrowband-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity, and spectrum efficiency, essentially in deep

coverage. Battery life of more than 10 years can be supported for a wide range of use cases.

1.12.3 **5G:** 5G is the fifth-generation cellular technology that revolutionizes ~~the~~ connectivity and enables use cases such as enhanced Mobile Broadband (eMBB), Massive Machine to Machine-Type Communications (mMTC), and ultra-reliable low latency communications (URLLC) in conjunction with new capabilities such as Artificial Intelligence (AI), Cloud Computing, Edge Computing, and the Internet of Things (IoT). AI, Cloud computing and Edge computing will help handle the data volumes generated by IoT, as 5G boosts network capability. mMTC supports extremely high connection densities, enabling industrial-scale IoT. In this scenario, 5G will be able to connect with a million sensors and devices per square kilometer. It will enable usage scenarios such as smart homes, smart energy/utility applications, smart agriculture, smart logistics, smart city, etc.

1.13 **Subscriber Identity Module (SIM) based M2M Communication**

1.13.1 Devices with M2M SIM cards can send and receive data across cellular networks. In IoT devices, the M2M SIM may share data directly with other devices and with the software that manages the platform. Therefore, the terms “M2M SIM” and “IoT SIM” are often used interchangeably**.** M2M SIMs operate using the same wireless cellular networks, but they offer benefits over the traditional mobile SIM cards such as:

- Durability- Long serviceable life even in harsh conditions
- Remotely Manageable through Over-the-Air (OTA) mechanism.
- Advanced functionality- Focuses on efficiency, reliability, and hardware longevity.

1.13.2 Different form factors of SIM cards:

- **Full-Size (1FF)** is the largest M2M SIM card, about the size of a credit card. It has been phased out in most of the cases by smaller modern SIMs.

- **Mini-SIM (2FF)** is the industry standard SIM card size, measuring 25mm x 15mm x 0.76mm. It's typically used in devices like vehicles, vending machines, and payment points.

- **Micro-SIM (3FF)** is half the size of the mini and is used in portable devices like tablets, GPS, mHealth, and other mobile IoT devices.

- **Nano-SIM (4FF)** is 40% smaller than the micro variation, making it great for small IoT devices. These SIMs have relatively little protection, so they're not recommended for harsh environments.

- **Embedded SIM (MFF2)** also known as eSIMs, measure only 6mm x 5mm x 1mm. The embedded SIM or eSIM is soldered directly to the device's motherboard, so it is fully encased in the device. That means it is a suitable choice for IoT devices deployed outdoors or in harsh conditions. For large-scale deployments, choosing an eSIM can also simplify the supply chain because it removes the step of physically installing a SIM in every device.

- **Embedded UICC (eUICC):** eUICC stands for **embedded Universal Integrated Circuit Card** (eUICC). It refers to the software component of eSIM that runs on a UICC and provides the capability to store multiple network profiles that can be

provisioned and managed Over-the-Air (OTA). There is often confusion around the term eSIM, as many people use it to refer to eUICC-enabled eSIMs. But the eSIM itself is simply- what it claims to be - an embedded SIM and does not automatically enable remote provisioning. More IoT designers are starting to embrace eUICC-enabled eSIMs because of their versatility and flexibility.

1.13.3 **eUICC:** The fundamental feature of eUICC technology is Over-the-Air (OTA) remote SIM provisioning. At present, both proprietary and GSMA-compliant subscription management solutions are available in the market[3]. Proprietary eSIMs are developed and deployed on the market by some of the largest device manufacturers or groups of mobile operators. Being an OEM's proprietary solutions, they work only in a closed and isolated environment. They are also incompatible with any other Subscription Management system in terms of eSIM interoperability or back-end infrastructure integration. GSMA-compliant solutions are developed in compliance with GSMA's Embedded SIM Remote Provisioning Architecture. It is supported by around 800 communication service providers all around the world and facilitates full interoperability for M2M/IoT devices.

1.13.4 The GSMA-compliant subscription solutions are available as two separate variants for **M2M** (SGP.01, SGP.02 & SGP.11) and **Consumer** (SGP.21, SGP.22, and SGP.23) devices. The M2M segment includes industrial IoT devices like sensors, trackers, cellular modules, meters, and other industrial non-end-user devices. The consumer segment includes consumer electronics devices like smartphones, wearables, laptops, and tablets.

[3] https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=39256199&file=2719-270219-eSIM.pdf

DoT Guidelines/Instructions on M2M Communications

1.14 Vide its letter No. 16-05/2013-AS-III/Vol.II/133/481 dated 09.12.2016, DoT has approved the 13-digit numbering scheme for SIM based M2M devices which will result in a capacity of 50 billion M2M SIMs in India. It has been implemented from 01st October 2018. The structure of 13-digit numbering scheme is:

Country Code 2 digits (+91)	M2M Identifier 3 digits	Licensee Identifier 4 digits (10000 blocks)	Device Number 6 digits (1 million)

1.15 The restrictive feature for M2M SIMs as mentioned in the para 4 of the DoT instructions dated 16th May 2018 were as follows:

"*…such SIMs will have restrictive features compared to traditional SIMs for voice/ data communications used for person to person (P2P) communication as mentioned below:*

a) *Outgoing / Incoming calls shall be allowed to maximum one (1) number only.*
b) *Likewise outgoing/ incoming SMS shall be allowed to / from predefined set of maximum two (2) numbers only.*
c) *Data communication shall be allowed only on maximum two (2) numbers of predefined Public IP addresses/ URL with fixed APNs or equivalent technology options by Licensee.*
d) *These restrictions are not applicable to calls made to emergency numbers like police, fire, ambulance, etc"*

1.16 DoT has issued following instructions dated 30th May 2019 regarding relaxation of the above restrictive feature for M2M connections.

"…. The restrictive feature for M2M SIMs as mentioned in the para 4 of the DoT instructions dated 16.05.2018 was replaced as:

a) *Outgoing / Incoming calls shall be allowed to maximum four (4) numbers only.*
b) *Likewise outgoing / incoming SMS shall be allowed to / from predefined set of maximum four (4) numbers only.*
c) *Data communication shall be allowed only on maximum four (4) numbers of predefined Public IP addresses/URL with fixed APNs or equivalent technology options by Licensee.*
d) *These restrictions are not applicable to calls made to emergency numbers like police, fire, ambulance, etc"*

1.17 DoT has issued instructions dated 16th May 2018 permitting the use of eSIM with both single and multiple profile configurations with Over-the-Air (OTA) subscription update facility, as per prevailing Global specifications and standards (GSMA).

On 17th January 2022, DoT has introduced a separate authorization under Unified License (Chapter XVI) on M2M for providing M2M connectivity including LPWAN connectivity to M2M Service providers.

1.18 DoT has issued the guidelines for 'Registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services' vide its letter No. 4-10/2015-NT dated 08th February 2022.

1.19 DoT has constituted two Committees, viz., M2M Policy Reform Committee & M2M Consultative Committee, for implementation of actionable items w.r.t. M2M as per National Digital Communication Policy-2018 and other reforms vide its letter No. 4-8/M2M Roadmap/2015-NT dated 16th February 2022.

Issues Highlighted by DoT

1.20 The brief background and the issues highlighted by DoT in its annexure to the reference letter dated 9th November 2021 are as below:

1. Background:

a. The embedded SIM is a form factor that is physically integrated into the device, mostly by soldering to the device Printed Circuit Board (PCB). The embedded SIM cannot be easily removed in the field. As a result, the embedded SIM requires remote provisioning, which is the ability to remotely select the SIM profile deployed on a SIM without physically changing the SIM card. This technology is standardized and can be implemented on a SIM card with any form factor. The term eUICC is used to represent a SIM card that can be remotely provisioned.

b. SIMs for the purposes of M2M communication are embedded (integrated/soldered) at the point of manufacturing to achieve the standard physical and environmental requirements and are deployed in domestic or international markets.

c. Today, there are multiple solutions (proprietary and GSMA) in the market to allow a SIM Card to be re -provisioned Over-the-Air with a new Service Provider, avoiding the MSP lock-in.

d. At present there are two technical options being discussed for M2M services to allow remote provisioning of IMSIs i.e., Soft-SIM and Embedded SIM. The first approach termed as 'Soft-SIM' has not been widely accepted by the industry due to certain security concerns required to be addressed. The second approach termed as 'embedded UICC' (eUICC) has been adopted and approved by GSMA.

e. The GSMA Embedded SIM specifications were developed specifically for the M2M market where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical.

f. GSMA specifications issued on eUICC provide a single, de-facto standard mechanism for the remote provisioning and management of M2M connections, allowing the "over-the-air" provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another.

g. The GSMA has approved the architecture and the technical specification documents for remote provisioning that could be deployed by the MNOs for M2M applications. Using this approach, the eUICC keeps all the security features of a regular UICC while adding the capability to securely provision a new 'profile' containing all the data required (including the IMSI) to represent a mobile subscription. The update of embedded UICC is made via over-the-air (OTA) technique. The GSMA documents describe the procedure for changing the eUICC profiles.

h. GSMA specifications refer for third party to manage and switch over of eSIM profile. Suitable mechanism in this regard needs to be prescribed for the TSP's.

2. TRAI recommendations related to eSIM: TRAI vide its letter No. 103-3/2016-NSL-II dated 5th September 2017 gave recommendations on various aspects of M2M. These include:

a. Devices with pre-fitted eUICC should be allowed to be imported only if it is able to get reconfigured 'Over-the-air' (OTA) with local subscription. GSMA approved guidelines shall be followed for provisioning of new profiles remotely with 'Over-the-air' (OTA) mechanism.

b. Devices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within the stipulated period or on

change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition based on the developments and requirements.

c. Country specific relaxation on permanent roaming of foreign SIMs, if any, can be considered based on the strategic importance, Bi-lateral or Multilateral trade agreements and principle of reciprocity by the government.

d. In case imported equipment to which the SIM/ device is fitted with such as automobile/ machines (like earth movers), arms etc. (requiring mandatory registration at local authorities such as RTO, State/District administration) is transferred/sold to another party before three years, the roaming device (eUICC) shall also be immediately configured with local subscription/eUICC of Indian TSP. The KYC details of the new owner/buyer must be compulsorily updated in the database of concerned authorities.

e. It should not be mandatory to use only domestically manufactured SIMs in M2M. Embedded SIMs with standard specifications can be imported and relevant information shall be submitted by importer while import of the devices/SIMs.

3. DoT instructions: DoT has issued instructions dated 16th May 2018 permitting the use of eSIM with both single and multiple profile configurations with Over-the-Air (OTA) subscription update facility, as per prevailing global specifications and standards (GSMA).

4. Issues Involved:

a. There are variances of eSIM in the market where multiple active profiles are being demanded by the industry. AIS-140 guidelines issued by the Ministry of Road transport & Highways (MoRTH) in the Automobile sector is one such example. In such cases, a third party is managing which profile will be active at what time and its location.

b. Some operators requested DoT:

i. That ITU allocated 901.XX MCC be recognized by DoT, as it is recognized globally by telecom standardization bodies like GSMA, BREC, ARCEP-France etc.

ii. That 901.XX MCC should not be treated as foreign IMSI range, as it is a non-geographic code with customized agreements with local licensed operator.

iii. That 901.XX MCC should not be considered in violations to national telecom policies, as it is specifically for IoT use cases and will never be used as consumer telecommunications.

iv. That 901.XX MCC should be considered as innovative service in telecommunication and should not be under strict telecom restrictions, as it does not use any national scarce resource.

v. That ITU is also allocating numbering series, which are not country specific, and shall also be permitted to use in India.

c. If scenarios in point b above are to be activated with Indian mobile operators, then probable issues faced would be: -

- *The mobile operators will be using IMSI or the numbering series which have not been allotted to them.*

- *There is no Inter-circle/Intra-circle roaming available to these connections.*

d. In case any business entity wishes to take VNO license and provide services as per point b above, probable issues faced by them would be:

i. The mobile operators will be using IMSI and may be numbering series which has not been allotted to them.

ii. There is no Inter-circle/ Intra-circle roaming available to these connections.

iii. Such operators are not allowed to have connectivity from multiple TSP.

e. The challenges mentioned above are applicable in case DoT enforces the TRAI recommendation as mentioned at point 2.b.

f. DoT is also getting references for TSP's communicating with SM-SR located in foreign countries certified as per GSMA standards. Comments are required for such use cases also.

g. An embedded SIM card (eUICC) cannot be manually replaced with a local SIM which implies that the M2M device will be connected to the visited mobile network as a roaming device. Taking control of M2M device activities and effectively detecting roaming devices in the network are among the list of challenges if operators want to optimize network performance and reduce operational and signaling costs.

h. Various IoT solution enabler who are not a network connectivity provider itself aggregates agreements with existing cellular networks which connect any device through cellular networks. Regulatory mechanisms for such aggregators need to be devised.

1.21 In view of the above background, DoT, through its letter dated 9th November 2021, has sought the recommendations of TRAI for holistic deployment of eSIM in Indian Telecom Network including implementation mechanism under different profile configurations and switch over of profiles by TSP's.

1.22 In this regard, additional inputs were requested from DoT vide letter dated 10th December 2021. DoT has given its response vide letter dated 26th May 2022. In its response, DoT has forwarded the copies of the representations received from stakeholders highlighting the issues related to eSIM profiling and associated issues, which DoT has already covered in its reference letter.

1.23 For drafting this consultation paper, various documents available in the public domain, published by government agencies/departments, telecom regulators in many countries, research agencies/institutions, academic institutions, telecom vendors, operators, and international agencies/forums etc. were referred to make the consultation paper balanced and comprehensive. Excerpts from certain documents, which had domain relevance, are also included in this Consultation Paper, wherever necessary.

1.24 The consultation paper is divided into three chapters. This Chapter deals with the Introduction and Background of the Consultation Paper. Chapter 2 deals with the Policy and Technical aspects of embedded SIM for M2M communications and various issues involved for the same. Chapter 3 summarizes the issues for consultation.

CHAPTER 2
POLICY AND TECHNICAL ASPECTS OF EMBEDDED SIM FOR M2M COMMUNICATIONS

2.1 Removable SIM cards are often inaccessible within M2M wireless modules making it difficult if not impossible to change the SIM once deployed. An embedded SIM, which is a programmable SIM card embedded directly into the device, never needs to be removed and new operator profiles are simply downloaded to the SIM when required. The Embedded SIM Specification simplifies logistical processes such as installation of a single SIM Stock Keeping Unit into an M2M device at the point of manufacture and download of an appropriate operator profile in the destination country for that device. It also removes the need for stock control and shipping of physical pre-provisioned SIM cards. All this operational flexibility is delivered with no compromise on security.

2.2 The **eUICC** is a form factor that is physically integrated into the device, mostly by soldering to the device's Printed Circuit Board (PCB) and cannot be removed or swapped from one device to another, unlike the traditional SIM cards. As a result, the embedded SIM requires Remote Profile Management (RPM) Over-the-Air (**OTA**) apart from the software update. RPM is the ability to remotely select the SIM profile deployed on a SIM without physically changing the SIM card. It may almost replace traditional SIM cards in mobile phones and tablets as it is possible to change operator on eUICC by merely rewriting the integrated SIM to new software settings.

2.3 eUICC has been adopted and approved by GSMA. The Telecommunication Engineering Center (TEC), in its TEC IR No. TEC/IR/WS/ESM-101 /01/MAR-19, also mentions GSMA SGP.02 Remote Provisioning Architecture for eUICC Technical Specification Version 3.2 on 27th June 2017, as an applicable standard for M2M SIM[4]. The GSMA eUICC

[4] https://tec.gov.in/public/pdf/GRMT/TEC-IR-WS-ESM-101-01-MAR-19.pdf

specifications were developed both for **Consumer SIM and M2M SIM** market where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical.

eUICC for M2M Communications

2.4 The GSMA eSIM solution for M2M devices targets Industrial M2M and IoT devices, including cellular modules, sensors, trackers, meters, and many other components, all applied in an industrial and non-end-user interactive environment. This solution serves the needs of business-to-business customers in the B2B2C channels, specifically on the Internet of Things (IoT) market. Remote SIM Provisioning for M2M utilizes a server-driven (push model) to provision and remotely manage operator Profiles. Here, end-user interaction is not necessary or desirable.

2.5 GSMA specifications issued on eUICC provide a single, de-facto standard mechanism for the remote provisioning and management of M2M connections, allowing the "over-the-air" remote provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another. The GSMA has approved the architecture and the technical specification documents for remote provisioning that could be deployed by the TSPs for M2M applications. Using this approach, the eUICC keeps all the security features of a regular UICC while adding the capability to securely provision a new 'profile' containing all the data required (including the IMSI) to represent a mobile subscription. The update of eUICC is made via OTA technique.

2.6 The GSMA document "SGP.01 Embedded SIM Remote Provisioning Architecture"[5] defines a common global architecture framework to enable the remote provisioning and management of the eUICC in M2M devices.

[5] https://www.gsma.com/esim/resources/sgp-01-v4-1-pdf/

Another GSMA document, "SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification"[6], provides a technical description of the eUICC architecture as well as the interfaces and security functions used within the Remote Provisioning Architecture.

2.7 **M2M eUICC Ecosystem**: It consists of various inter-related entities, viz. the eUICC, the eUICC Manufacturer (EUM), the M2M Device Manufacturer, the Mobile Network Operator (MNO), M2M Service Provider (M2M SP) and Certificate Issuer (CI) and associated network elements i.e., Subscription Management-Data Preparation (**SM-DP**) and Subscription Management-Secure Routing (**SM-SR**). The network elements, namely SM-DP and SM-SR provide the remote subscription management functions. Profile management is governed by Policy Rules that are contained in the Operator's Profile and in the SM-SR. Policy Rules are controlled by the operator and enforced by the eUICC and SM-SR on behalf of the Operator.

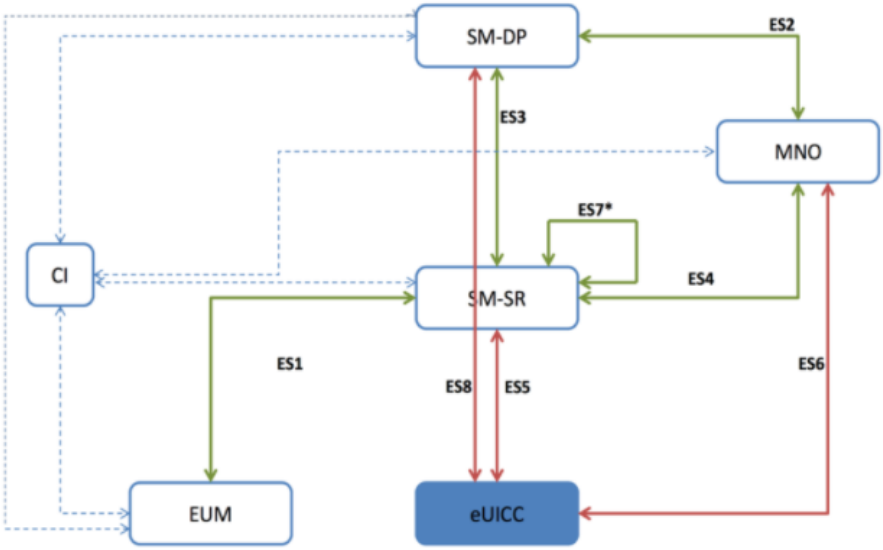

Figure: M2M eSIM (Main System Elements) [Source: GSMA]

[6] https://www.gsma.com/esim/resources/sgp-02-v4-1-pdf/

2.8 M2M eUICC Ecosystem: Roles of the Entities

2.8.1 **eUICC:** The eUICC is a discrete hardware component in a standardized ETSI Form Factor. It can contain one or more Profiles, of which only one shall be enabled at any point in time. Ownership of the physical eUICC can change throughout its lifetime.

2.8.2 **eUICC Manufacturer (EUM):** The EUM is a supplier of the eUICCs and the resident software, who fabricates the physical eUICC hardware. It is responsible for the initial cryptographic configuration and security architecture of the eUICC. The EUM delivers eUICCs containing a Provisioning Profile and/or one or more Operational Profiles to the M2M Device manufacturer. It also issues eUICC certificates to authenticate and certify the eUICC to other entities (viz., SM-DP, SM-SR). The EUM production site must be SAS-UP (Security Accreditation Scheme for UICC Production) certified. This is a well-established scheme through which UICC and eUICC manufacturers subject their production sites and processes to a comprehensive security audit. The GSMA has developed the auditing standards, requirements, and methodologies for SAS in collaboration with SIM suppliers and world-class security auditing companies.

2.8.3 **M2M Device Manufacturer:** The Device Manufacturer builds M2M devices which comprise a communication module and an eUICC containing at least one Provisioning Profile or Operational Profile that is enabled. It also prints the eUICC Identification (EID) on the Device. The Device manufacturer can select any certified eUICC and order it in the necessary quantity directly from the EUM. Thus, it buys connectivity from the TSP, buys eUICCs from the EUM, solders eUICC into end device and markets the resulting product.

2.8.4 **Operator:** It is a company providing wireless cellular network services. It selects at least one SM-DP, and has a direct interface to

the SM-SR. The operator owns the Profile and thus defines the Policy Rules to control the Profile management. The selected operator initiates the download of a particular Profile to an eUICC subject to current Policy Rules. It will receive confirmation of the successfully completed download and installation of the Profile. The enabled operator can use an OTA Platform to manage the content of its enabled Profile in the eUICC.

2.8.5 **Subscription Manager -Data Preparation (SM-DP):** The SM-DP is part of Operator Network, and it acts on behalf of the operator to serve any approved eUICC. It builds Personalized Profiles for the targeted eUICC and installs them on the eUICC through the SM-SR. Further, the SM-DP prepares, stores, and protects operator profiles and tracks all imported and known subscriptions. The SM-DP must be GSMA SAS-SM (Security Accreditation Scheme for Subscription Management) certified.

2.8.6 **Subscription Manager -Secure Routing (SM-SR):** The SM-SR may obtain the Platform Management Credentials of the eUICC from the EUM (in case of initial registration) or establish them through the previous SM-SR. (in case of SM-SR swap). It loads, enables, disables, and deletes profiles on the eUICC in accordance with the Operator's Policy Rules. It maintains a secure connection between SM-DP and eUICC for the delivery of profiles. It holds a database of all the eUICCs under its control and the key sets used to manage them. eUICCs delivered by the EUM should always be registered to only one SM-SR at a particular instant**.** It can be changed during the lifetime of the eUICC via SM-SR swap. The SM-SR shall be GSMA SAS-SM certified.

2.8.7 **M2M Service Provider (M2M SP):** M2M SP relies on an Operator providing the Profiles on the eUICC. Using Profile Lifecycle Management Authorization (PLMA), the Operator may provide an interface to the M2M SP in order to allow it to manage the Operator's

profile. Thus, the M2M-SP may have a direct interface to the SM-SR to manage those profiles for which PLMAs have been set by the Operator. It may also act as a third party that hosts the SM-SR.

2.8.8 **Certificate Issuer (CI):** The Certificate Issuer issues certificates for eUICC remote provisioning system entities and acts as a trusted third party for the authentication of the entities of the system. It provides certificates for the EUM, SM-SR, and SM-DP. Only eUICC manufacturers, and SM-SR and SM-DP hosting organizations that have successfully been accredited by the GSMA SAS can apply for the necessary certificates from the GSMA Certificate Issuer to participate in the GSMA approved ecosystem. To name a few, Cybertrust and Digicert are two CI agencies[7].

2.9 eUICC Profile Creation

A Profile comprises the operator data related to a subscription, including the operator's credentials. The Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under license. The eUICC can accommodate multiple SIM Profiles. This Profile needs to be remotely downloaded, installed, and activated so that the device is able to connect to an operator's network. This process consists of two steps, namely Bootstrap Profile Creation and Operational Profile Creation.

2.9.1 **Bootstrap Profile Creation:** Bootstrap profile is needed for configuring the eUICC. This is a Profile which, when installed on an eUICC, enables access to communication network(s). It enables an M2M device to access a mobile network only for the purpose of management of Operational Profiles on the eUICC. It contains one or more Network Access Applications and associated Network Access Credentials. Initially, the OEM signs an MoU with an Operator for obtaining mobile network connectivity. It requests the

[7] https://www.gsma.com/esim/gsma-root-ci/

Operator for the Bootstrap Profile. At the same time, the OEM also signs an MoU with the EUM for obtaining eUICCs. Once the Operator sends the Bootstrap Profile to the OEM, it forwards the same to the EUM. The Bootstrap Profile can only be personalized by the EUM. The EUM thus burns the Bootstrap Profile and the eUICC certificate onto the eUICC. At initial switch on of the eUICC, this Bootstrap Profile on this eUICC provides connectivity for the M2M device, which allows the Operator the ability to download and activate an Operational Profile.

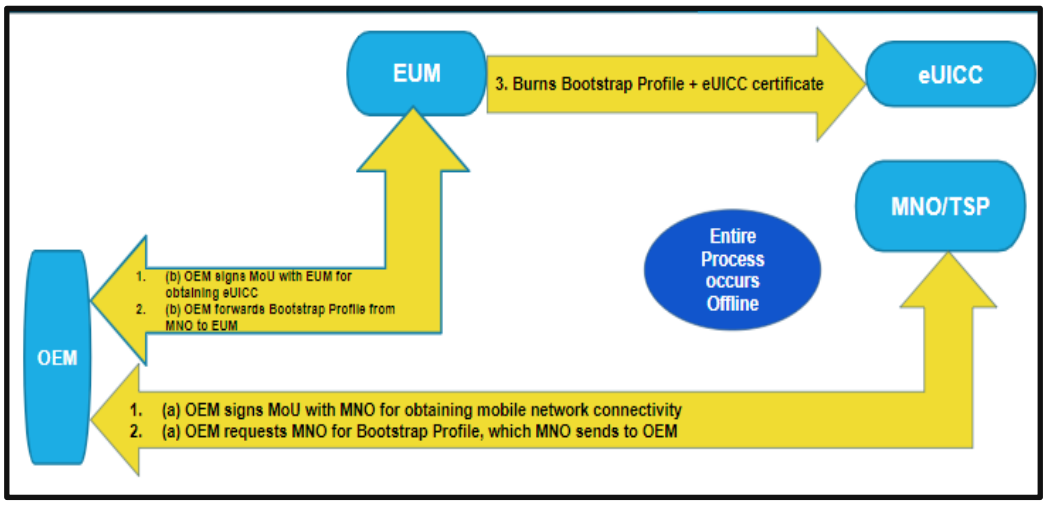

Figure: Bootstrap Profile Creation

2.9.2 **Operational Profile Creation:** The Operational Profile enables the device to access a mobile network for operation. It contains one or more Network Access Applications, associated Network Access Credentials, Operator's (e.g., STK) applications and third party applications. At first, the SM-DP receives a Profile Description from the Operator. The Profile Description is the description of a Profile in a format specific to the Operator, e.g., Excel table, xml format and plain text. The SM-DP then creates Un-personalized Profile accordingly, with the help of the EUM. Next, the Operator provides certain input data (IMSI, etc.) to the SM-DP. The SM-DP generates Personalization Data for the targeted eUICC (e.g., Network Access Credentials and other data) based upon input data from the

Operator. It finally builds Personalized Profiles for the targeted eUICC and installs it on the eUICC through the SM-SR.

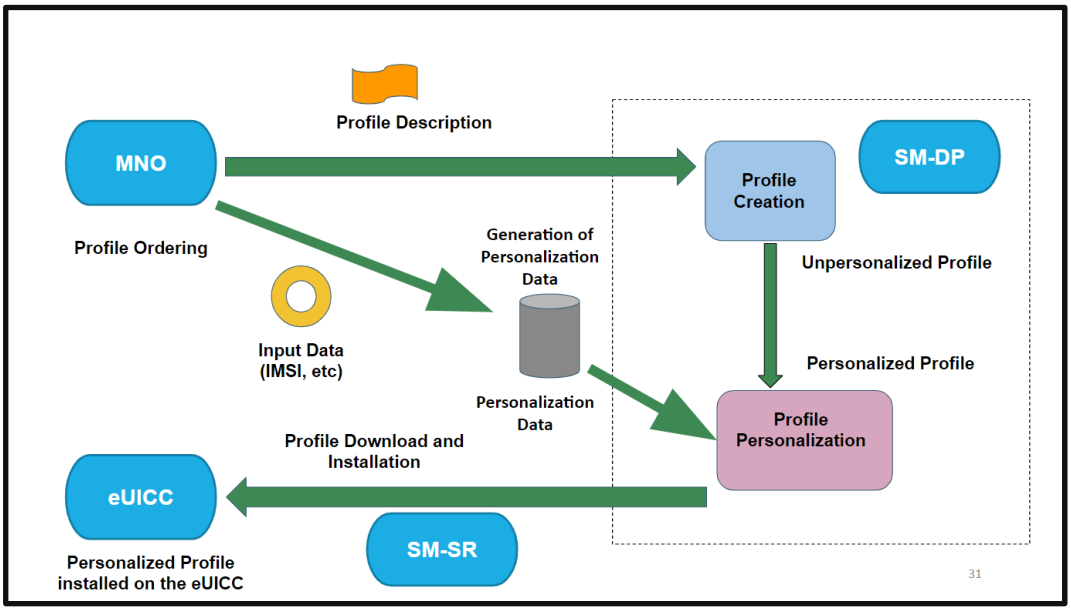

Figure: Profile Creation, Ordering and Personalization

SM-DP and SM-SR Ownership- Various Models

2.10 The GSMA specifications provide ample flexibility as far as the ownership of SM-DP and SM-SR are concerned. This gives rise to various use case models in which the Telecom Operator, the OEM or the M2M SP are responsible for management of the SM-DP and/or SM-SR. Three such key scenarios are examined ahead, in which the SM-SR can either be hosted by Telecom Operator, OEM or M2M-SP. In each case, the SM-DP is with the Operator.

2.10.1 **SM-SR Managed by Operator:** In this model, each Operator provides its own SM-DP and manages its own Profile via its SM-SR. When an OEM contracts with a single mobile network operator, say Operator 1, it provides a pre-installed bootstrap profile. After a period, if the OEM decides to change the contract from Operator 1 to Operator 2, the Operators swap their own SM-SR. SM-SR1 sends all eUICC data to SM-SR2, and new keys are established between SM-SR2 and eUICC. In this case, the SM-DP

and SM-SR may be physically located within the data center of the operator's country. Alternatively, the SM-DP and SM-SR may be provided by a third-party hosting the server in a different country as the operator. In this model, full control of the provisioning system by the operator minimizes the risk of any potential security issues.

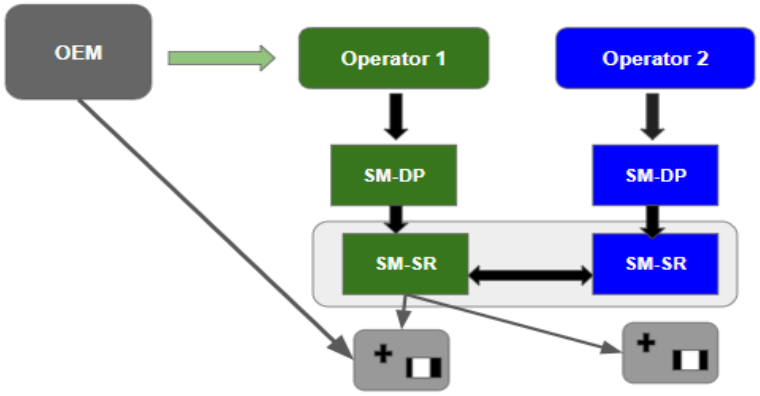

Figure: SM-SR managed by each Operator

2.10.2 **SM-SR Managed by OEM:** In this model, each operator provides its own SM-DP and manages it via a common SM-SR hosted by the OEM. The SM-SR handles the Enable, Disable, or Delete operations based on the MoU between the OEM and TSP. While one of the operators provides a pre-installed Bootstrap profile, the OEM contracts with a number of mobile network operators to achieve global coverage. Here the SM-DP may be physically located within the data center of the operator's country or provided by a third-party hosting the server in a different country as the operator. However, the SM-SR must be physically located within the data center of the OEM's country. In this case, the OEM has direct control on post-activation management of the TSP profile, including swapping and deletion of the profile.

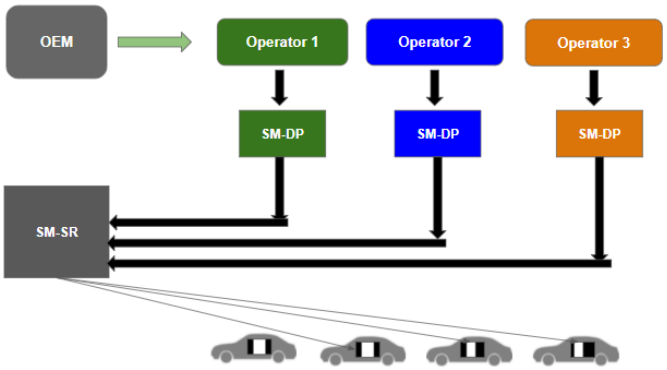

Figure: SM-SR managed by OEM

2.10.3 **SM-SR Managed by M2M Service Provider (M2MSP):** In this model, each operator provides their own SM-DP to create their own profile and manages it via a common SM-SR hosted by the M2MSP. The M2MSP obtains the Profile Lifecycle Management Authorization (PLMA) from concerned operators to perform Profile Lifecycle Management. Here the M2M SP acts as a single point of integration between OEM, EUM, and end-user. The OEM needs to send Bootstrap Activation requests as well as Commercial Activation requests to the M2M SP along with valid supporting documents, post which activation is done in a few working days. The M2M SP carries out Network Switches in real-time network coverage, and the OEM does not have an interface to view the data[8].

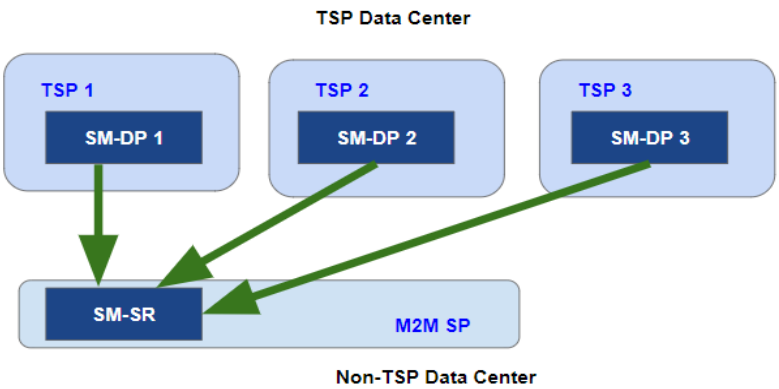

Figure: SM-SR managed by M2M SP

[8] https://sensorise.net/customer-engagement-panel/faqs/

2.11 Global scenario for M2M eSIM Subscription Models leads to the fact that in most of the countries, the eSIM manufacturers are maintaining SM-DP and SM-SR, but in some countries the Network Operators and M2MSPs are also doing the same. The Global scenario of eSIM Subscription Models is provided in Annexure-II.

M2M Device Deployment: Different Scenarios

2.12 With regards to the location of the device with pre-fitted eUICC, there may be three (3) distinct scenarios, as follows:

2.12.1 **Scenario 1- Device manufactured in India and deployed within India:** In this case, the SM-DP and SM-SR will be in India and SM-SR can either be with the OEM or the mobile Operator or M2M SP.

2.12.2 **Scenario 2- Device Imported into India for deployment:** Following phases are involved for deployment once the equipment manufactured by a foreign OEM, pre-fitted with an eUICC, is imported in India.

2.12.2.1 **Roaming Agreement:** The relevant foreign Connectivity Provider (say, TSP-F) initially enters into a Roaming Agreement with an Indian TSP (say, TSP1). As per TRAI recommendation dated 5th September 2017, *"Devices fitted with eUICC should be allowed to operate in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The*

Authority/Licensor shall review the condition later based on the developments and requirements".

DoT has yet to issue any guidelines/instructions in this regard.

2.12.2.2 **SM-DP Integration:** Next, in order to mandatorily convert/ reconfigure the eUICC into Indian TSP's SIM within the stipulated period or on change of ownership of the device, whichever is earlier, the SM-DP of TSP-1 has to be integrated with SM-SR of TSP-F to download the former's local profile onto eUICC. However, the control over the eUICC still remains with the foreign SM-SR.

2.12.2.3 **SM-SR Swap:** To establish a full control on the eUICC by an Indian entity, **SM-SR swap** must be conducted between the foreign SM-SR and the Indian SM-SR.

2.12.2.4 **SM-SR Integration:** Now, after the completion of SM-SR swap process (between foreign SM-SR and Indian SM-SR), if the OEM (Indian subsidiary) wants to avail the services of another Indian TSP (say TSP-2 in India), the Profile of TSP-2 can be downloaded by SM-DP of TSP-2 onto the eUICC through SM-SR of TSP-1. For this purpose, **SM-SR integration** is must, i.e., SM-SR of TSP-1 must be integrated to SM-DP of TSP-2.

2.12.3 **Scenario 3 - Device manufactured in India and exported abroad:** It will be similar to the Scenario 2. However, regulation of the importing country will apply.

Examination of Issues

2.13 **Issue 1:** TRAI has earlier recommended that the foreign eUICC fitted devices may be permitted to be on roaming with Indian TSP's network for a maximum period of three years only, within which the eUICC should mandatorily be configured with Indian TSP's profile. The TRAI recommendation is under consideration of DoT and currently no timelines have been prescribed by DoT in this regard. The recommended timeline of maximum three years from the date of activation of roaming may be considered to be reviewed as it is considered too long by some stakeholders. In view of above, the stakeholders are requested to comment on the following question:

Q1. Whether the TRAI recommended timeline, about the foreign eUICC fitted devices to be on roaming with Indian TSP's network for a maximum period of three years only, needs a review? If yes, what should be the timeline after which the eUICC should mandatorily be configured with Indian TSP's profile?

2.14 **Issue 2:** At present, foreign eUICC fitted devices may be imported, with the possibility to download local subscription profiles for local regulatory requirements. The foreign eUICC needs to be registered with the local network to be able to swap the profile using subscription management technology as per GSMA global guidelines. In the case of foreign eUICC fitted devices coming to India, the Indian TSP's profile may be downloaded to eUICC as per timelines prescribed by the Government. This is done through the integration of SM-DP of Indian TSP with SM-SR of foreign TSP. While the profile of Indian TSP is getting added to the eUICC, control of the eUICC remains with the foreign SM-SR. For having control over the eUICC by the Indian TSPs, controlling SM-SR should belong to Indian TSPs, which can be done through SM-SR swap. Currently, SM-SR swap is not taking place, after SM-DP of an Indian TSP is integrated to SM-SR of foreign TSP. That is, the profile of an Indian TSP is getting added to the eUICC, but

control of the eUICCs is remaining with the foreign SM-SR. This raises security and privacy concerns due to sharing of sensitive data such as device location etc. with foreign SM-SR. One option may be that as soon as an Indian TSP's profile is downloaded onto eUICC through foreign SM-SR, there should be SM-SR swap. There is a need to examine the SM-SR swap between foreign TSP and Indian TSP. In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question:

Q2. Whether there is a need to change the controlling SM-SR from the foreign agent (TSP/non-TSP) to Indian TSP in case of foreign eUICC fitted devices operating in India? If yes, what should be the methodology and time period within which it should be done?

2.15 **Issue 3:** For the eUICC working under the control of SM-SR of a particular TSP in India, it is possible to download the profile of another TSP on the eUICC through GSMA prescribed OTA profile subscription mechanism. This can be done only when the SM-SR of each TSP is integrated with SM-DP of other TSP. At present SM-SR integration is missing among Indian TSPs, i.e., SM-SR and SM-DP of the TSPs are not integrated among each other. Without this integration, the profile of a new TSP cannot be added to an eUICC. In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question:

Q3. Whether there is a need for the SM-SR of each TSP to be integrated with the SM-DP of other TSPs? If yes, what should be the methodology for integration? Please specify the timelines also.

2.16 **Issue 4:** Considering the case in which the device is manufactured and used within India, a situation may arise in which an OEM wants to entirely discontinue with the services of the current TSP (whose SM-SR is currently controlling its eUICC), and switch to another TSP. This will require an SM-SR swap from the existing TSP to the other TSP. To make this possible,

there may be a need to mandate TSPs for carrying out SM-SR swap, as per request of device manager (OEM). In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question:

Q4. Whether there is a need to prescribe SM-SR swapping among the Indian TSPs? If yes, what should be the modalities and procedure for such a swap?

2.17 **Issue 5:** Presently, switching from one TSP to another is based on contractual agreements between TSPs and OEM. The device end-user cannot initiate switchover in case of dissatisfactory consumer experience. It is desirable to explore the possibilities whether the switchover from one TSP to another can be made user-driven, besides OEM-driven. In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question

Q5. Whether the profile switchover, from one TSP to another, is driven by the user or OEM? If yes, what methods can be deployed to execute such switchover?

2.18 **Issue 6:** As per global practices, SM-SR is owned and managed by either a TSP or an OEM or a third party (such as M2M Service Provider). Currently in India, there are no prescribed guidelines on this issue and for domestically issued eUICC, the SM-SR is being owned and managed by TSPs. There is a need to explore the possibilities about owning and managing SM-SR by a third party, which may be non-TSP entities, such as OEMs and M2M Service Providers. In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question:

Q6. Whether non-TSP entities, such as OEMs and M2M Service Providers, should be permitted to own SM-SR and manage the subscribed profiles

for their devices? If yes, what should be the methodology and procedure?

Global IMSI ranges for supporting IoT and M2M Connectivity

2.19 A SIM card contains various information such as Integrated Circuit Card Identifier (ICCID), International Mobile Subscriber Identity (IMSI), Personal Identification Number (PIN), and Authentication Keys. The IMSI is a string of decimal digits, up to a maximum length of 15 digits, which identifies a unique subscription. The IMSI consists of three fields: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN).

2.20 901.xx is a global IMSI series without ties to any country, thus providing network-agnostic, cross-border connectivity at a single price, thus helping manufacturers to build equipment in any part of the globe and deploy anywhere. Global SIMs have traditionally been used for Maritime and Aerospace connectivity for both satellite and cellular connectivity. They assist in emergency communication in the wake of disaster.

- '901' is the Mobile Country Code (MCC), assigned and administered by ITU.

- 'xx' is the Mobile Network Code (MNC), assigned and administered by ITU-TSB.

2.21 A written request for obtaining 901.xx IMSI must be submitted to the director of the ITU-TSB. The same has been assigned to 91 entities between 1999 and 2021[9].

[9] https://www.itu.int/net/ITU-T/inrdb/e212_901.aspx

2.22 Demand for global connectivity for the Internet of Things (IoT) and Machine-to-Machine (M2M) applications is motivating an increasing number of IoT and M2M players to apply for ITU-allocated 'global IMSI ranges'. Global International Mobile Subscriber Identity (IMSI) ranges are signified by the shared Mobile Country Code '901', a code without ties to any country.

2.23 Using non-geographic Mobile Network Code (901.XX), the IoT and M2M players can enter into connectivity access agreements with local MNOs (Mobile Network Operators) in each country. Although the technical set-up is built on top of GSMA standardized roaming framework (as it is cost effective), these Unilateral Connectivity Access Agreements are usually tailored for the IoT use-cases, and it may be different from bilateral International Roaming Agreements. The agreements can be customized based on the local MNO's terms and conditions suitable to local market and regulations.

2.24 DoT in its reference letter has mentioned the request of stakeholders for the use of ITU allocated shared Mobile Country Code 901.XX (Global IMSI) for M2M Communication. Stakeholders have requested DoT that 901.XX series should not be treated as foreign IMSI range, as it is a non-geographic code with customized agreements with local licensed operators. In view of the foregoing discussion, the stakeholders are requested to provide their comments on the following question:

Q7. Whether the use of ITU allocated shared Mobile Country Code 901.XX (Global IMSI) be permitted in India for M2M Communication? If yes, what should be the methodology and procedure? If not, what are the reasons and challenges in implementation of Global IMSI? Please elaborate.

eUICC for Consumer eSIM

2.25 The eUICC will not only cater to M2M models but will have a significant impact on the Consumer segment as well. The Consumer solution targets end-users as well as enterprises that use devices targeted to the consumer market. The Consumer solution manages end-user interaction via the mobile device end-user interface, and supports standalone and companion device types. It has a different backend infrastructure and different roles assigned to architectural entities. The GSMA Remote SIM Provisioning Consumer solution follows a client-driven (pull model) approach and enables control over remote provisioning and local management of operator profiles by the end-user of the device. In addition to the M2M solution framework, a consideration of requirements for end user-managed devices necessitates more features and more complex use case scenarios.

2.26 **Consumer eUICC Ecosystem: Roles of the Entities**

Several entities overlap with the M2M Ecosystem, namely the eUICC, EUM, Device Manufacturer, Operator, and Certificate Issuer. The new key functional roles introduced by GSMA to provision the OTA subscription management are the Subscription Manager Discovery Server ("SM-DS"), Subscription Manager Data Preparation + ("SM-DP+"), and Local Profile Assistant ("LPA"). The architecture is shown in the figure below.

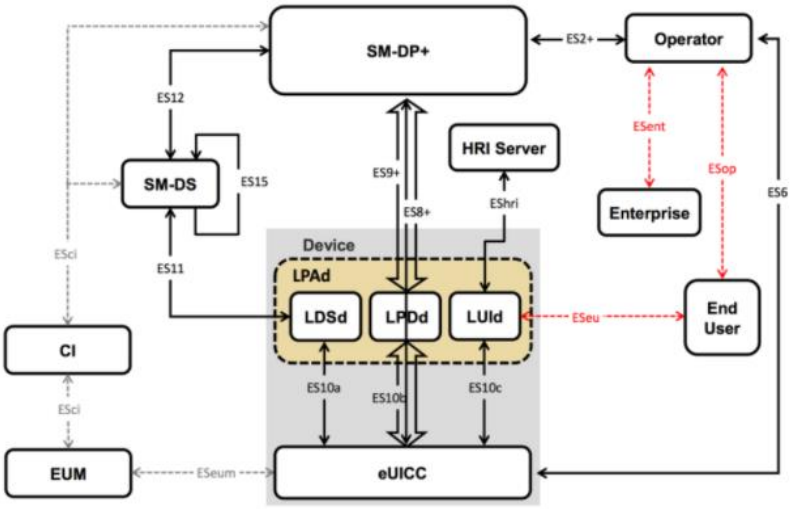

Figure: Remote SIM Provisioning for Consumer Architecture[10]

2.26.1 **eUICC**. The eUICC in the Consumer solution serves the same high-level purpose as that in the M2M solution, but its implementation is different to support the end-user interaction. It downloads and installs the Profile sent from an SM-DP+, performs Local Profile Management Operations sent from the LPA, and carries out Profile data changes sent from the Operator. Two PKI Certificates are required for eUICC Authentication against an SM-DP+ and SM-DS:

- EUM Certificate to generate the eUICC Certificate and authenticate against SM-DP+.
- eUICC Certificate to authenticate against an SM-DP+/SM-DS.
- *In order to get these certificates, the eUICC should be GSMA certified.*

2.26.2 **eUICC Manufacturer**. The eUICC Manufacturer delivers the eUICCs and bears responsibility for its initial cryptographic configuration and security architecture. The EUM issues the eUICC Certificate to allow eUICC authentication to other entities.

[10] eSIM Whitepaper: The what and how of Remote SIM Provisioning (GSMA)

It is responsible for the implementation of any LPA elements that reside in the eUICC and the compliance of the LPA with the requirements. Relevant parts of the eUICC Manufacturer's products and processes are certified by a GSMA-approved certification process

2.26.3 **Device Manufacturer**. The Device Manufacturer is responsible for implementation of any LPA elements that reside on the Device and the compliance of the LPA with the requirement. It is also responsible for the implementation of any application that resides on the Primary Device allowing Local User Interface access to the Companion Device.

2.26.4 **Operator**. It generates Profile Data and sends it to the SM-DP+. Based on the End User request, it creates the subscription contract, and generates the QR (Quick Response) code to allow the End User to download the Profile as required. It specifies the Profile characteristics and any features and applications analogous to removable UICCs. It can use an OTA Platform to manage the content of its Enabled Profile in the eUICC (RAM, RFM).

2.26.5 **Certificate Issuer (CI)**. The Certificate Issuer issues Certificates for GSMA accredited Remote SIM Provisioning entities and acts as a trusted third party for their authentication. It communicates with the SM-DP+, SM-DS, and the EUM through interfaces. eUICC manufacturers, and SM-DP+ and SM-DS hosting organizations that have successfully proven their compliance to both the security and functional requirements can apply for the necessary certificates from the GSMA Certificate Issuer to participate in the GSMA approved Consumer solution ecosystem

2.26.6 **LPAd (Local Profile Agent in the Device)**. The LPAd is a functional element in the Device or in the eUICC that provides the Local Profile Download (LPD), Local Discovery Service (LDS) and Local User Interface (LUI) features. It acts as a Proxy to download the Profile from an SM-DP+ to an eUICC. It sends the encrypted Profile Package to the eUICC. The LPAd basically serves as an entry point for all the end-user activities related to eSIM profile management, including to add, enable, disable, or delete a profile, to set or edit a profile name and list all locally available profiles. It provides the User Interface to capture the User Intent, Local Profile Management Operations, or scan the QR code. It instructs the eUICC to perform Local Profile Management Operations as per End User request. The LPA needs to be GSMA functional compliance certified using eSIM Compliance Process.

2.26.7 **Subscription Management Data Preparation + (SM-DP+)**. The SM-DP+ is given the + designation as it encapsulates the functions of both the SM-DP and the SM-SR of the M2M solution. The SM-DP+ is responsible for the creation, download, remote management functions such as enabling, disabling, updating, and deleting, as well as the protection of operator credentials (the Profile). It establishes an **end-to-end secure channel** to the eUICC to download and install Profile Packages on it. **It must be owned by the Operator and can be located anywhere**. The SM-DP+ may be linked with a particular Device via: QR code provided by an Operator, or SM-DS, or default SM-DP+ stored on the eUICC. It requires the following three PKI Certificates (*In order to get these certificates, SM-DP+ shall be GSMA certified)*:

- For Profile Binding: To encrypt the profile for a single eUICC
- For SM-DP+ Authentication to the eUICC
- For SM-DP+ Authentication to the LPA

2.26.8 **Subscription Manager Discovery Server (SM-DS)**. The SM-DS provides a means for an SM-DP+ to reach the eUICC without having to know which network the device is connected to. It has been designed for the temporary storage of alerts issued by SM-DP+ to specific eUICCs. Thus, it can act as a helper function in situations where SM-DP+ address is unknown to an eUICC. The SM-DS allows the SM-DP+ to post alerts to a secure noticeboard and for devices to extract those alerts. After an eUICC contacts the SM-DS and finds out such a pending alert, the SM-DS sends the right SM-DP+ address to the Device. This feature is important as devices can be connected using different access networks with different addresses. The SM-DS is also used to notify the LPA when Profile data is available for download to the eUICC. It requires the following two PKI Certificates (*In order to get these certificates, SM-DP+ shall be GSMA certified)*:

- For SM-DS Authentication to the eUICC.
- For SM-DS Authentication to the LPA and SM-DP+.

2.26.9 **End User**. The End User is a human who uses the Device and/or the services related to the Enabled Profile. They set up a contract with their chosen mobile network operator, and instead of receiving a SIM card, they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system. The various options to configure an eSIM solution within a device include - use of QR Code, pre-configured devices, use of SM-DS and companion devices. For example, a QR (Quick Response) code will contain the address of the Remote SIM Provisioning system (SM-DP+ server), which allows the device to connect to that system and securely download a SIM Profile. Once the Profile is installed and activated, the device can connect to that operator's network. Further, all the Profile Management

Operations are triggered by the End User via a User interface (LUId).

2.27 eSIM Activation[11]

Broadly, there are three different methods to activate an eSIM enabled consumer device:

2.27.1 **QR Activation Code**: The consumer is provided with a QR Code to be scanned with their smartphone to download the eSIM profile. In its 2D barcode format, the Code contains a Matching ID number and SM-DP+ address, which are used to reach a dedicated SM-DP+ server and download a dedicated eSIM profile package identified with the Matching ID. To attach the smartphone with the SM-DP+, a primary connection should be available, either based on Wi-Fi or an eSIM Bootstrap Profile provided by the OEM. This activation method is widely used for most of the launches of eSIM-enabled consumer devices, such as Samsung's Gear S2 3G smartwatch (e.g., by TIM Italy, Orange France) as well as Apple's latest generation eSIM-compliant iPhones. The method is in vogue in Russia, where the steps in the process for getting an eSIM plan involve its online purchase, receiving a QR-code via mail, scanning it with the device and following on-screen instructions to activate its services[12].

2.27.2 **Default SM-DP+ address activation:** In this case, the device's eUICC is pre-provisioned with the operator's SM-DP+ address during the device manufacturing stage. It is a fully automatic activation and doesn't require any interaction from the end-user except turning on the device itself. Once switched on, the device directly connects to the SM-DP+ server to retrieve its complete

[11] https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/connectivity/esim/consumer-esim-device-activation-modes

[12] https://www.esim.net/helpdesk/russia-esim/#does

eSIM profile. Here the mobile operators need to work closely with OEMs to customize the devices to their network.

2.27.3 **SM-DS Activation**: In this case, the end-user purchases a mobile phone device and eSIM subscription separately**.** Once switched on, the device automatically and instantly retrieves the eSIM profile, corresponding to the mobile subscription bought by the user. A minimum first level of native connectivity is required for the devices to attach the smartphone with the SM-DS platform. It requires mobile operators to connect their SM-DP+ platform to the SM-DS platform.

2.28 SM-DP+: Consumer Subscription Model

2.28.1 **Each Operator Manages their own SM-DP+:** In this model, each Operator controls Profile Download and Installation operations while the end User manages their profile installed on the eUICC (Enable, Disable or Delete). The SM-DP+ may be physically located within the data center of the operator's country. Alternatively, the SM-DP+ may be provided by a third party hosting the server in a different country as the operator. Since each SM-DP+ is unique to each operator, the Profile information of each operator remains isolated from the other and switching from one Profile to another is entirely controlled by the end User. However, the location of the SM-DP+ may be a concern.

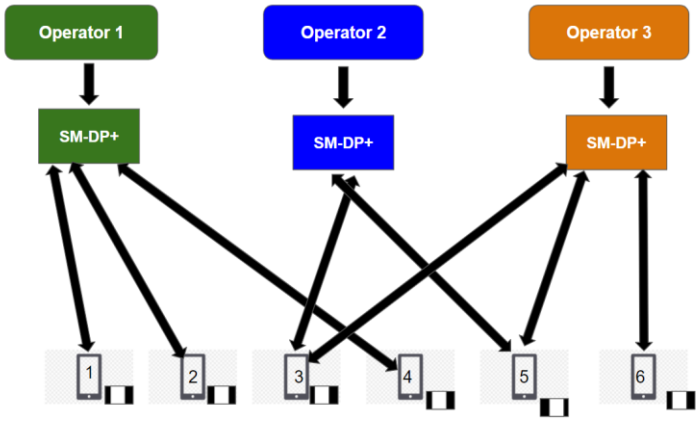

Figure: Each Operator Manages their own SM-DP+

2.28.2 **Shared SM-DP+ between Operators:** In this model, each Operator manages its profile (Download and Installation Operations) via a common SM-DP+. This may refer to a situation in which one Operator, say Operator-1 owns an SM-DP+, and shares it with Operators 2 & 3 who can store their Profiles here. It may be lucrative for Operators 2 & 3 since they do not have to establish their own SM-DP+ servers. However, there may be concerns if Operator-1 takes advantage of its SM-DP+ ownership rights and refuses to switch to Profiles of Operators 2 & 3 even when requested by the end User. Nevertheless, the MoU terms between the Operators will probably take care of these aspects.

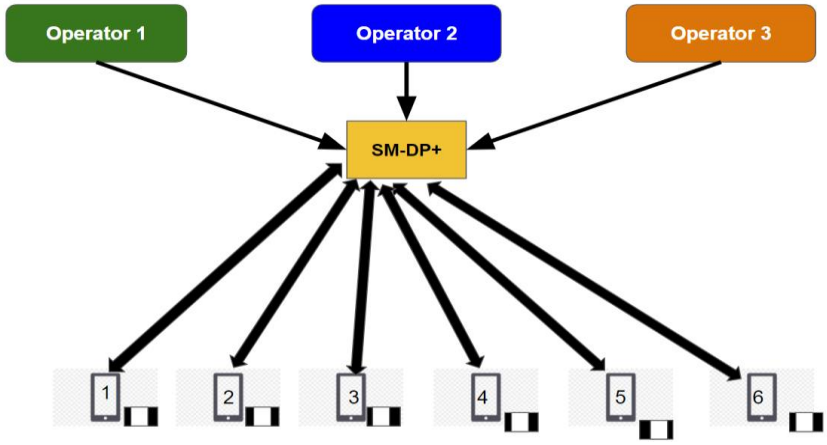

Figure: Shared SM-DP+ between Operators

2.28.3 **A single Operator manages multiple SM-DP+:** In this model, one SM-DP+ exclusively manages profile download installation for one country, and another SM-DP+ does the same for a different country. This may take care of the concerns arising for the case in which an eSIM contains the profile of an Operator based in Country-A, but has SM-DP+ in Country B. This model will make it possible for a single Operator to maintain country-specific SM-DP+s. Another SM-DP+ manages the enterprise profile. This means that a single operator may maintain separate SM-DP+s, one for end-user profiles and one for enterprise profiles

that use devices targeted to the consumer market. Here, an SM-DP+ may be physically located within the data center of the operator's country. Alternatively, some of the SM-DP+ may be provided by a third-party hosting the server in a different country as the operator.

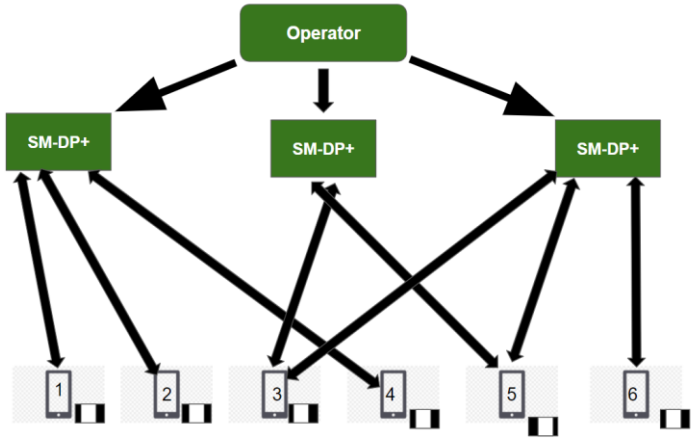

Figure: A Single Operator manages Multiple SM-DP+

2.29 Global scenario for Consumer eSIM Subscription Models leads to the fact that in most of the countries, the eSIM manufacturers are maintaining SM-DP/SM-DP+ and SM-SR, but in some countries the Network Operators and M2MSPs are also doing the same. The Global scenario of Consumer eSIM Subscription Models is provided in Annexure-II.

Q8. Is there any issue, pertaining to the Consumer eSIM, that needs to be addressed? Please highlight the issue and suggest mechanism to address it with justification.

CHAPTER 3

ISSUES FOR CONSULTATION

Q1. Whether the TRAI recommended timeline, about the foreign eUICC fitted devices to be on roaming with Indian TSP's network for a maximum period of three years only, needs a review? If yes, what should be the timeline after which the eUICC should mandatorily be configured with Indian TSP's profile?

Q2. Whether there is a need to change the controlling SM-SR from foreign TSP to Indian TSP in case of foreign eUICC fitted devices operating in India? If yes, what should be the methodology and time period within which it should be done?

Q3. Whether there is a need for the SM-SR of each TSP to be integrated with the SM-DP of each other TSP? If yes, what should be the methodology for integration? Please specify the timelines also.

Q4. Whether there is a need to prescribe SM-SR swapping among the Indian TSPs? If yes, what should be the modalities and procedure for such swap?

Q5. Whether the profile switchover, from one TSP to another, is driven by the user or OEM? If yes, what methods can be deployed to execute such switchover?

Q6. Whether non-TSP entities, such as OEMs and M2M Service Providers, should be permitted to own SM-SR and manage the subscribed profiles for their devices? If yes, what should be methodology and procedure?

Q7. Whether the use of ITU allocated shared Mobile Country Code 901.XX (Global IMSI) be permitted in India for M2M Communication? If yes, what should be the methodology and procedure? If not, what are the reasons and challenges in implementation of Global IMSI? Please elaborate.

Q8. Is there any issue, pertaining to the Consumer eSIM, that needs to be addressed? Please highlight the issue and suggest mechanism to address it with justification.

Q9. Give your comments on any related matter that is not covered in this Consultation Paper.

ANNEXURE-1

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

No. 4-35/M2M e-SIM/2021-NT Dated: 09th November, 2021

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

Sub: Recommendations of TRAI on usage of Embedded SIM for M2M Communications – regarding

SIMs for the purposes of M2M communication are embedded (integrated/soldered) at the point of manufacturing in order to achieve the standard physical and environmental requirements and are deployed in domestic or international market. Today, there are different solutions (proprietary and GSMA) in the market to allow a SIM Card to be re -provisioned over the air with a new Service Provider, avoiding the MSP lock-in.

2. DoT had issued instructions dated 16.05.2018 permitting the use of e-SIM with both single and multiple profile configurations with Over the Air(OTA) subscription update facility, as per prevailing global specifications and standards(GSMA).

3. There are various issues involved in deployment of embedded SIM. A brief consisting of background of e-SIM and issues involved is attached as Annexure-I.

4. In view of above, TRAI is requested to provide its recommendations under section 11(1)(a) of TRAI Act, 1997 as amended from time to time for holistic deployment of e-SIM in Indian Telecom network including implementation mechanism under different profile configurations and switch over of profiles by TSP's.

Enclosure: As above

(Prashik Jawade)
ADG (NT-II)

Annexure to DoT Reference Letter

Embedded SIM

1. Background:

a. The embedded SIM is a form factor that is physically integrated into the device, mostly by soldering to the device Printed Circuit Board (PCB). The embedded SIM cannot be easily removed in the field. As a result, the embedded SIM requires remote provisioning, which is the ability to remotely select the SIM profile deployed on a SIM without physically changing the SIM card. This technology is standardized and can be implemented on a SIM card with any form factor. The term eUICC is used to represent a SIM card that can be remotely provisioned.

b. SIMs for the purposes of M2M communication are embedded (integrated/soldered) at the point of manufacturing in order to achieve the standard physical and environmental requirements and are deployed in domestic or international market.

c. Today, there are multiple solutions (proprietary and GSMA) in the market to allow a SIM Card to be re -provisioned over the air with a new Service Provider, avoiding the MSP lock-in.

d. At present there are 2 technical options being discussed for M2M services to allow remote provisioning of IMSIs i.e. Soft-SIM and Embedded SIM. The first approach termed as 'Soft-SIM' has not been widely accepted by the industry due to certain security concerns required to be addressed. The second approach termed as 'embedded UICC' (eUICC) has been adopted and approved by GSMA

e. The GSMA Embedded SIM specifications were developed specifically for M2M market where it can be challenging to provision connectivity from the outset, or when deployed devices have a long lifetime and/or are deployed in locations where physical SIM replacement is not practical.

f. GSMA specifications issued on eUICC provide a single, de-facto standard mechanism for the remote provisioning and management of M2M connections, allowing the "over the air" provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another.

g. The GSMA has approved the architecture and the technical specification documents for remote provisioning that could be deployed by the MNOs for M2M applications. Using this approach, the eUICC keeps all the security features of a regular UICC while adding the capability to securely provision a new 'profile' containing all the data required (including the IMSI) to represent a mobile subscription. The update of embedded UICC is made via over-the-air (OTA) technique. The GSMA documents describe the procedure for changing the eUICC profiles.

h. GSMA specifications refer for third party to manage and switch over of e-SIM profile. Suitable mechanism in this regards needs to be prescribed for the TSP's

2. TRAI recommendations related to e-SIM:

TRAI vide its letter No. 103-3/2016-NSL-II dated 5th Sept. 2017 gave recommendations on various aspects of M2M. These include:

a. Devices with pre-fitted eUICC should be allowed to be imported only if it has the ability to get reconfigured 'Over the air' (OTA) with local subscription. GSMA approved guidelines shall be followed for provisioning of new profile remotely with 'Over-the-air' (OTA) mechanism.
b. Devices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition later based on the developments and requirements.
c. Country specific relaxation on permanent roaming of foreign SIMs, if any, can be considered based on the strategic importance, Bi-lateral or Multi-lateral trade agreements and principle of reciprocity by the government.
d. In case imported equipment to which the SIM/ device is fitted with such as automobile/ machines (like earth movers), arms etc. (requiring mandatory registration at local authorities such as RTO, State/ District administration) is transferred/ sold to another party before three years, the roaming device (eUICC) shall also be immediately configured with local subscription/eUICC of Indian TSP. The KYC details of the new owner/ buyer must be compulsorily updated in the database of concerned authorities.
e. It should not be mandatory to use only domestically manufactured SIMs in M2M. Embedded SIMs with standard specifications can be imported and relevant information shall be submitted by importer while import of the devices/SIMs.

3. DoT instructions:

DoT has issued instructions dated 16.05.2018 permitting the use of e-SIM with both single and multiple profile configurations with Over the Air(OTA) subscription update facility, as per prevailing global specifications and standards(GSMA).

4. **Issues involved:**

a. There are variances of E-SIM in the market where Multiple active profiles are being demanded by the Industry. AS140 guidelines in the Automobile sector are one such example. In such cases, third party is managing that which profile will be active at what time and at what location?

b. Some operators requested DoT:
   i. That ITU allocated 901.XX MCC be recognized by DoT, as it is recognized globally by telecom standardization bodies like GSMA, BREC, ARCEP-France etc.
   ii. That 901.XX MCC should not be treated as foreign IMSI range, as it is a non-geographic code with customized agreements with local licensed operator
   iii. That 901.XX MCC should not be considered in violations to national telecom policies, as it is specifically for IoT use cases and will never be used as consumer telecommunications
   iv. That 901.XX MCC should be considered as innovative service in telecommunication and should not be under strict telecom restrictions, as it does not use any national scarce resource
   v. That ITU is also allocating numbering series, which are not country specific, and shall also be permitted to use in India.

c. If scenarios in point b above are to be activated with Indian mobile operators than probable issues faced are:

   i. The mobile operators will be using IMSI and may be numbering series which has not been allotted to them.
   ii. There is no Inter-circle/ Intra-circle roaming available to these connections.

d. In case any business entity wishes to take VNO license and provide services as per point b above, probable issues faced by them are:

   i. The mobile operators will be using IMSI and may be numbering series which has not been allotted to them.
   ii. There is no Inter-circle/ Intra-circle roaming available to these connections.
   iii. Such operators are not allowed to have connectivity from multiple TSP.

e. The challenges mentioned above are applicable in case DoT enforces the TRAI recommendation as mentioned at point 2.b.

f. DoT is also getting references for TSP's communicating with SM-SR located in foreign country certified as per GSMA standards. Comments are required for such use cases also.

g. An embedded SIM card (eUICC) cannot be manually replaced with a local SIM which implies that the M2M device will be connected to the visited mobile network as a roaming device. Taking control of M2M device activities and effectively detecting roaming devices in the network are among the list of challenges if operators want to optimize network performance and reduce operational and signaling costs.

h. Various IoT solution enabler who are not a network connectivity provider itself aggregates agreements with existing cellular networks which connects any device through cellular networks. Regulatory mechanisms for such aggregator need to be devised.

****

ANNEXURE-II

Global Scenario for M2M/Consumer eSIM Subscription Models [13]

Customer/ State/City	Use Case	Service Provider (SP)	SP's Profile	Services	Country
TESLA	Captive	IDEMIA AMERICA Corp	eSIM manufacturer	SM-SR	USA
Daimler	Captive	IDEMA Romania	eSIM manufacturer	SM-SR	EU
Sterling, USA	Service to MO & OEM	IDEMIA AMERICA Corp	eSIM manufacturer	SM-SR, SM-DP, SM-DP+	USA
Aschheim, Germany	Service to MO & OEM	G&D	eSIM manufacturer	SM-SR, SM-DP, SM-DP+	Germany
Munich, Germany	Service to MO & OEM	G&D	eSIM manufacturer	SM-SR, SM-DP, SM-DP+	Germany
Bucharest	Service to MO & OEM	IDEMIA ROMANIA	eSIM manufacturer	SM-SR, SM-DP, SM-DP+	Romania
Beirut, Lebanon	Service to MO & OEM	Invigo Offshore	Software Services	SM-SR, SM-DP, SM-DP+	Lebanon
Dublin, Republic of Ireland	Service to MO & OEM	Kigen (UK) Limited	eSIM manufacturer	SM-SR, SM-DP, SM-DP+	Ireland
Shenzhen, China	IoT Services	Links Field Networks Ltd	IoT Services	SM-SR, SM-DP+	China
Chicago, USA	Service to MO & OEM	Valid USA Inc	Payment and Identity Services	SM-SR, SM-DP, SM-DP+	USA
Noida, India	Service to MO & OEM	Bharti Airtel India	Network Operator	SM-SR, SM-DP, SM-DP+	India
Mumbai, India	Service to MO & OEM	Reliance Jio Infocomm	Network Operator	SM-SR, SM-DP, SM-DP+	India
Thane, India	Service to MO & OEM	Vodafone India	Network Operator	SM-SR, SM-DP, SM-DP+	India

[13] https://www.gsma.com/security/sas-accredited-sites/