Telecom Regulatory Authority of India

Recommendations on
Usage of Embedded SIM for Machine-to-Machine (M2M) Communications

New Delhi, India

21.03.2024

Mahanagar Doorsanchar Bhawan, Jawahar Lal Nehru Marg, New Delhi – 110002

CONTENTS

CHAPTER 1
INTRODUCTION AND BACKGROUND

A. Introduction

1.1 Internet of Things (IoT) refers to the interconnection of many devices and objects utilizing internet protocols that can occur with or without the active involvement of individuals using the devices. The International Telecommunication Union (ITU-T)[1] has defined IoT as below:

"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. By exploiting identification, data capture, processing, and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, while ensuring that security and privacy requirements are fulfilled".

1.2 As per the National Telecom M2M Roadmap[2] issued by the Department of Telecommunications (DoT), Ministry of Communications, Government of India in May 2015, "*IoT is connected network of embedded devices capable of having M2M communication without human intervention."*

1.3 As per Telecommunication Engineering Centre (TEC), which is a technical body of DoT, *"M2M refers to the technologies that allow wired/ and wireless system to communicate with devices of the same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, meter reading, temperature etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information"*. [3]

[1] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items
[2] https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf
[3] https://www.tec.gov.in/public/pdf/M2M/link-for-point-1.pdf

1.4 The wireless communication technologies used for M2M communications may broadly be classified as below:

(a) Fixed and Short-Range Technologies: RFID, Bluetooth, Zigbee, Wi-Fi etc.

(b) Long Range Technologies: (i) Non-3GPP Standards: LoRaWAN, Sigfox, etc., and (ii) 3GPP Standards: LTE-M, NB-IoT, 5G, etc.

1.5 For providing M2M communications using 3GPP standards, Subscriber Identity Modules (SIMs) are used. SIMs store communication profiles that uniquely identify cellular subscriptions. A communications profile includes Mobile Station International Subscriber Directory Number (MSISDN) and International Mobile Subscriber Identity (IMSI). The SIM comes in various form factors and can be classified as below:

(a) Physical SIM: SIM form factors Full-Size (1FF), Mini-SIM (2FF), Micro-SIM (3FF), Nano-SIM (4FF) are the physical SIMs which can be easily removed and inserted as per user requirements. The Mobile Network Operator (MNO) is fixed in each SIM card and cannot be changed. Integrated Circuit Card Identification (ICCID) is used as the unique key to identify the SIM card. A physical SIM card can store the communication profile of only one MNO.

(b) Embedded SIM: The SIM with machine-to-machine form factor (MFF2) is known as embedded SIM or eSIM. It is soldered directly to the motherboard of M2M device, fully encased in the device. Embedded SIM (eSIM) and embedded Universal Integrated Circuit Card (eUICC) are often used interchangeably, even though there is a difference between the two. The eSIM is the hardware component of the SIM and a physical form that can be soldered into a solution. On the other hand, eUICC refers to the software component of eSIM that provides the capability to store multiple network profiles that can be provisioned and managed Over-the-Air (OTA). ICCID is the key used to identify profiles and eUICC-ID (EID) is used as the unique key to identify the eSIM.

1.6 At present, both proprietary and GSMA-compliant subscription management solutions are available in the market. Proprietary solutions work only in a closed

and isolated environment and are 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.

1.7 The GSMA-compliant subscription solutions are available in two separate variants, viz. M2M eSIM and Consumer eSIM with two separate specification SGP.02[4] and SGP.22[5] respectively. The M2M segment includes M2M 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. The GSMA-compliant subscription management solutions are broadly described below.

(1) GSMA specifications for M2M eSIM

1.8 The GSMA document SGP.01 'Embedded SIM Remote Provisioning Architecture' defines a common global architecture framework to enable the remote provisioning and management of the eUICC in M2M devices. GSMA document SGP.02 provides a standard mechanism for the remote provisioning and management of M2M connections, allowing the over-the-air (OTA) remote provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another. 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. Using this approach, the eUICC keeps all the security features of a regular Universal Integrated Circuit Card (UICC) while adding the capability to securely provision a new profile containing all the data required to represent a mobile subscription.

1.9 The GSMA remote provisioning architecture for M2M consists of various inter-related entities, viz. eUICC, eUICC Manufacturer (EUM), M2M Device, Mobile

[4] https://www.gsma.com/esim/wp-content/uploads/2020/06/SGP.02-v4.1.pdf
[5] https://www.gsma.com/esim/wp-content/uploads/2020/06/SGP.22-v2.2.2.pdf

Network Operator (MNO), M2M Service Provider (M2M SP), Certificate Issuer (CI), Subscription Manager-Data Preparation (SM-DP) and Subscription Manager Secure Routing (SM-SR).

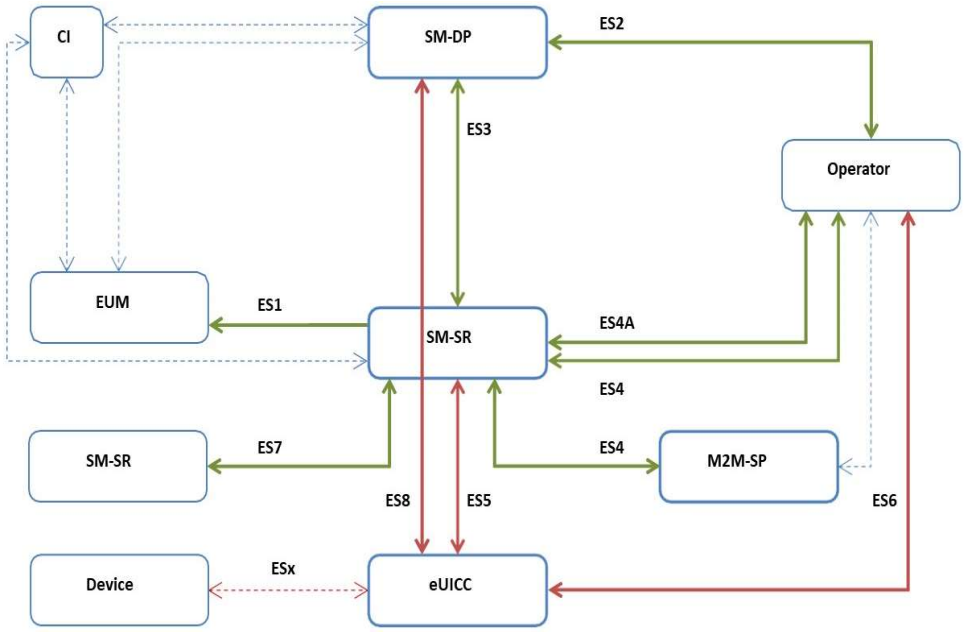

Figure 1.1: Remote Provisioning Architecture for M2M eSIM

[Source: GSMA SGP.02[6]]

(a) eUICC: It can contain one or more profiles, of which only one shall be enabled at any point in time.

(b) eUICC Manufacturer (EUM): The EUM is a supplier of eUICCs. It fabricates 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 Security Accreditation Scheme for UICC Production (SAS-UP) certified.

[6] https://www.gsma.com/esim/wp-content/uploads/2020/07/SGP.02-v4.2.pdf

(c) Device: The device manufacturer builds M2M devices which comprise a communication module and an eUICC containing at least one provisioning profile (also known as 'bootstrap profile') or operational profile that is enabled. It also prints the eUICCID (EID) on the device. The device manufacturer can select any certified eUICC and order it in the necessary quantity directly from the EUM.

(d) Operator: It is an entity providing wireless cellular network services which selects at least one SM-DP and has a direct interface to the SM-SR. The operator owns the profile and defines the policy rules to control the profile management. The 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 Over the Air (OTA) platform to manage the content of its enabled profile in the eUICC.

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

(f) Subscription Manager-Secure Routing (SM-SR): The SM-SR obtains the platform management credentials of the eUICC from the EUM (in case of initial registration) or establishes 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 should always be registered to only one SM-SR at a particular instant. The controlling SM-SR of an eUICC can be changed during the lifetime of the eUICC via SM-SR swap. The SM-SR must be GSMA SAS-SM certified.

(g) 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.

(h) Certificate Issuer (CI): The CI 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.

(2) GSMA specifications for Consumer eSIM

1.10 The GSMA remote SIM provisioning consumer solution targets the consumer market. The consumer solution manages end-user interaction via the mobile device end-user interface and supports standalone and companion device types. The 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. This architecture for consumer eSIM consists of various inter-related entities, viz. eUICC, EUM, M2M Device, MNO, M2M SP and CI and associated network elements i.e., Subscription Manager Discovery Server (SM-DS), Subscription Manager Data Preparation+ (SM-DP+), and Local Profile Assistant (LPA). The following figure depicts the GSMA's framework for remote SIM provisioning and management of the eUICC for consumer devices.

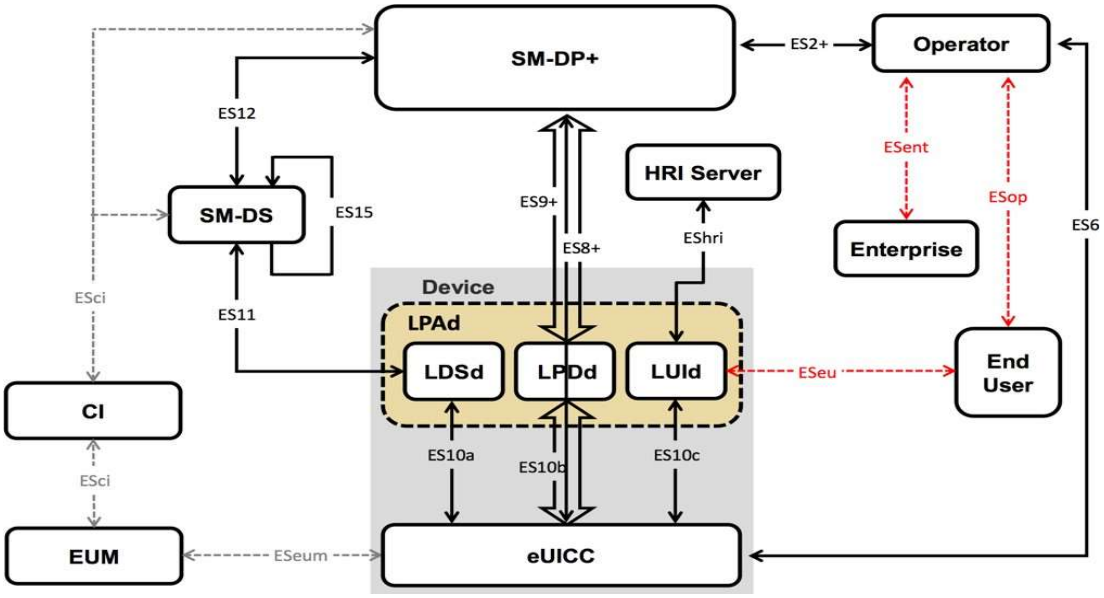

Figure 1.2: Remote SIM Provisioning and Management of the eUICC for Consumer Devices [Source: GSMA SGP.22[7]]

(a) eUICC: The eUICC in the consumer solution serves the same 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.

(b) eUICC Manufacturer (EUM): The EUM 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. It is responsible for implementation of any LPA elements that reside in the eUICC and compliance of the LPA with the requirements.

(c) Device: 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 implementation of any application that

[7] https://www.gsma.com/esim/wp-content/uploads/2020/06/SGP.22-v2.2.2.pdf

resides on the primary device allowing Local User Interface (LUI) access to the Companion Device.

(d) Operator: It generates profile data and sends it to the SM-DP+. Based on the end user request, it creates subscription contract and generates Quick Response (QR) 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 over-the-air (OTA) platform to manage the content of its enabled profile in the eUICC.

(e) Certificate Issuer (CI): The CI 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.

(f) Local Profile Agent in the Device: The Local Profile Agent in the Device (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 pull the profile from an SM-DP+ to an eUICC.

(g) Subscription Manager Data Preparation+ (SM-DP+): The SM-DP+ encapsulates the functions of both the SM-DP and the SM-SR of the M2M solution. It is responsible for the creation, download, and remote management functions such as enabling, disabling, updating, deleting and protection of the profile. It establishes an end-to-end secure channel for the eUICC to download and install profile packages on it. It must be owned by an operator and can be located anywhere. The SMDP+ may be linked with a particular device via a QR code provided by an Operator, SM-DS, or default SM-DP+ stored on the eUICC.

(h) 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.

(i) 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. Once the profile is installed and activated, the device can connect to that operator's network.

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

(1) National Telecom M2M Roadmap (May 2015)

1.11 In May 2015, DoT published the National Telecom M2M Roadmap[8] to outline the broad policy and regulatory approach to facilitate the M2M ecosystem in the country.

(2) DoT's assignment of a separate numbering scheme for M2M SIMs (December 2016)

1.12 Through a letter dated 09.12.2016[9], DoT conveyed the approval of 13-digit numbering scheme for SIM-based M2M devices. This new numbering scheme of 13 digit for M2M devices will result in a capacity of 50 billion M2M SIMs in India. The structure of the 13-digit numbering scheme is as below:

[8] https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap_0.pdf
[9] https://dot.gov.in/sites/default/files/M2M%20numbering.pdf?download=1

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

(3) TRAI's Recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' (September 2017)

1.13 Through a letter dated 05.01.2016, DoT sent a reference to TRAI seeking recommendations of TRAI on Quality of Service (QoS) in M2M Services, M2M Roaming Requirements, and M2M Spectrum Requirements. In response, after following a consultation process, TRAI sent the Recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications[10] dated 05.09.2017 to DoT.

(4) DoT's instructions for implementing restrictive features for M2M SIMs (May 2018)

1.14 Through a letter dated 16.05.2018[11], DoT issued instructions for implementing restrictive features for SIMs used only for Machine-to-Machine (M2M) communication services (M2M SIMs) and related Know Your Customer (KYC) instructions for issuing M2M SIMs to entity/ organisation providing M2M communication services under bulk category and instructions for Embedded-SIMs (e-SIMs). The relevant extract of the said instructions dated 16.05.2018 is reproduced below:

"4. …for M2M services, the mobile connections shall be issued by the licensees in the name of entity/ organization providing M2M Services as per the procedure in force for Bulk connections … subject to the condition that 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.*

[10] https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf
[11] https://dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

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.

** Such numbers shall be part of the setup of entity/ organization providing M2M Services. Further, list of such numbers is to be provided by the entity/ organization providing M2M Services to the Licensees, while obtaining SIM cards. At a later stage, if need arises, entity/ organization providing M2M Services can ask the Licensee to reconfigure these numbers."*

1.15 The afore-mentioned instructions dated 16.05.2018 provided as below in respect of eSIMs:

"13. To cater the need of modern technological developments in M2M/IoT, it has been decided to permit the use of "Embedded-Subscriber Identity Module (e-SIM)" with both Single and Multiple profile configurations with Over the Air (OTA) subscription update facility, as the case may be, as per the prevailing global specifications and standards (GSMA).

14. The licensees profiling e-SIMs shall take all reasonable steps to ensure that the device manufacturer embedding such SIM do not tamper the e-SIM at manufacturing stage.

15. In order to facilitate Mobile Number Portability (MNP) and to avoid Telco lock-in for all use case scenarios of e-SIM, the Licensees shall be permitted for Profile updation via Over the Air (OTA) feature, as per the prevailing global specifications and standards.

16. The Licensee must ensure that while allowing the use of such e-SIMs in its network, it must fulfill all the Security and Lawful Interception & Monitoring related terms and conditions of license agreement."

(5) The strategies of NDCP-2018 for the growth of M2M communication (May 2018)

1.16 In May 2018, the Central Government issued the National Digital Communication Policy-2018[12] (NDCP-2018). The strategies of NDCP-2018 for the growth of M2M communication in the country are given below:

"2.2 Ensuring a holistic and harmonised approach for harnessing Emerging Technologies

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

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

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

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

iv. …"

……

(d) Enabling Hi-speed internet, Internet of Things and M2M by rollout of 5G technologies:

…

v. Developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices

vi. Defining policy for EMF radiation for M2M devices, with accompanying institutional framework to coordinate government-funded and India-specific research in this regard

(e) Ensuring adequate numbering resources, by:

i. Allocating 13-digit numbers for all M2M mobile connections

ii. …"

[12] https://dot.gov.in/sites/default/files/Final%20NDCP-2018.pdf?download=1

(6) DoT's instructions for relaxation of the restrictive features for M2M connections (May 2019)

1.17 Through a letter dated 30.05.2019[13], DoT issued instructions for relaxation of the restrictive features for M2M connections. The relevant extract of the said instructions dated 30.05.2019 is reproduced below:

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

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."

(7) DoT's instructions on personalisation of SIM Cards (August 2019)

1.18 Through a letter dated 19.08.2019[14], DoT issued following instructions for personalisation of SIM cards:

"It has been decided that Personalisation of SIM Cards, provided to subscribers for accessing the mobile network of Licensed Telecom Service Providers, shall be mandatorily done within India w.e.f. 01.03.2020."

1.19 Later, through the letter No.800-04/2017/AS.II dated 16.04.2021, DoT stated, *inter-alia*, as below:

"2. Now, it has been decided by the competent authority that the above mentioned instructions issued for personalisation of SIM cards shall be extended to e-SIMs

[13] https://dot.gov.in/sites/default/files/M2M%20SIMs%20Relaxation_0.PDF?download=1
[14] https://dot.gov.in/sites/default/files/SIM%20personalisation%20and%20its%20corrigendum.pdf?download=1#:~:text=800%2D04%2F2017%2FAS,Standard%20Operating%20Procedure%20(SOP).

also. The IT equipment and the data utilized for personalisation of e-SIMs shall be within India."

(8) DoT's Standard Operating Procedure for personalization of SIM cards (July 2021)

1.20 Through a letter dated 16.07.2021[15], DoT released a Standard Operating Procedure (SOP) to be followed by the Licensed Telecom Service Providers and SIM Manufacturers for personalization of SIM cards. Through the para 6.3.1 of the SOP dated 16.07.2021, DoT issued instructions on 'Security of Data in motion and in use' as below:

"*6.3.1 Security of Data in motion and in use:*

Data in motion involves transfer of keys operator profile, application information, algorithm, or any relevant data etc. between MNO and SIM manufacturer either through network or physical media. It also includes transfer of data within MNOs premises (from creation of SIM personalisation related data to be sent to the SIM personalisation agency till loading of keys in the system) and movement of data in the SIM manufacturer premises during SIM personalisation lifecycle. Therefore, effective security controls should be implemented during the all stages at MNO premises and at SIM manufacturer's premises.

Following are the important security controls to be implemented while data is in motion:

i. Data exchange with internal and external stakeholder should be done in encrypted form atleast through SFTP and secure VPN with TLS certificate from both sides.

ii. Adequate access control mechanism should be maintained at each stage of movement of data.

iii. Direct access to the data should be avoided without check and balance mechanism. All administrative access to data should be done where explicitly authorised by using Biometric or any other equivalent authentication mechanism.

[15] https://dot.gov.in/sites/default/files/SOP%20for%20Personalisation%20of%20SIM%20cards.pdf?download=1

iv. Roles and responsibilities of authorised person for data access at each node whether at production house or R&D centre should be well defined on the organization's Security policy.

v. The application(s) and hardware platform used for processing SIM personalisation data should be free from any security vulnerabilities."

(9) Introduction of M2M Authorization under Unified License Agreement (January 2022)

1.21 In January 2022, DoT introduced a separate authorization on Machine-to-Machine (M2M) under Unified License Agreement[16].

(10) DoT's M2MSP Registration Guidelines (February 2022)

1.22 Through an Office Memorandum dated 08.02.2022, DoT issued 'Guidelines for Registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services'[17] (hereinafter, also referred to as DoT's M2MSP Registration Guidelines dated 08.02.2022). Through the said OM, DoT instructed that in order to address concerns like interface issues with telecom service providers (TSPs), Know your customer (KYC), security and encryption, all M2M service providers utilizing telecom facilities from authorized TSPs should have M2MSP registration.

1.23 In the DoT's M2MSP Registration Guidelines dated 08.02.2022, M2MSP was defined as below:

"M2M Service Provider" (M2MSP) is an Indian company, registered under the Indian Companies Act, 2013 or an LLP (Limited Liability Partnership) registered under LLP Act, 2008 or a partnership firm which provides M2M services to third parties using telecom resources. Provided that

---

16 https://dot.gov.in/sites/default/files/UL%20AGREEMENT%20with%20Audiotex%20M2M%20without%20INSAT%20MSSR%2017012022_0.pdf?download=1

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

(a) such third parties utilising M2M services from registered M2MSP in connection with its products or as part of its offerings to its end customers as a product or service, and

(b) any organization which intends to provide M2M services for its own use (captive use) and not for commercial purpose, shall also be covered under this definition."

(11) TEC's Recommendations on Security by Design for IoT Manufacturers (March 2023)

1.24 Telecom Engineering Center (TEC), a technical body of DoT, issued the Technical Report TEC 31328:2023[18] dated 28.03.2023 on 'Security by Design for IoT Device Manufacturers'. Relevant extract of the Hardware security recommendations given in the said technical report is reproduced below:

"5. For SIM based devices following hardware security provisions are recommended:

i. UICC/ eUICC enabled IoT device shall reserve minimum 32K of Non-Volatile Memory (NVM)/space for installing Government notified application like disaster management, social welfare, security, health, safety. (Ref:/ UICC ITSARhttp://nccs.gov.in).

ii. To protect SIM from IMSI catcher, Subscription Concealed Identifier (SUCI) and Subscription Permanent Identifier (SUPI) should be integrated in SIM for 5G cellular technology security.

iii. For eSIM business in India, the certificate issuer for eSIM Remote Service Provisioning (RSP) needs to be located in India under GSMA.

iv. In view of security of IT infrastructure related to eSIM remote service provisioning (SM-DP, SM-SR and SM-DP+), these IT infrastructures need to be owned by any registered entity with DoT and located within Indian territory."

[18] https://tec.gov.in/public/pdf/M2M/Security%20by%20Design%20for%20IoT%20Device%20Manufacturers.pdf

(12) Addendum to the DoT's M2MSP Registration Guidelines (January, 2024)

1.25 On 01.01.2024, DoT issued an 'addendum to the guidelines for registration of M2M Service Providers (M2M SPs) & WPAN/ WLAN Connectivity Providers for M2M Services'. Through the said addendum, DoT notified as below:

"2. In order to proliferate the standard-based and secure M2M/ IoT ecosystem and to address the concerns of M2M Service Providers and WPAN/WLAN Connectivity Providers for M2M services, related to interface with TSPs, KYC, Security, Encryption etc., it has been decided to extend the scope of the registration to also allow all types of business entities such as company, Government Departments/ Organizations, Partnership Firms, LLPs, Institutions, Undertakings, Proprietorship Firms, Societies and Trusts to apply for registration as M2M Service Providers and WPAN/WLAN Connectivity Provider for M2M services, as the case may be, as part of the above guidelines.

3. Accordingly, all the entities providing M2M services or WPAN/ WLAN connectivity for M2M services, shall register with DoT through the SaralSanchar portal (https://saralsanchar.gov.in) by 31.03.2024, failing which the telecom resources taken from Authorised Telecom Licensees of DoT are liable to be withdrawn/ disconnected."

C. DoT's Reference dated 09.11.2021

1.26 The Department of Telecommunications (DoT) sent a reference letter dated 09.11.2021 on the subject- "Recommendations of TRAI on usage of Embedded SIM for M2M Communications-regarding" (**Annexure-I)** to Telecom Regulatory Authority of India (hereinafter also referred to as "TRAI", and "the Authority"). Through the said reference, DoT requested TRAI to provide its recommendations for holistic deployment of eSIM in Indian Telecom Network including implementation mechanism under different profile configurations and switch over of profiles by TSPs. The said reference is reproduced below:

"*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 eSIM 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 eSIM and issues involved is attached as Annexure-I.

4. *In view of the 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.*

1.27 The background note annexed with the DoT's reference letter dated 09.11.2021 is reproduced 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 in order 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 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 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 e-SIM profile. Suitable mechanism in this regard 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 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 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 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 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. AIS-140 guidelines issued by the Ministry of Road transport & Highways (MoRTH) in the Automobile sector are one such example. In such cases, a third party is managing 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, then probable issues faced are: -*
   i. *The mobile operators will be using IMSI and may be the numbering series which have 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 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.*

1.28 Through a letter dated 10.12.2021, TRAI sought certain additional information from DoT with respect to the DoT's Reference dated 09.11.2021. In response, through a letter dated 26.05.2022, DoT sent copies of the representations received from stakeholders highlighting the issues related to eSIM profiling and associated issues.

D. TRAI's Consultation Process w.r.t. DoT's Reference dated 09.11.2021

1.29 In respect of the DoT's Reference dated 09.11.2021, the Authority issued a Consultation Paper on 'Embedded SIM for M2M Communications' on 25.07.2022 (hereinafter also referred to as "the CP dated 25.07.2022") to solicit views of stakeholders on the subject. Written comments on the CP dated 25.07.2022 were invited from stakeholders by 22.08.2022 and counter-comments by 05.09.2022. Upon request of some stakeholders, the last dates for furnishing comments and counter-comments were extended to 19.09.2022 and 03.10.2022 respectively. The Authority received a total of 15 comments. The comments received from stakeholders were placed on TRAI's website www.trai.gov.in. An online Open House Discussion (OHD) was held on 14.12.2022 with stakeholders through virtual mode. Based on the comments and counter-comments received from stakeholders during the consultation process, and further analysis, the Authority has arrived at the present recommendations.

1.30 These recommendations comprise of three chapters. Chapter 1 provides an introduction and background to the subject. Chapter 2 presents an analysis of the issues raised in the CP dated 25.07.2022 considering comments and counter-comments received from stakeholders and the recommendations of the Authority

thereon. Chapter 3 provides a summary of the recommendations of the Authority on the subject.

CHAPTER 2
ANALYSIS OF ISSUES

2.1 Through the CP dated 25.07.2022, the Authority solicited views of stakeholders on the following issues related to the usage of embedded SIM for M2M communication:

(a) Need to review the TRAI's recommended timeline for the foreign eUICC fitted devices to be on roaming in Indian TSP's network;

(b) Need for changing the controlling SM-SR from foreign TSP to Indian TSP in case of foreign eUICC fitted devices operating in India;

(c) Need for integration of SM-SR of each Indian TSP with the SM-DP of the other Indian TSP;

(d) Need for prescribing SM-SR swapping among Indian TSPs;

(e) Issue of profile switch-over from one TSP to another TSP;

(f) Need for permitting non-TSP entities, such as OEMs and M2MSPs, to own SM-SR;

(g) Need for permitting ITU allocated shared Mobile Country Code 901.XX (Global IMSI) in India; and

(h) Issues pertaining to Consumer eSIM.

2.2 An analysis of the afore-mentioned issues based on the comments and counter comments received from stakeholders is presented below.

A. Need to review the TRAI's recommended timeline for the foreign eUICC fitted devices to be on roaming in Indian TSP's network

2.3 Earlier, through a reference dated 05.01.2016, DoT had sought TRAI's recommendations on Quality of Service (QoS) in M2M services, M2M roaming requirements, and M2M spectrum requirements. In this regard, TRAI issued a consultation paper on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 18.10.2016. Through the said Consultation Paper dated 18.10.2016, the Authority had raised, *inter-alia*, the following issue for consultation with stakeholders:

"In case of M2M devices, should:

(a) *Roaming on permanent basis be allowed for foreign SIM/ eUICC; or*

(b) *Only domestically manufactured SIM/ EUICC be allowed? and/ or*

(c) *There be a timeline/ lifecycle of foreign SIMs to be converted into Indian SIMs/ eUICC?*

(d) *Any other option is available?*

Please explain implications and issues involved in all the above scenarios."

2.4 On the conclusion of the consultation process, the Authority issued its recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-machine (M2M) Communications' dated 05.09.2017. In the said recommendations, the Authority observed, *inter-alia*, as below:

"3.98 …in M2M scenario it is expected that large number of devices will be deployed for an average life span for 10-15 years with minimal or no requirement of human interventions. Long lifespan of the device in permanent roaming may not be suitable for overall interest of the nation as there are possibilities that goods/ equipment/ vehicles once imported by a person or a company are resold to another person in local market, thus creates an issue of authenticity and identity of the person. The issue is clearly linked with applicability of KYC rules and traceability of the person and device.

3.99 The Authority has also noted the security risks involved and possibility of hacking of entire network or system in intelligent and connected M2M/ IoT networks. Recent attack of 'Ransomeware' malware is just an example how it can affect the lives of citizens by attacking ATMs and banking system. As of now 100% Foreign Direct Investment (FDI) is allowed in many sectors and foreign companies are awarded turn-key contracts on long term basis. In view of the industrial automation at large scale, there are fair chances of vulnerability to hacking of the country's strategic sectors/networks such as power, telecom etc. …"

2.5 Based on its analysis, the Authority had recommended, *inter-alia*, as below through the afore-mentioned recommendations dated 05.09.2017:

"5.7 The Authority recommends that:

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, Bilateral 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."

2.6 DoT has not yet implemented the afore-mentioned recommendation. At present, no timelines have been prescribed by DoT for the foreign eUICC fitted devices to be on roaming in Indian TSP's network.

2.7 In the present consultation process, the Authority decided to review the earlier recommended timeline of maximum three years for the foreign eUICC fitted devices to be on roaming. Accordingly, through the CP dated 25.07.2022, stakeholders' comments were invited 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?

(1) Responses of Stakeholders on the Q1

2.8 In response to the afore-mentioned question, three types of views were received from stakeholders, as outlined below:

(a) Most stakeholders opined that the timeline should be reduced.

(b) A stakeholder asserted that the recommended timeline of maximum three years does not require any review.

(c) A few stakeholders contended that there should be no restriction on international roaming of M2M devices.

2.9 A summary of the comments received from the stakeholders, who have opined that the timeline should be reduced, is given below:

(a) TRAI's recommendation for the foreign eUICC fitted devices to be on roaming in Indian TSP's network for a maximum period of three years was issued prior to the DoT's instructions dated 16.05.2018 and 30.05.2019 and was therefore proposed without considering the restrictive features of M2M SIMs. Hence, the said recommendation should be revised in view of the changed regulatory oversight and the ground situation. With a view to facilitate IoT devices with foreign eUICC but at the same time to ensure that such devices are compliant with Indian regulations, six months is a reasonable time for migrating from a roaming profile to a local profile and therefore, the timelines should be reduced to six months.

(b) As per the framework laid down by DoT in 2018 for M2M services in the country, there is a need to enforce restrictive communication features on M2M SIMs or eSIMs given the flexibility provided with respect to relaxed KYCs. Also, there is a mandate on M2M Service Providers (M2MSPs) to ensure that the details of end users are made available to TSPs. These requirements were introduced in the spirit of national security and to prevent potential misuse or abuse of M2M SIMs. In contrast to this, telecom service providers in many

countries do not need to fulfill any customer application form (CAF) or Know Your Customer (KYC) guidelines and are issuing UICC and eUICC to global IoT service providers. Therefore, if international roaming SIMs are not converted into profiles of Indian TSPs within a specified timeframe, it will lead not only to non-fulfilment of Indian security requirements but will also to a non-level playing field between Indian TSPs and foreign TSPs. Therefore, all such connections need to be brought within the ambit of the Indian KYC rules by converting them into profiles of Indian TSPs. It will help in dealing with any security threat and/ or prevent the misuse of UICC or eUICC in India. Hence, for a foreign UICC or eUICC entering India on international roaming, a period of up to six months should be given for the UICC or eUICC to be mandatorily configured with a profile of an Indian TSP.

(c) There are concerns of non-availability of M2M services in the State of Jammu & Kashmir in case of imported devices pre-fitted with foreign SIM cards due to restrictions placed on international SIMs roaming in Jammu & Kashmir. Considering the matured Indian market and to ensure that all eUICCs working in India follow Indian security and regulatory requirements, the three-year period should be reduced to six months.

(d) Though it may be desirable to have a liberalized regime for implementation of international roaming to cater to the emerging market requirements, however, keeping in view the overarching requirements of national security, it may perhaps be prudent to specify conversion of foreign SIMs for all M2M connections (working on eSIMs) to Indian SIMs within a reasonable time frame, which may be suitably decided by the Authority.

(e) As the M2M technology is sufficiently mature in India, the roaming grace period should not be more than a year.

2.10 The stakeholder, who asserted that the earlier recommended timeline of maximum three years does not require any review, did not provide any justification in support of its assertion.

2.11 The inputs of the stakeholders, who have contended that there should be no restriction on international roaming of M2M devices, may be summed up as below:

(a) Neither the telecom license, nor any TRAI regulation has prescribed any duration for which an international customer can roam within India. Foreign eUICC fitted device roaming with Indian TSP's networks is a scenario of international roaming which works as per the mutual agreement entered between the foreign carrier whose eUICC is fitted in the device and the Indian TSP with whom the foreign carrier has the roaming agreement. Hence, roaming of an eUICC fitted devices in India should be left to the market forces.

(b) Any roaming restriction would significantly hamper the growth of M2M/ IoT services in the country. However, in case a timeline is being envisaged for roaming of foreign eUICC fitted devices in India, then the TRAI recommended period of three years should be continued. It will enable sufficient time for the end user and M2MSP to get the services transferred, without any service disruption. Further, the timeline of three years should apply only for the new devices and not on existing devices. Existing devices may be permitted to continue with roaming profiles, as the migration will be a complex task for all the operators, end users and M2MSPs.

(2) Analysis in respect of the Q1

2.12 While analyzing the matter, the Authority took note of the following aspects:

(a) In respect of foreign SIMs to be used in India, DoT's National Telecom M2M Roadmap (May 2015)[19] provides, *inter-alia*, as below:

"4.2.3. International Roaming

There may be some scenarios, wherein MSP or manufacturer may be an entity located in foreign country and it may prefer to fit the foreign telecom service provider's SIM in the machine to be used in India always. Like, a car may be manufactured in a foreign country with a foreign telecom operator's SIM in it. In such cases, SIM shall be always in roaming state outside its home network (permanent roaming) and KYC details of car user shall not

[19] https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

get updated in normal course in the database of Indian TSP. In case of TSPs devising some mechanism for affecting KYC compliance for M2M international In-roamers, there need not be any security related apprehension and resulting restriction in such cases. Government is of the view that Law Enforcement Agencies should have single point of interaction for getting the KYC details of SIM users which in present human usage scenario is TSPs.

There are logistical and technical difficulties in the immediate prohibition of foreign SIM cards in machines imported in the country, as SIM modules are generally secured and not intended to be replaced in normal course. Also testing of machines at manufacturing stage may require fully equipped communication module.

Devices which are imported from foreign countries may use embedded or soft SIMs or other such feasible technologies, where TSP profile/ IMSI can be updated over the air. Alternatively, manufacturers of M2M devices may tie up with Indian TSPs for equipping them with Indian SIMs. Keeping all these aspects in view, the government is of the opinion that in long run, foreign SIM should be permitted in the devices to be used in India only on the condition of fulfillment of traceability criteria. It is felt that reasonable notice time should be given to all stakeholders, particularly those selling devices or vehicles fitted with foreign SIMs, so as to enable them to enter into commercial arrangements with Indian TSPs and perform requisite technical integration & testing to enable them to use alternate feasible technologies i.e. Soft-SIMs, Embedded SIMs etc. To begin with, machines sold and manufactured in India may be allowed to be equipped with SIMs of Indian TSPs only.

Already operation devices or vehicles with foreign SIMs in customer's custody may prove tricky. The manufacturers of such devices may find it imprudent to maintain two categories of devices – one in perpetual roaming state and other in home network and will find it more economical to gradually retrofit all such devices with Indian SIMs. Thus the timelines for prohibiting selling of machines with foreign SIMs in the country and timeline for switchover of

already operational machines with foreign SIMs to Indian SIM may be decided in consultation with relevant stakeholders." [Emphasis supplied]

(b) Through the instructions dated 16.05.2018[20], DoT has mandated that the issuance of M2M SIMs by authorized telecom licensees to the entities providing M2M services will follow KYC norms prior to the issuance of such SIMs. For M2M services, the mobile connections shall be issued by the licensees in the name of entity/ organization providing M2M services as per the procedure in force for bulk connections[21] subject to the condition that such SIMs will have restrictive features compared to traditional SIMs for voice/ data communications used for person-to-person (P2P) communication. The updated restrictive features for M2M connections prescribed by DoT through instructions dated 30.05.2019[22] are given below:

"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.

** Such numbers shall be part of the setup of entity/ organization providing M2M Services. Further, list of such numbers is to be provided by the entity/ organization providing M2M Services to the Licensees while obtaining SIM cards. At a later stage, if need arises, entity/ organization providing M2M Services can ask the Licensee to reconfigure these numbers.*

Note: These restrictive features requirements shall be configured by Licensees only in their network including VPN."

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

[21] Through the instruction No. 800-09/2023-AS.II dated 31.08.2023, DoT has discontinued the process of issuing connections under bulk category. Instead, a new category of 'business connections' has been introduced.

[22] https://dot.gov.in/sites/default/files/M2M%20SIMs%20Relaxation_0.PDF?download=1

(c) Through the instructions dated 16.05.2018, DoT has also mandated that the ownership of all M2M SIMs shall be with the entity/ organization providing M2M services.

(d) The Unified License Agreement mandates that *"[t]he details of all the customers of M2M services i.e., physical custodian of M2M devices having M2M subscription shall be maintained. Updated information regarding (a) details of M2M devices, (b) Make, Model, Registration number etc. of the M2M devices (i.e. Cars, Utility Meters, POS etc.) & (c) corresponding physical custodian's name and address shall be made available to Licensor. Any changes in customers and M2M devices details shall be updated."*

(e) Through the Office Memorandum (OM) dated 08.02.2022[23], DoT has issued 'Guidelines for Registration Process of M2M Service Providers (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services'. Through these guidelines, DoT has mandated that *"[i]n order to address concerns like interface issues with TSP, KYC, Security and encryption, all M2M service providers utilizing telecom facilities from authorized TSPs should have M2MSP registration."* The guidelines require M2MSP registrant to fulfill the terms and conditions mentioned therein. The technical conditions imposed on M2MSP registrant include, *inter-alia*, the following:

"1. M2MSP shall take the Telecom Resources from an Authorized Telecom Licensee having valid license under Indian Telegraph Act, 1885. …

…….

3. Registrant shall adhere to Know Your Customer (KYC) and related guidelines issued by the Authority to Authorized Telecom Licensee from time to time for all Telecom resources including SIM enabled devices and numbering resources. The Authority reserves the right to call for such details as and when required.

4. The details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Up-dated information regarding (a) details of M2M end device i.e. IMEI, ESN etc., (b)

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

Make, Model, Registration number etc. of the machines (i.e. Cars, Utility Meters, POS etc.) & (c) corresponding physical custodian's name and address shall be made available to Authorized Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated."

2.13 In short, Government of India has put in place a mechanism for regulatory oversight over the M2M connections issued in India in terms of KYC norms, requirement for maintaining updated details of M2M customers etc. Besides, there are restrictive features on voice calls/ SMS/ data communication from M2M connections issued by Indian telecom service providers. These restrictive features cannot be made applicable on voice calls/ SMS/ data communication from M2M connections issued by foreign telecom service providers as they are not under the purview of Indian telecom licensing regime. Similarly, the regulatory oversight in terms of KYC norms and requirement for maintaining updated details of M2M customers does not become applicable on the M2M connections issued by foreign telecom service providers. A few stakeholders have contended that a foreign eUICC roaming in India will not be complying with the domestic regulatory and security guidelines thus, compromising the security of the country and creating a non-level playing field with competing eUICC from Indian telecom service providers. The Authority took note of the fact that M2M services will not be available to foreign eUICC fitted devices in Jammu & Kashmir due to restrictions placed on international SIMs roaming in Jammu & Kashmir. The Authority also noted that through National Telecom M2M Roadmap (May 2015), DoT has emphasized the need for a timeline for prohibiting selling of machines with foreign SIMs in the country and a timeline for switchover of already operational machines with foreign SIMs.

2.14 Through the recommendations dated 05.09.2017, the Authority had recommended that *"[d]evices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within he 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". The Authority notes that at the time when this recommendation was made, the ecosystem for M2M services was in an infant stage. In the past six years, the M2M services market has witnessed significant growth worldwide. As per FMI-Future market Insight,[24] the worldwide market for M2M services in the year 2022 was US$39.7 Billion. The FMI-Future market Insight suggests that in the Asia Pacific market, the development of government funded programs such as smart cities, smart meters, and policies, will facilitate a wide scale deployment of M2M services. At present, there are more than 34 million M2M cellular mobile connections in India.

2.15 The Authority also took note of the fact that consumer cellular mobile connections[25], held by persons, generally remain on international roaming for short periods of time, and return to their respective home countries thereafter. On the other hand, the M2M cellular mobile connections, fitted in imported devices, remain on international roaming for long periods of time, and seldom return to their home countries. Therefore, the M2M eSIMs fitted in imported devices may require a different regulatory treatment other than that for consumer cellular mobile connections, on international roaming.

2.16 In short, the eco-system for M2M services has developed significantly in the country as compared to the year 2017 when the earlier recommendations on M2M services were sent to the Government. In the interim period, the Government has imposed specific security and regulatory requirements on the operation of M2M cellular mobile connections issued by Indian telecom service providers.

2.17 Considering the foregoing discussion, the Authority is of the view that the maximum period for which a foreign M2M eSIM may roam on Indian TSP's network needs to be reduced from the TRAI's earlier recommended timeline of three years.

[24] https://www.futuremarketinsights.com/reports/managed-m2m-services-market

[25] Cellular mobile connections are of two kinds viz. consumer (P2P) cellular mobile connections, and M2M cellular mobile connections. Consumer (P2P) cellular mobile connections are held by persons, and M2M cellular mobile connections are fitted in devices.

2.18 The Authority notes that most of the stakeholders, who are in favour of reduction in the maximum period for which a foreign M2M eSIM may remain on roaming in Indian TSP's network, have suggested that migration to Indian TSP's profile should be completed within 6 to 12 months. In this regard, the Authority notes that the National Telecom M2M Roadmap issued by DoT in May 2015 suggested, *inter-alia*, that *"reasonable notice time should be given to all stakeholders, particularly those selling devices or vehicles fitted with foreign SIMs, so as to enable them to enter into commercial arrangements with Indian TSPs and perform requisite technical integration & testing to enable them to use alternate feasible technologies i.e. Soft-SIMs, Embedded SIMs etc."* [Emphasis supplied]

2.19 The Authority noted that with the help of GSMA's remote SIM provisioning feature, profile(s) of Indian TSPs can be installed over-the-air on an M2M eSIM, fitted in a device imported in India. Therefore, a period of six months from the date of activation in India will be sufficient for M2M eSIM customers to arrange for profile switch-over from foreign to Indian. Accordingly, the Authority is of the view that change of foreign profile(s) to Indian profile(s) on M2M eSIMs, fitted in the devices imported to India, should be completed within a period of six months from the date of activation of international roaming on such M2M eSIMs.

2.20 **Earlier, through the recommendation No.5.7(b) of the recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that *"[d]evices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition based on the developments and requirements".***

Based on a review of the said recommendation, the Authority recommends that all communication profiles on any M2M eSIM fitted in

an imported device on international roaming in India should be mandatorily converted/ reconfigured into communication profiles of Indian telecom service providers within a period of six months from the date of activation of international roaming in India on such M2M eSIM or on change of ownership of the device, whichever is earlier.

B. Issue of profile switch-over from one TSP to another TSP

2.21 At present, the end user of the M2M device cannot initiate profile switchover in case of dissatisfactory consumer experience. In this regard, through the CP dated 25.07.2022, the Authority solicited comments of stakeholders 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?

(1) Responses of stakeholders on the Q5

2.22 In response to the above question, most stakeholders have opined that switchover of profile from one TSP to another should be driven by OEM/ application service provider/ M2MSP and not by the user. Only a few stakeholders have suggested that such switchover can be initiated by users as well.

2.23 A summary of the comments of the stakeholders, who have opined that switchover of profile from one TSP to another should be driven by OEM/ application service provider/ M2MSP, and not by the user, is given below:

(a) M2M ecosystem is mainly driven by the OEMs who take M2M services from the M2MSP who, in turn, subscribes M2M cellular mobile connections from telecom service providers (TSPs). While the end users make use of the eUICC fitted devices, a variety of functions are controlled and consumed by the OEMs. For example, in the case of connected cars, while the end users are the respective owners of the cars, the data related to telematics, vehicle's performance etc. is consumed by the OEMs. Besides, the OEMs own the

subscription of M2M eSIMs, hence the profile switchover should be driven by the OEMs.

(b) As per the GSMA document GSMA CLP.05-v1.0[26] (Business Process for Remote SIM provisioning in M2M), OEM should initiate the process of profile switchover from one TSP to another.

(c) It is the M2MSP, who enters into commercial agreements with TSPs and is responsible for providing M2M services to customers. Based on the analysis of network performance and commercial considerations, the M2MSP can take a decision to use the services of another TSP in case it deems the performance of the current TSP unsatisfactory. Therefore, switchover or migration from one TSP to another should be driven by M2MSPs. It will not be feasible to accommodate the request of profile switchover from individual users

2.24 On the other hand, one of the stakeholders has mentioned that from a technical perspective, profile switchover largely depends on how the terms of service and business relationship are defined in any service agreement between the initial TSP and the OEM and the user; an agreement permitting a profile switch to another TSP, whether initiated by the OEM or a user, must also be aligned to technical abilities, clear methodology and legal relationships between the parties. Another stakeholder has mentioned that subject to technical feasibility, the option of profile migration should be available to the end customer. Another stakeholder has opined that it will depend on the type of service and as to who pays for the cellular connectivity.

(2) Analysis in respect of the Q5

2.25 While analyzing the issue, the Authority took note of the following aspects:

[26] https://www.gsma.com/iot/wp-content/uploads/2015/02/CLP.05-v1.0-BPD.pdf

(a) The DoT's instructions dated 16.05.2018 provide, *inter alia*, that *"for M2M services, the mobile connections shall be issued by the licensees in the name of entity/ organization providing M2M Services".*

(b) DoT's M2M registration guidelines dated 08.02.2022 provide that *"all M2M service providers utilizing telecom resources from authorized TSPs should have M2MSP registration."* These guidelines also provide that *"[i]n case any Authorized Telecom Licensee wishes to provide M2M services to third parties, it can do so under current licensing framework without requiring to register for M2MSP or WPAN/ WLAN Connectivity Providers."*

(c) The GSMA's document CLP.05-v1.0 titled 'Business Process for Remote SIM provisioning in M2M' dated 18.02.2015 recognizes that *"changes of Operator Profiles, especially over a large set of eUICC devices can be a complex activity. Such transfers need to be carried out in a structured, methodical way".* The said GSMA document specifies a detailed business process flow for transfer of profiles on M2M eSIMs between two operators, when an OEM[27] wishes to switch connectivity provider.

2.26 At present, the licensed TSPs in India provide M2M cellular mobile connections to M2MSPs, who in turn, provide M2M services to the OEMs. Specifically, in case of M2M eSIMs, the communication profiles of TSPs in India are installed on M2M eSIMs on the request of M2MSPs on behalf of the concerned OEMs. Also, the transfer of communication profiles from one TSP to another is initiated on the request of the M2MSPs on behalf of the concerned OEMs.

2.27 The Authority noted that M2MSPs obtain bulk subscription for cellular connectivity on the devices fitted with M2M eSIMs from TSPs. The commercial considerations of cellular connectivity through M2M eSIMs are decided on bulk basis between M2MSPs and TSPs. The M2MSPs and OEMs monitor the data emanating from the

[27] GSMA CLP.05-v1.0 (Business Process for Remote SIM provisioning in M2M) dated 18.02.2015 defines OEM as *"an entity that is providing M2M service to the end customer using a device containing an eUICC."*
The M2MSP Registration Guidelines dated 06.02.2022 define "Original Equipment Manufacturer (OEM)" as an organization that makes devices containing M2M eSIM.

devices fitted with M2M eSIMs. They can assess the network performance of the serving TSP.

2.28 In short, OEMs and M2MSPs are well-placed to decide profile switchover from one TSP to another based on commercial considerations and network performance. The Authority is of the view that as the commercial agreements between the TSPs and M2MSPs in respect of the subscriptions for M2M eSIMs are carried out on a bulk basis, it would be difficult to accommodate the request of profile switchover from individual users.

2.29 Considering the comments of stakeholders and further analysis, **the Authority recommends that the switch-over of the communication profile on M2M eSIMs from one licensed telecom service provider (TSP) to another TSP should be driven by the concerned Original Equipment Manufacturer (OEM) of the devices containing M2M eSIMs.**

C. Need for permitting non-TSP entities to own SM-SR

2.30 The GSMA's M2M eSIM architecture envisages two subscription management servers for remote SIM provisioning as given below:

(a) Subscription Manager- Data Preparation (SM-DP): It prepares operational and bootstrap profiles to be securely provisioned on eUICCs and manages the installation of these profiles on eUICCs.

(b) Subscription Manager- Secure Routing (SM-SR): It acts as a gateway between SM-DP and eUICC. It allows a secure transport of both platform and profile management commands to load, enable, disable, and delete profiles on eUICCs. An eUICC is always linked to only one SM-SR. An eUICC always needs to have either a bootstrap profile or a full operational profile from the operator installed to ensure communications between the eUICC and the SM-SR.

2.31 Together, the subscription management servers viz. SM-DP and SM-SR enable the OEMs and M2MSPs to manage connectivity for their devices over-the-air (OTA)

securely. GSMA has also prescribed a Certificate Issuance process, which ensures that the various system entities (SM-DP, SR-SR, EUM, eUICC) can all be trusted by each other. At present GSMA plays the role of Certificate Issuer (CI). The interaction between SM-DP, SM-SR and eUICC requires an end-to-end security (authentication), as it relies on digital certificates (PKIs)[28] or pre-shared keys (PSKs). GSMA revokes the certificates if there are any security issues. The compliance requirements focus on security assurance and interoperability. The following figure[29] illustrates the GSMA's security compliance framework for eSIM:

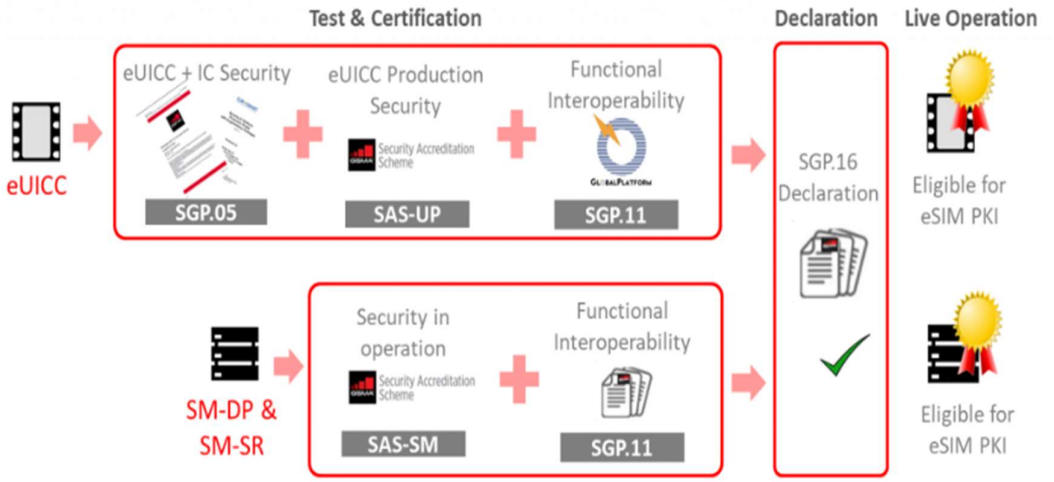

Figure 2.1: GSMA's security compliance framework for eSIM

2.32 Only eUICC manufacturers, and SM hosting organisations (SM-DP, SM-SR, or SM-DP+) that have successfully been accredited by the GSMA SAS can apply for the necessary certificates from the GSMA Certificate Issuer (CI) to participate in the GSMA approved M2M ecosystem. In a nutshell, the GSMA approved ecosystem for remote provisioning of M2M eSIMs is a secure system.

2.33 In many countries of the world, SM-SR is owned and managed by either a TSP or an original equipment manufacturer (OEM) or a third party such as M2MSP. At present, for domestically issued eUICCs in India, the controlling SM-SR is being

[28] PKI is an acronym of 'public key infrastructure'.
[29] https://www.gsma.com/esim/compliance/

owned and managed by the licensed TSPs. With a view to explore the possibility of owning and managing SM-SR by non-TSP entities such as OEMs and M2MSPs, the Authority solicited, through the CP dated 25.07.2022, comments of stakeholders on the following question:

Q6. Whether non-TSP entities, such as OEM 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?

(1) Responses of stakeholders on the Q6

2.34 In response to the above question, two types of views have been received from stakeholders, as outlined below:

(a) View-1: Non-TSP entities, such as OEMs and M2MSPs, should also be permitted to own SM-SR.

(b) View-2: The ownership of SM-SR and SM-DP should continue to remain with only TSPs.

2.35 A summary of the comments received from the stakeholders, who have opined that non-TSP entities should be permitted to own SM-SR, is given below:

(a) For supporting innovation and growth, M2MSPs, registered under DoT's guidelines, should be allowed to own, and manage SM-SR as long as they have to follow the same rules as the one imposed on TSPs. Any M2MSP, willing to manage subscription, may deploy its own SM-SR and integrate it with the interested TSPs as per the GSMA standards.

(b) The concerns of security and customer data privacy related concerns flagged by the Authority in the Consultation Paper have been addressed sufficiently under the 'Guidelines for Registration Process of M2M Service Providers (M2MSP) and WPAN/ WLAN Connectivity Provider for M2M Services' dated 08.02.2022 (M2MSP registration guidelines). Therefore, the entities desirous of owning SM-SR should be required to register under the M2MSP registration guidelines.

(c) As per global practice, application service providers, OEMs and M2MSPs own and manage SM-SR to cater to the requirements of their M2M connectivity, SIM profiling and SIM profile swapping. Similar standards should be followed in India and M2MSPs should be allowed to have their own SM-SR. This will provide greater flexibility and choice to OEMs and M2M users.

2.36 On the other hand, the stakeholders, who are of the view that the ownership of SM-SR and SM-DP should continue to remain with only TSPs, have contended that considering the Indian security requirements and the involvement of confidential data, SM platform (SM-DP and SM-SR) should be established only under the ownership of TSPs. This will help eliminate the risks involved with the misuse of customer profile data and will ensure secure profile storage and management of information.

(2) Analysis in respect of the Q6

2.37 The Authority took note of the fact that as per GSMA specifications, SM-SR plays an important role in the M2M services eco-system. It obtains the platform management credentials of the M2M eSIMs from the EUM (in case of initial registration) or establishes them through the previous SM-SR (in case of SM-SR swap). SM-SR 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. SM-SR holds a database of all the eUICCs under its control and the key sets used to manage them.

2.38 Considering the crucial role played by SM-SR in the M2M services eco-system, and the need for an adequate security of M2M eco-system in India, the Authority is of the view that the provision of SM-SR should be under an adequate regulatory oversight.

2.39 As far as TSPs are concerned, the Authority is of the view that the entities holding telecom service licenses, under which M2M services may be provided, should be permitted to own, and manage SM-SR, because such entities are integral

constituents of M2M ecosystem, and they are under an adequate regulatory oversight in the country.

2.40 The Authority noted that a few stakeholders have argued that the M2MSPs, which are registered under DoT's M2MSP Guidelines dated 08.02.2022, should also be allowed to own, and manage SM-SR if they follow the same rules as the one imposed on TSPs. In this regard, the Authority examined the level of regulatory oversight on M2MSP registrants vis-à-vis licensed telecom service providers. The Authority observed that the technical and security conditions imposed on M2MSP registrants are lighter than those imposed on licensed telecom service providers in the country. The Authority also took note of the fact that earlier, in accordance to the DoT's M2MSP Registration Guidelines dated 08.02.2022, only an Indian company, registered under the Indian Companies Act, 2013 or an LLP (Limited Liability Partnership) registered under LLP Act, 2008 or a partnership firm could be registered as M2MSP. However, through an addendum dated 01.01.2024 to the M2MSP Registration Guidelines, DoT has allowed all types of business entities such as company, Government Departments/ Organizations, Partnership Firms, LLPs, Institutions, Undertakings, Proprietorship Firms, Societies and Trusts to apply for M2MSP registration.

2.41 In light of the above facts, the Authority is of the view that M2MSP registered entities in the present form may not be permitted to own and manage SM-SR in the country. Essentially, the eligibility conditions as well as the technical and security conditions applicable for any entity to own and manage SM-SR should be enhanced over and above the conditions imposed on M2MSP registrants.

2.42 While examining eligibility conditions, the Authority noted that, as per the extant telecommunication service licensing framework in the country, only the companies registered under the Indian Companies Act are permitted to obtain service licenses from DoT. The Authority is of view that given the important role played by the entities holding SM-SR in the M2M eco-system, the entities holding SM-SR in India should be under an adequate corporate regulatory oversight. Accordingly, the Authority is of the view that an M2MSP registrant may be permitted to own and

manage SM-SR in the country if it is a company registered under the Indian Companies Act.

2.43 The Authority is also of the view that an M2MSP intending to own and manage SM-SR should be subjected to additional technical and security conditions over and above those applicable under the extant M2MSP Registration Guidelines. In this regard, the Authority has formulated additional terms and conditions to be fulfilled by M2MSP registrants, if they intend to own and manage SM-SR in India. The recommended additional terms and conditions to be fulfilled by the M2MSP registrants are enclosed as **Annexure-II** of these recommendations.

2.44 Further, as the SM-SR acts as a gateway between SM-DP and M2M eSIMs, the Authority is of the view that the entities eligible to own and manage SM-SRs should be permitted to interface with the SM-DPs held by the licensed telecom service providers in India, upon the request of concerned OEMs and M2MSPs. Such enablement will be required particularly for the M2MSPs, as they are not licensed entities. For this purpose, enabling provisions would require to be created in the relevant license/ authorization/ registration.

2.45 In view of the above, **the Authority recommends that –**

(a) The following entities should be permitted to own and manage SM-SRs in the country:

(i) Unified Access Service License holder;

(ii) Unified License (Access Service Authorization) holder;

(iii) Unified License (Machine-to-Machine Authorization) holder;

(iv) Unified License for VNO (Access Service Authorization) holder;

(v) Unified License for VNO (Machine-to Machine Authorization) holder; and

(vi) The companies holding M2MSP Registration with a specific permission to own and manage SM-SR in India.

The recommended additional terms and conditions to be imposed on M2MSP registrants for granting permission to own and manage SM-SR in India are enclosed as Annexure-II of these recommendations. These additional terms and conditions should be included in the DoT's 'Guidelines for Registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services' dated 08.02.2022 (as amended). DoT may include other conditions, as deemed fit.

(b) Each SM-SR site should be GSMA Security Accreditation Scheme for Subscription Management (SAS-SM) certified. The holders of SM-SR should submit a copy of the GSMA SAS-SM certificate to DoT before operationalizing any SM-SR in India.

(c) DoT should include suitable provisions in the relevant license/ authorization/ registration to enable the entities holding SM-SRs in India to interface their SM-SRs with the SM-DPs held by the licensed telecom service providers in the country, upon the request of the concerned OEMs/ M2MSPs.

D. Need for changing SM-SR from foreign entity to Indian entity in respect of the foreign M2M eSIMs fitted devices operating in India

2.46 Through the CP dated 25.07.2022, stakeholders' comments were invited on the following question:

Q2. Whether there is a need to change the controlling SM-SR from 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?

(1) Responses of stakeholders with respect to Q2

2.47 In response to the above question, contrasting views have been received from stakeholders. A few stakeholders have contended that the change of foreign SM-

SR to Indian SM-SR should be mandated for the eUICCs fitted in the devices imported to India. A summary of the inputs provided by such stakeholders is given below:

(a) The current practice of keeping the control of M2M eSIM with the foreign SM-SR, even after downloading and activating Indian TSP's profile on the eUICC is not ideal. The current practice leads to data collection by controlling SM-SR, which should not be permitted, once the Indian TSP's profile is downloaded on M2M eSIM. The migration of SM-SR should ideally be done to Indian SM-SR immediately on the downloading of Indian profile; however, it is possible that owing to this being a new intervention, more time may be required for the design, development, testing and integration process. Nevertheless, in any case, this timeline should not exceed one year.

(b) Change of controlling SM-SR from a foreign entity to an Indian entity may be considered to counter security and privacy concerns arising due to the sharing of sensitive data such as device location with foreign SM-SR. If such swapping is not done, it will be a security threat to all the end point devices, which are deployed in the critical use cases. SM-SR should move to India along with the profile.

2.48 On the other hand, many stakeholders are of the view that the change of foreign SM-SR to Indian SM-SR should not be mandated. The inputs of such stakeholders are given in brief as below:

(a) For a device assembled or manufactured outside India, an M2M eSIM is integrated with the device, and a bootstrap profile is burnt on the M2M eSIM through an SM-SR, located outside India. In case of import of such devices to India, change of foreign SM-SR to the Indian SM-SR should not be mandated; instead, the foreign SM-SR should be allowed to download Indian TSP's profiles on such M2M eSIMs. It would not be possible for say a Europe based business entity to deploy its SM-SR in India, just for the M2M eSIMs that roam in India. The profile data is fully encrypted and integrity protected in SM-DP before getting downloaded to M2M eSIM in

India via foreign SM-SR. It is only decrypted at the M2M eSIM which is anyways located in India. The SM-SR does not decrypt the profile data being downloaded by the SM-DP; instead, it provides a secure environment to download the profile. Besides, SM-SRs are also GSMA-SAS[30] security certified. To ensure security of the M2M eco-system, profile downloads on M2M eSIMs should be permitted from only those SM-SRs, which are security certified by GSMA.

(b) Change of SM-SR from a foreign entity to an Indian entity should not be mandated as it is a technically and commercially complicated process. Cross-border and cross-vendor SM-SR swaps are too complex and time consuming and can sometimes affect business viability thereby leading to loss of business and opportunities.

(c) From the business perspective, generally, the business responsible for the delivery and performance of eUICC fitted devices would want to retain control of the SM-SR function and not be forced to change it to a new TSP.

(d) While SM-DP should remain in India, the SM-SR should be allowed to be situated across the geographical boundaries on any GSMA certified site. In this case, the Indian TSP's profile will be downloaded on M2M eSIMs through an integration of Indian TSP's SM-DP with foreign SM-SR. The GSMA's framework for eSIM solutions is a comprehensive framework and has well defined interfaces with requisite security features. GSMA also provides certification to the sites for SM-DP/ SM-SR set-up; hence GSMA certification for the sites can be made as a requirement for using the SM-SR situated outside India.

(e) SM-SR swap is an exceptional scenario and most of stakeholders may not have adequate learning for SM-SR swap. Many stakeholders will be involved in changing SM-SR, such as service providers, end customers, SIM manufacturers etc. Therefore, in case the change of SM-SR is mandated, it may pose operational challenges. The eco-system is yet not matured to cater to the mandatory change of SM-SR at this stage. Considering challenges in mandatory change of SM-SR, integration of Indian TSP's SM-

[30] GSMA-SAS refers to GSMA's Security Accreditation Scheme.

DP with foreign SM-SR is a better alternative at this stage and it must be explicitly allowed. It would require the Indian TSP's profiles to be shared outside the Indian jurisdictions, which should be explicitly allowed in regulatory norms.

(f) The SM-DP/ SM-SR architecture, which is certified by GSMA, is a secure architecture. As the profile is securely encrypted and routed from the SM-DP to the M2M eSIM, any tampering with the profiles is difficult. As the SM-SR does not have access to any sensitive data, there are no privacy issues in keeping SM-SRs outside India.

2.49 A few stakeholders, who are of the view that the change of foreign SM-SR to Indian SM-SR should not be mandated, have opined that in some cases, there may be a need for changing SM-SR from a foreign entity to an Indian entity; in such cases, change of the controlling SM-SR from foreign entity to an Indian entity should be facilitated by explicitly allowing it in the DoT's guidelines; however, the change of SM-SR should be carried out as per GSMA's prescribed process; proprietary solutions should not be allowed. Such stakeholders have suggested that TRAI should recommend a flexible approach and explicitly allow both the options viz. integration of Indian SM-DP with foreign SM-SR as well as change of controlling SM-SR from foreign to India.

(2) Analysis in respect of the Q2

2.50 In the para 2.20 above, the Authority has recommended that all communication profiles on any M2M eSIM fitted in an imported device on international roaming in India should be mandatorily converted/ reconfigured into communication profiles of Indian telecom service providers within six months from the date of activation of international roaming on such M2M eSIM. This would require communication profiles of Indian telecom service providers to be installed in M2M eSIMs on international roaming prior to the removal of the profiles of foreign telecom service providers. For downloading a profile of a new TSP on any M2M eSIM, GSMA

framework for remote SIM provisioning provides two separate subscription management specifications as given below:

(a) Profile interoperability: Using this feature, a new profile coming from any SM-DP can be downloaded in the eUICC via the existing SM-SR, after integration of the new SM-DP with the existing SM-SR, as depicted below. This scenario does not require change of SM-SR.

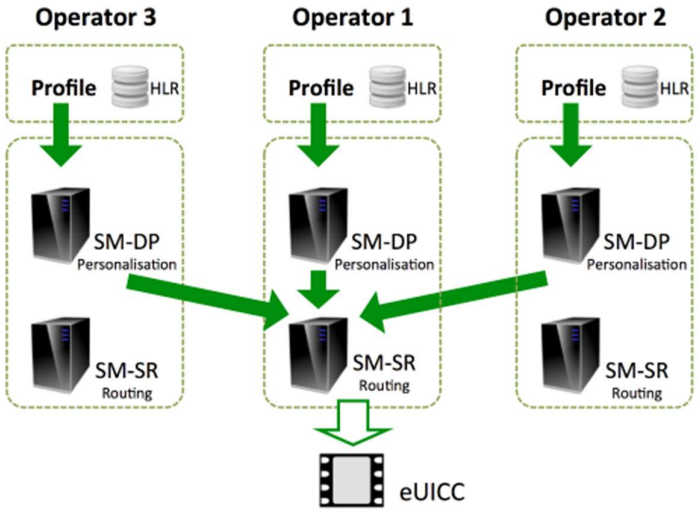

Figure 2.2: Profile interoperability[31] through integration of SM-DP of another operator with the existing SM-SR

(b) SM-SR switch process: In SM-SR switch process, the SM-SR linked with an eUICC can be replaced with another SM-SR, as depicted below. SM-SR switch requires keys to be exchanged between the two SM-SRs. After completion of the SM-SR switch, a new profile can be downloaded to the eUICC via the new SM-SR.

[31] https://www.gsma.com/iot/wp-content/uploads/2015/02/CLP.05-v1.0-BPD.pdf

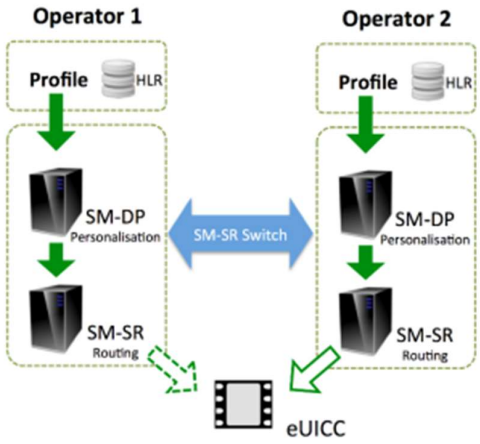

Figure 2.3: SM-SR Switch[32]

2.51 The Authority noted that the amongst the afore-mentioned features of GSMA remote SIM provisioning framework, the profile inter-operability feature is simpler as it obviates the need for SM-SR switch, prior to downloading the profile of another TSP on an M2M eSIM.

2.52 The Authority notes that on the issue as to whether there is a need to change the controlling SM-SR from a foreign entity to an Indian entity in case of foreign eUICC fitted devices operating in India, the core arguments of stakeholders are as follows:

(a) Argument in support of mandating SM-SR swap: If SM-SR is not changed from foreign to Indian, it will lead to data collection by foreign SM-SR; the sharing of sensitive data such as device location with a foreign SM-SR may give rise to security and privacy concerns.

(b) Arguments against mandating SM-SR swap:

(i) SM-SR swap is an exceptional scenario. It can be too complex and time consuming and can sometimes affect business viability. It is a technically and commercially complicated process. Most of the stakeholders may not have adequate learning of SM-SR swap. At this stage, the eco-system is not fully matured to cater to mandatory SM-SR swap. In case SM-SR swap is mandated, it may pose operational challenges. Instead of

[32] https://www.gsma.com/iot/wp-content/uploads/2015/02/CLP.05-v1.0-BPD.pdf

mandating SM-SR swap, profile switching should be allowed through integration of Indian TSP's SM-DP with foreign SM-SR.

(ii) Under the remote SIM provisioning framework of GSMA for M2M eSIMs, the profile data is fully encrypted, and integrity protected in SM-DP. The SM-SR does not decrypt the profile. It is only decrypted in M2M eSIMs, which are anyway located in India.

2.53 While examining the afore-mentioned arguments of stakeholders, the Authority took note of the following aspects:

(a) As per GSMA specifications for M2M eSIM, SM-SR provides a secured link for downloading the encrypted profile from SM-DP into the M2M eSIM. SM-SR does not decrypt profile data.

(b) For installing the profiles of Indian telecom service providers on M2M eSIMs prior to the removal of the profiles of foreign telecom service providers, GSMA's framework for M2M eSIMs provides two alternatives viz. -

(i) profile download through the existing (foreign) SM-SR of the M2M eSIMs after integrating the Indian TSP's SM-DP with foreign SM-SR; or

(ii) SM-SR switch (also referred to as 'SM-SR swap') from foreign to Indian, followed by profile download through the new (Indian) SM-SR.

(c) SM-SR switch is a complex activity[33]. It involves a complicated and expensive[34] process[35].

2.54 Keeping in view the comments of stakeholders and further analysis, the Authority is of the view that, at present, the M2M eco-system is not mature enough for mandating SM-SR swap, though it may be kept as an option. Mandating SM-SR swap may entail operational challenges, at this stage. This is neither essential. GSMA framework for remote SIM provisioning provides alternative solutions for

[33] https://webbingsolutions.com/will-gsma-sgp-32-mark-a-new-dawn-for-iot/ [Although it's technically possible to change a SM-SR, in practice it's very difficult to switch devices from one Operator's SM-SR to the other, since it requires legal contracting between competitors. It might become very complex, and very often is just not feasible.]

[34] https://www.emnify.com/blog/iot-esim-myths [The SM-SR swap involves a six-digit expense.]

[35] https://www.comreg.ie/media/2021/11/ComReg-21114a.pdf [To do SM-SR swap, operator A and operator B need to connect their SM-SRs so that data about the eSIMs is exchanged between them. Then the new SM-SR is the sole SM-SR connected to the eSIMs and serves them with the new profile data. Commercially, it is possible for the previous operator to charge the customer to facilitate the switch. This charge would in this model most likely come as a one-time fee.]

profile switching such as profile inter-operability through integration of SM-DP of another operator with the existing SM-SR. As SM-SR does not decrypt the profile data being downloaded from SM-DP to the M2M eSIM, the profiles of Indian telecom service providers on M2M eSIMs deployed in the devices imported in India may be allowed to be installed through the existing (foreign) SM-SR if the foreign SM-SR is GSMA-SAS security certified. As M2M ecosystem is at an early stage of growth, it would be preferable to provide flexibility to the customers, rather than prescribing an arduous mechanism for switching SM-SR.

2.55 The Authority noted that one of the stakeholders, who has stated that the integration of Indian TSP's SM-DP with foreign SM-SR is a better alternative at this stage, has also mentioned that such integration would require the Indian TSP's profile to be shared outside the Indian jurisdictions, which must be explicitly allowed in regulatory norms. The Authority is of the view that enabling provisions should be created in the relevant telecommunication service licenses to permit the integration of the SM-DP of Indian TSP with the foreign SM-SR. The Authority will monitor the development of the M2M services ecosystem and may revisit its viewpoint on this matter at an appropriate time.

2.56 Considering the comments of stakeholders and further analysis, **the Authority recommends that –**

(a) for installation of profiles of Indian TSPs on M2M eSIMs fitted in the devices imported in India, the concerned OEM and M2MSP should be given the flexibility to choose between the following options under the GSMA framework for remote SIM provisioning -

(i) profile download from the SM-DP of the Indian TSP to the M2M eSIMs through the existing (foreign) SM-SR, if the foreign SM-SR is GSMA-SAS security certified; or

(ii) profile download from the SM-DP of the Indian TSP to the M2M eSIMs through the new (Indian) SM-SR, after SM-SR switch from foreign to Indian.

(b) To implement the recommendation (a)(i) above, DoT should include enabling provisions for permitting the integration of the SM-DP of Indian TSP with the foreign SM-SR in the relevant telecommunication service licenses viz. -

(i) Unified Access Service License;

(ii) Unified License (Access Service Authorization);

(iii) Unified License (Machine-to-Machine Authorization);

(iv) Unified License for VNO (Access Service Authorization); and

(v) Unified License for VNO (Machine-to Machine Authorization).

(c) The Authority will monitor the development of the M2M communication services ecosystem and may review this recommendation at an appropriate time.

E. Need for integration of SM-SR of each TSP with the SM-DP of each other TSP

2.57 Through the CP dated 25.07.2022, stakeholder's inputs were solicited 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.

(1) Responses of stakeholders on the Q3

2.58 In response to the afore-mentioned question, contrasting views have been received from stakeholders. A couple of stakeholders have favoured mandatory integration of the SM-SR of each TSP with the SM-DPs of other TSPs. A summary of comments received from such stakeholders is given below:

(a) Integration of SM-SRs with SM-DPs should be mandatory to avoid monopolization of business. It provides not only flexibility in the business but also transparency. Such integration is well defined by GSMA. A period of six

months should be enough for integration as all TSPs in India are well prepared for it.

(b) To achieve compatibility, SM-SRs and SM-DPs should be inter-operable with each other.

2.59 On the other hand, most stakeholders have opposed mandatory integration of the SM-SR of each TSP with the SM-DPs of other TSPs. A summary of the comments received from such stakeholders is given below:

(a) There is no need for a regulatory intervention for integration between SM-DPs and SM-SRs of Indian TSPs. At present, the M2M ecosystem is in a nascent stage, and the market for eUICC fitted devices needs development and innovation. Therefore, market forces should be allowed to work.

(b) At present, there are no use cases requiring downloading of one TSP's profile on an eUICC controlled by SM-SR of another TSP. However, considering the evolving use cases, this possibility cannot be ruled out. Therefore, integration of the SM-SR of each TSP with the SM-DPs of other TSPs should be driven by the customer requirement, if established in due course of time.

(c) Keeping in mind the successful cooperation between various market participants in designing and implementing working solutions for carrier switching for M2M, and the absence of any demonstrable market failure, a regulatory mandate to require number porting or other switching mechanisms is premature and unjustified. Stakeholders should be free to pursue a choice of commercial models and technical solutions and accommodate switching where appropriate for the device and circumstances. However, no obligations on such switching should be imposed.

(2) Analysis in respect of the Q3

2.60 While analysing the issue, the Authority took note of the following aspects:

(a) GSMA has prescribed specifications for integration of SM-SR with SM-DP. The integration of SM-SR with SM-DP is an involved exercise, which requires technical intervention at both the servers: SM-DP and SM-SR.

(b) The integration of an SM-SR with a new SM-DP needs to be undertaken only when there is a requirement to add profiles of another TSP on the M2M eSIMs controlled by the SM-SR. A need for such integration arises infrequently.

2.61 Considering the comments received from stakeholders and further analysis, the Authority is of the view that mandatory integration of the SM-SR of each TSP with the SM-DPs of other TSPs is not required, at this stage. However, the concerned M2MSP/ OEM should be mandatorily facilitated whenever it intends to add profiles of another licensed telecom service provider on the M2M eSIMs subscribed by it. Specifically, if an M2MSP/ OEM intends to add profiles of another licensed telecom service provider on the M2M eSIMs subscribed by it, the M2MSP registrant/ telecommunication service licensee, whose SM-SR controls the M2M eSIMs, should mandatorily facilitate integration of its SM-SR with the SM-DP of the licensed telecom service provider, whose communication profiles are to be installed in the M2M eSIMs. The integration of SM-SR with the SM-DP should be carried out in accordance to the GSMA's specifications. The Authority is of the view that a period of three months would be sufficient for the completion of such an integration.

2.62 Accordingly, **the Authority recommends that the M2MSP registrant/ telecommunication service licensee, whose SM-SR controls M2M eSIMs in India, should not refuse integration of its SM-SR with the SM-DP of the licensed telecom service provider, whose profiles are to be added in such M2M eSIMs, upon the request of the concerned OEM/ M2MSP. The integration of SM-SR with SM-DP should be carried out in accordance to the GSMA's specifications and should be completed within a period of three months from the date of receipt of the formal request from the concerned OEM/ M2MSP.**

F. Need for prescribing SM-SR swapping among Indian TSPs

2.63 In the CP dated 25.07.2022, the Authority envisaged that a situation may arise in which a customer may want to discontinue the subscription of the current TSP

(whose SM-SR is currently controlling its eUICC) and switch to another TSP. This situation will require an SM-SR swap from the existing TSP to the other TSP. To make this possible, there could be a need to mandate TSPs for carrying out SM-SR swap, as per the request of customers. In this regard, through the CP dated 25.07.2022, the Authority solicited comments from stakeholders 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.

(1) Responses of stakeholders on the Q4

2.64 In response to the above question, three kinds of views have been received from stakeholders:

(a) View-1: There is a need to prescribe SM-SR swapping among the Indian TSPs.

(b) View-2: SM-SR swapping among the Indian TSPs should not be mandatory.

(c) View-3: SM-SR swapping among the Indian TSPs should be facilitated upon the customer's request.

2.65 Only a couple of stakeholders have favoured the prescription of SM-SR swapping among the Indian TSPs. In support of their viewpoint, they have contended that for achieving compatibility, all vending parties' SM-SR and SM-DPs must be inter-operable with each other.

2.66 A few stakeholders have opposed mandating SM-SR swapping among the Indian TSPs. A summary of the viewpoint of such stakeholders is given below:

(a) Indian TSPs are already licensed and regulated by DoT/ TRAI. Such licensing and regulatory norms apply equally to all Indian TSPs and there is no concern related to security requirements or level-playing field, which may merit the need for SM-SR swapping. To meet the requirement of change in profile of an Indian TSP with another TSP, there should be integration of SM-DP and SM-SR among Indian TSPs which may cater all customer requirements.

(b) SM-SR swap is an exceptional scenario and most of stakeholders may not have adequate learning. There will be many stakeholders involved in transferring the SM-SR which may pose operational challenges.

(c) There is no need for regulatory intervention for SM-SR swap among Indian TSPs. It should be left to the market forces.

2.67 On the other hands, many stakeholders have suggested a middle path. They have opined that SM-SR swapping among the Indian TSPs should be facilitated upon the customer's request. A summary of the viewpoint of such stakeholders is given below:

(a) The option of SM-SR swapping amongst Indian TSPs must be available with the customer. The TSPs should facilitate other TSPs and M2MSPs to migrate from their profile to other TSP's profile through its own SM-SR. Switching of TSP is required to provide the necessary flexibility to the end users which will be like the MNP options available to the mobile users in India. Hence, the end user may be allowed to switch SM-SR from existing SM-SR provider to another SM-SR provider as per its choice and all these options should be facilitated by the existing SM-SR provider via SM-SR swap.

(b) In case an Indian SM-SR provider is shutting down services, it should be mandated to provide services and migration support for a reasonable period after sending closure notice to customers. This will allow customers to choose another operator and ensure smooth migration to new SM-SR.

(2) Analysis in respect of the Q4

2.68 The issue of SM-SR swap from foreign to Indian has already been analyzed above in the section related to the Q2. The Authority is of the view that SM-SR swap is a complex activity, which involves a complicated and expensive process, and therefore, it should not be generally resorted to. However, there could be some exceptional scenarios requiring SM-SR swap, such as below:

(a) The entity, which is holding the controlling SM-SR of the M2M eSIMs of an OEM/ M2MSP, is about to shut down its services.

(b) The OEM/ M2MSP wants to surrender all the M2M eSIM cellular mobile connections subscribed from a licensed telecom service provider, which also owns the controlling SM-SR of such M2M eSIMs. After the surrender, the customer intends to subscribe M2M eSIM cellular mobile connections from another licensed telecom service provider and intends to swap the controlling SM-SR to another entity.

2.69 In the scenarios like the ones mentioned above, it would be necessary to facilitate SM-SR swap upon the request of the concerned OEM/ M2MSP.

2.70 In view of the comments of stakeholders and further analysis, the Authority is of the view that even though in most of the cases, the profile switchover between Indian TSPs can be done easily by way of integration of SM-DP of the new TSP with the existing SM-SR, customers might have to resort to SM-SR switching in exceptional circumstances. In such cases, SM-SR switching between Indian TSPs should be mandatorily facilitated upon the request of concerned OEM/ M2MSP. Such SM-SR switching should be carried out in accordance to the GSMA's specification. The Authority is of the view that a period of six months would be sufficient for completion of such switching.

2.71 Considering the above, **the Authority recommends that the M2MSP registrant/ telecommunication service licensee, whose SM-SR controls M2M eSIMs in India, should mandatorily facilitate switching of its SM-SR with the SM-SR of another entity, eligible to hold SM-SR in India, upon the request of the concerned OEM/ M2MSP. Such SM-SR switching should be carried out as per the GSMA's specifications and should be completed within a period of six months from the date of receipt of the formal request from the concerned OEM/ M2MSP.**

G. Need for permitting ITU allocated shared Mobile Country Code 901.XX (Global IMSI) in India

2.72 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 not used for dialing purposes in the public switched network. The IMSI is required so that a visited network[36] can identify a roaming mobile terminal or mobile user, e.g. in order to query a subscriber's home network for subscription and billing information.

2.73 The IMSI is a string of decimal digits, up to a maximum length of 15 digits, which identifies a unique mobile terminal or mobile subscriber internationally. The IMSI consists of three fields viz.

(a) Mobile Country Code (MCC),
(b) Mobile Network Code (MNC), and
(c) Mobile Subscriber Identification Number (MSIN).

2.74 Mobile Country Code (MCC): The MCC is the first field of the IMSI and is three digits in length. An MCC either identifies a country or a group of networks that share an MCC for international services.

2.75 Mobile Network Code (MNC): The MNC is the second field of the IMSI and is two to three digits in length. The MNC, in combination with the MCC, uniquely identifies the home network of the mobile terminal or mobile user.

2.76 Mobile Subscriber Identification Number (MSIN): The MSIN is the third field of the IMSI and is maximum of 10 digits. The MSIN, within a given MCC + MNC, identifies a unique mobile terminal or mobile subscriber within a public network.

[36] Visited network is the network providing service to a user when the user roams outside the home network.

2.77 Telecommunications Standardization Bureau (TSB)[37], a body within ITU-T, assigns MCCs to countries and assigns MCCs to be shared by Networks. MNCs are administered by the designated administrator within each country or by TSB in the case of Networks. MSINs are administered by the MNC assignee.

2.78 TSB has assigned shared Mobile Country Code 901 for extra-territorial use. The IMSI range with MCC 901.XX has no ties to any single country. 'XX' is the Mobile Network Code (MNC), assigned and administered by ITU-TSB. A written request for obtaining 901.XX IMSI must be submitted to the director of the ITU-TSB. The IMSI range 901.XX is also referred to as global IMSI range. Global IMSI ranges enable 'global SIMs' cross-border connectivity.

2.79 Global IMSIs have traditionally been used for maritime and aerospace connectivity for satellite connectivity. Fresh interest in global IMSI ranges is now emerging from industry players working to offer global M2M and IoT services.

2.80 DoT in its reference letter dated 09.11.2021 mentioned that it received requests from stakeholders that –

(a) ITU allocated 901.XX MCC be recognized by DoT, as it is recognized globally by telecom standardization bodies like GSMA, BEREC, ARCEP-France etc.

(b) 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.

(c) 901.XX should not be considered in violation to national telecom policies, as it is specifically for IoT use cases and will never be used as consumer communications.

[37] TSB provides secretarial support for the work of the ITU-T Sector and services for the participants in ITU-T work, diffuses information on international telecommunications worldwide and establishes agreements with many international Standards Development Organizations.
Source: https://www.itu.int/en/ITU-T/info/tsb/Pages/geninfo.aspx

(d) 901.XX MCC should be considered as an innovative service in telecommunication and should not be under strict telecom restrictions as it does not use any national scarce resource.

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

2.81 In this regard, through the CP dated 25.07.2022, the Authority solicited comments of stakeholders 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.

(1) Responses of stakeholders on the Q7

2.82 In response to the above question, broadly three kinds of views have been received from stakeholders, as outlined below:

(a) View-1: Mobile Country Code 901.XX (Global IMSI) should be permitted in India for M2M communication.

(b) View-2: It will not be appropriate to permit Mobile Country Code 901.XX (Global IMSI) for M2M communication in India.

(c) View-3: 901.XX IMSI series should be permitted for a limited period on M2M eSIMs on international roaming in India. Beyond this period, the profile of Indian operators should be configured into such M2M eSIMs.

2.83 A summary of comments of the stakeholders, who have favored permitting Mobile Country Code 901.XX (Global IMSI) in India for M2M Communication, is given below:

(a) 901.XX IMSI series is recognized by telecom standardization and many of the operators. IoT service providers around the world have been allotted this series by ITU for global IoT deployments. Hence, 901.XX IMSI series should be recognized by TRAI/ DoT for use for IoT/ M2M usage by M2MSPs. The M2MSPs

are regulated by DoT under the M2MSP registration guidelines. The M2MSP registration guidelines impose requirements such as inspections, security conditions etc. on M2MSPs, which make them highly regulated entities, in line with national security interests. M2MSPs are also required to ensure maintenance of records of end users of devices. M2MSP registration guidelines specify that M2MSPs have to inform DoT about the location of IT and network systems, which will ensure that DoT is informed about the application server location of M2MSPs. The 901.XX IMSI owner can provide a mirror of the traffic when requested to the Indian regulatory authorities. This can even be managed through the local TSPs, on whose networks, connectivity will be provided. Security obligations have already been placed by DoT on M2MSPs in the M2MSP registration guidelines.

(b) 901.XX IMSI series should be allowed under international roaming arrangements. With reference to the TRAI's recommendations to convert the international roaming connections to local connections, if regulations of every country make it mandatory for the 901.XX IMSI series to be converted to a local connection after a defined period, the whole basis of the ITU in setting up 901.XX exclusively for cross-border M2M use-cases will be defeated. Therefore, an exception should be made to the 901.XX IMSI series to ensure that these IMSIs work in India in line with the global practices adopted for M2M business.

2.84 The comments of the stakeholders, who have opposed permitting Mobile Country Code 901.XX (Global IMSI) in India for M2M Communication, may be summarized as below:

(a) There will be security issues with the use of 901.XX series as there will be no mode to monitor the devices with this series and it will not be possible to impose Indian regulations such as restrictions placed by DoT on such numbers. DoT has specified that mobile based M2M services have to follow 13-digit numbering; these 13-digit numbers are required to comply with the restrictive features for voice, data, and SMS, as prescribed by DoT from time to time. There will be no means to ensure compliance with Indian M2M oversight by the devices working with 901.XX numbers in India. In absence of

any such controls, global IMSIs can violate DoT's instructions dated 16.05.2018 and 30.05.2019 and can also remain on permanent roaming. This would be contrary to the temporary international roaming provided to foreign IMSIs, and if allowed, it may accentuate the problem. This will also lead to tilting the level-playing field.

(b) Furthermore, the interception of global IMSIs on the basis of IMSI/ MSISDN would be a challenge. There are other concerns as well in the use of these numbers for M2M services in India such as (i) home node mapping like HSS, PCRF, SCEF, (ii) routing aspects, (iii) how MSISDN to IMSI mapping be maintained for such IMSI series. The access authorizations are given separately for 22 licensed service areas (LSAs). This may give rise to the requirement of separate global IMSI series for each of its 22 LSAs and separate configurations in each of such LSAs. This would be a very complex process and use of 901.XX number will further complicate the existing arrangements.

(c) Global IMSI may become a security threat to the country. There is a concern as to where KYC is being managed. The serving TSP will have to take over the responsibility if any security threat occurs by the subscriber or data tunneling to foreign.

2.85 A few stakeholders have suggested a middle path. Such stakeholders include a few stakeholders who have opposed permitting 901.XX series in India for M2M communication. They have suggested that the global IMSI series for M2M should be treated as roaming IMSI in the network of Indian TSPs. A summary of their comments may be summarized as below:

(a) Any IMSI series which does not have Mobile Country Code of India should be treated as roaming IMSI in the network of Indian TSPs. As the entities owning the IMSI series would be global in nature, Indian Government would have limited capability to impose local M2M rules. This would pose concerns similar to foreign M2M eSIMs roaming in India.

(b) Global IMSIs can be used for limited use cases like that of an initial bootstrap and subsequently profile of Indian operator to be pushed as operational profile. This will ensure that the use of global IMSI does not create an issue of any

operational challenges of managing number series which is not owned by MNO/ VNO, lawful interception etc.

(c) Mobile Country Code 901.XX (Global IMSI) is already working in India as per International roaming arrangements. While the use of global IMSI can be permitted in India for IoT/ M2M use cases, global IMSI will fall under permanent international roaming if they do not involve the use of Indian TSP's profiles. This issue is similar to foreign M2M eSIMs on roaming in India which involves non-availability of KYC information and non-enforcement of restrictive features. Given the regulatory and security concerns, the international roaming SIMs with global IMSIs, allocated to foreign entities but operational in India, should be allowed to be used in India if these are mandatorily converted to Indian TSP profiles within six months.

(2) Analysis in respect of the Q7

2.86 In India, Department of Telecommunications (DoT) has formulated the National Numbering Plan 2003[38] (NNP 2003), which provides a set of rules and guidelines for the use and assignment of numbers to telephone services delivered over the public networks. In formulating NNP 2003, the dialing procedure as per ITU Recommendation E.164[39] has been followed. E.164-number is composed of a variable number of decimal digits arranged in specific code fields. The E.164-number code fields are the country code (CC) and the remaining fields are specific to the use being made.

2.87 The Mobile Station International Subscriber Directory Number[40] (MSISDN), and international mobile subscriber identity (IMSI) are two important numbers used for identifying a mobile subscriber in Public Land Mobile Network (PLMN). The IMSI is often used as a key in the home location register ("subscriber database") and the

[38] Source: https://dot.gov.in/sites/default/files/nnp2003_0_0.pdf?download=1

[39] ITU Recommendation E.164 provides the number structure and functionality for the five categories of numbers used for international public telecommunication: geographic areas, global services, networks, groups of countries (GoC) and resources for trials. For each of the categories, it details the components of the numbering structure and the digit analysis required to successfully route the calls.

[40] Mobile Station International Subscriber Directory Number (MSISDN) is commonly referred to as telephone number.

MSISDN is the number normally dialed to connect a call to the mobile phone. The MSISDN follows the numbering plan defined in the ITU Recommendation E.164. As indicated earlier in this section, IMSI is composed of MCC, MNC and MSIN. MCC is allocated by ITU-TSB.

2.88 As per the NNP 2003, DoT assigns mobile number series to be used as MSISDN and Mobile Network Code (MNC) to the licensed wireless access service providers in the country.

2.89 It is noteworthy that DoT allocates mobile number series and MNCs to Network Service Operators (NSOs) only, and not to any Virtual Network Operators (VNOs). As per the 'Guidelines for Grant of Unified License (Virtual Network Operators) dated 17.01.2022', *"[a]n NSO shall allocate a numbering range to their VNO(s) from the numbering range allocated to it by the Licensor. VNOs shall utilize the network codes of the parent NSO.*" Further, under the DoT's M2MSP Registration Guidelines dated 08.02.2022, DoT has not assigned any numbering resource to M2MSPs.

2.90 In short, at present, only the licensed wireless access service providers in the country can obtain numbering resources such as mobile number series, and Mobile Network Code (MNC) from DoT.

2.91 A few stakeholders have suggested that if ITU-STB allocates 901.XX IMSI series to M2MSPs in India, this IMSI series should be recognized by TRAI/ DoT as home IMSI and should not be treated as foreign IMSI. On the other hand, many other stakeholders have opined against it. While examining the comments of stakeholders, the Authority took note of the following aspects:

(a) Global IMSIs have traditionally been used for maritime and aerospace connectivity for satellite connectivity. Lately a few industry players have obtained global IMSIs from ITU to provide M2M and IoT services as well. Worldwide, the use of global IMSIs for eSIMs is still at an infant stage.

(b) Under NNP 2003, only the licensed wireless access service providers in the country can obtain numbering resources such as mobile number series, and Mobile Network Code (MNC) from DoT. Under the DoT's M2MSP registration

guidelines dated 08.02.2022, M2MSPs M2MSP have to take the telecom resources from an authorized telecom licensee having valid license under Indian Telegraph Act, 1885, to provide M2M services to third parties.

(c) The regulatory oversight, in terms of security conditions and technical conditions etc., imposed on M2MSPs under the M2MSP registration guidelines is much lighter than that on Unified Licensees. Further, DoT has imposed specific regulatory and security conditions on the licensed telecom service providers on the use of M2M eSIMs in the country in terms of restriction on voice, SMS and data usage and KYC requirements.

(d) The country has been divided into 22 licensed service areas (LSAs) for the purpose of granting access service licenses. DoT assigns a separate Mobile Network Code (MNC) for use in an LSA to licensed wireless access service providers in India. If a licensed wireless access service provider operates in all 22 LSAs in the country, DoT assigns to it 22 separate MNCs, one in each LSA. This framework works well for the identification of the home network of a mobile subscriber and the routing of telecommunication traffic in inter-circle roaming scenario. On the other hand, under the M2MSP registration framework in the country, M2MSP registration is granted on a national basis. Further, at present, ITU-TSB grants only one 901.XX IMSI to an applicant for global IMSI for IoT/ M2M communication. In other words, ITU-TSB can assign only one Mobile Network Code (MNC) to an M2MSP. In the Indian scenario with 22 LSAs, the assignment of a single MNC by ITU-TSB to a M2MSP in India, will not work well with the service area-based licensing framework in the country.

2.92 In view of the comments received from stakeholders and further analysis, **the Authority recommends that keeping in view the challenges in its implementation, the use of 901.XX IMSI series allocated by ITU-TSB to Indian entities should not be permitted for providing M2M services in India, at this stage. The Authority will monitor the developments in the M2M communication services ecosystem and may review this recommendation at an appropriate time**.

2.93 The Authority also examined the comments received from stakeholders that the 901.XX (global IMSI) series for M2M communication may be treated as roaming IMSI in the network of Indian TSPs. The Authority is of the view that treating any IMSI series, which does not have Mobile Country Code (MCC) of India, as roaming IMSI in the network of Indian TSPs does not pose any regulatory concern. Given the regulatory and security concerns, the imported devices fitted with M2M eSIMs with global IMSIs, allocated to foreign entities, may be allowed to be used in India with restriction on the period of international roaming in India, in a manner similar to the normal IMSIs i.e. all profiles of foreign telecom service providers configured in M2M eSIMs with global IMSIs should be removed within six months from the date of activation of international roaming.

2.94 In view of the comments of stakeholders and further analysis, **the Authority recommends that the M2M eSIMs with global IMSIs assigned to foreign entities should be treated like foreign M2M eSIMs working in international roaming in India, and all restrictions imposed on foreign M2M eSIMs working in international roaming in India should also be applied on the M2M eSIMs fitted with global IMSIs assigned to foreign entities.**

H. Issues pertaining to Consumer eSIMs

2.95 Through the CP dated 25.07.2022, stakeholders' comments were invited on the following question:

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.

(1) Responses of Stakeholders on the Q8

2.96 In response to the above question, a few stakeholders have stated that many handset manufacturers have introduced eSIM in their handsets and the trend is

expected to continue to grow. At present, there is no guideline allowing transfer of profile from one eSIM capable phone to another eSIM capable phone. In the case of physical SIM, this scenario is possible as customer can remove the SIM card from his old mobile phone and insert it into a new mobile phone. In the interest of consumer convenience and to prevent frauds, there is need for a standard process for transfer of profile from one eSIM capable phone to another eSIM capable phone if there is no change in KYC details.

(2) Analysis in respect of the Q8

2.97 The Authority examined the comments received from stakeholders in respect of the standard process for transfer of profile from one eSIM capable phone to another eSIM capable phone. The Authority observed that, at present, there are no standard solutions for device-to-device transfer of profiles on consumer eSIMs. The Authority is of the view that there is a need for detailed technical deliberations on the issue of device-to-device transfer of profiles on consumer eSIMs before arriving at a standard process for this purpose. In India, Telecom Engineering Centre (TEC), which is a technical body of DoT, develops standards for telecommunication sector in the country. TEC can obtain inputs from relevant stakeholders and examine the possibility of devising a standard process for device-to-device transfer of profiles on consumer eSIMs.

2.98 In view of the above, **the Authority recommends that the Government, through Telecom Engineering Centre (TEC), the technical arm of DoT, may examine the possibility of devising a standard process for device-to-device transfer of profiles on consumer eSIMs.**

I. Miscellaneous Issues

2.99 Through the CP dated 25.07.2022, stakeholders were requested to give comments on any related matter that is not covered in the consultation paper. In response, a

few stakeholders have brought to the attention of the Authority certain concerns related to eSIM, as summarized below:

(a) The restriction on the maximum number of public IPs/ URLs currently applicable for eSIMs should be relaxed.

(b) In the case of service barring orders issued by the competent authorities due to the law and order situations, the 13-digit M2M telephone numbers should be exempted.

(c) To enable use cases such as import of vehicles and devices from global manufacturers, eSIM production outside India should be permitted. Personalization of eSIM at non-India location should be permitted.

2.100 The afore-mentioned suggestions have issues beyond the scope of the present consultation and will be examined as and when DoT sends a reference on such issues to TRAI for making recommendations.

2.101 The following chapter provides a summary of recommendations.

CHAPTER 3
SUMMARY OF RECOMMENDATIONS

3.1 Earlier, through the recommendation No.5.7(b) of the recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that *"[d]evices fitted with eUICC shall be allowed in operation in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP's SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition based on the developments and requirements".*

Based on a review of the said recommendation, the Authority recommends that all communication profiles on any M2M eSIM fitted in an imported device on international roaming in India should be mandatorily converted/ reconfigured into communication profiles of Indian telecom service providers within a period of six months from the date of activation of international roaming in India on such M2M eSIM or on change of ownership of the device, whichever is earlier.

[Para 2.20]

3.2 The Authority recommends that the switch-over of the communication profile on M2M eSIMs from one licensed telecom service provider (TSP) to another TSP should be driven by the concerned Original Equipment Manufacturer (OEM) of the devices containing M2M eSIMs.

[Para 2.29]

3.3 The Authority recommends that –

(a) The following entities should be permitted to own and manage SM-SRs in the country:

(i) Unified Access Service License holder;

(ii) Unified License (Access Service Authorization) holder;

(iii) Unified License (Machine-to-Machine Authorization) holder;

(iv) Unified License for VNO (Access Service Authorization) holder;

(v) Unified License for VNO (Machine-to Machine Authorization) holder; and

(vi) The companies holding M2MSP Registration with a specific permission to own and manage SM-SR in India.

The recommended additional terms and conditions to be imposed on M2MSP registrants for granting permission to own and manage SM-SR in India are enclosed as Annexure-II of these recommendations. These additional terms and conditions should be included in the DoT's 'Guidelines for Registration process of M2M Service Providers (M2MSP) & WPAN/WLAN Connectivity Providers for M2M Services' dated 08.02.2022 (as amended). DoT may include other conditions, as deemed fit.

(b) Each SM-SR site should be GSMA Security Accreditation Scheme for Subscription Management (SAS-SM) certified. The holders of SM-SR should submit a copy of the GSMA SAS-SM certificate to DoT before operationalizing any SM-SR in India.

(c) DoT should include suitable provisions in the relevant license/ authorization/ registration to enable the entities holding SM-SRs in India to interface their SM-SRs with the SM-DPs held by the licensed telecom service providers in the country, upon the request of the concerned OEMs/ M2MSPs.

[Para 2.45]

3.4 The Authority recommends that –

(a) for installation of profiles of Indian TSPs on M2M eSIMs fitted in the devices imported in India, the concerned OEM and M2MSP should be given the flexibility to choose between the following options under the GSMA framework for remote SIM provisioning -

(i) profile download from the SM-DP of the Indian TSP to the M2M eSIMs through the existing (foreign) SM-SR, if the foreign SM-SR is GSMA-SAS security certified; or

(ii) profile download from the SM-DP of the Indian TSP to the M2M eSIMs through the new (Indian) SM-SR, after SM-SR switch from foreign to Indian.

(b) To implement the recommendation (a)(i) above, DoT should include enabling provisions for permitting the integration of the SM-DP of Indian TSP with the foreign SM-SR in the relevant telecommunication service licenses viz. -

(i) Unified Access Service License;

(ii) Unified License (Access Service Authorization);

(iii) Unified License (Machine-to Machine Authorization);

(iv) Unified License for VNO (Access Service Authorization); and

(v) Unified License for VNO (Machine-to Machine Authorization).

(c) The Authority will monitor the development of the M2M communication services ecosystem and may review this recommendation at an appropriate time.

[Para 2.56]

3.5 The Authority recommends that the M2MSP registrant/ telecommunication service licensee, whose SM-SR controls M2M eSIMs in India, should not refuse integration of its SM-SR with the SM-DP of the licensed telecom service provider, whose profiles are to be added in such M2M eSIMs, upon the request of the concerned OEM/ M2MSP. The integration of SM-SR with SM-DP should be carried out in accordance to the GSMA's specifications and should be completed within a period of three months from the date of receipt of the formal request from the concerned OEM/ M2MSP.

[Para 2.62]

3.6 The Authority recommends that the M2MSP registrant/ telecommunication service licensee, whose SM-SR controls M2M eSIMs in India, should mandatorily facilitate switching of its SM-SR with the SM-SR of another entity, eligible to hold SM-SR in India, upon the request of the concerned OEM/ M2MSP. Such SM-SR switching should be carried out as per the GSMA's specifications and should be completed within a period of six months from the date of receipt of the formal request from the concerned OEM/ M2MSP.

[Para 2.71]

3.7 The Authority recommends that keeping in view the challenges in its implementation, the use of 901.XX IMSI series allocated by ITU-TSB to Indian entities should not be permitted for providing M2M services in India, at this stage. The Authority will monitor the developments in the M2M communication services ecosystem and may review this recommendation at an appropriate time.

[Para 2.92]

3.8 The Authority recommends that the M2M eSIMs with global IMSIs assigned to foreign entities should be treated like foreign M2M eSIMs working in international roaming in India, and all restrictions imposed on foreign M2M eSIMs working in international roaming in India should also be applied on the M2M eSIMs fitted with global IMSIs assigned to foreign entities.

[Para 2.94]

3.9 The Authority recommends that the Government, through Telecom Engineering Centre (TEC), the technical arm of DoT, may examine the possibility of devising a standard process for device-to-device transfer of profiles on consumer eSIMs.

[Para 2.98]

Annexure I

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)

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

RECOMMENDED ADDITIONAL TERMS AND CONDITIONS FOR M2MSP REGISTRANTS WITH PERMISSION TO OWN AND MANAGE SM-SRs IN INDIA

[To be included in the DoT's 'Guidelines for Registration process of M2M Service Providers (M2MSP) & WPAN/ WLAN Connectivity Providers for M2M Services' dated 08.02.2022 (as amended)]

A. Additional definitions

1. **"Embedded SIM** (**eSIM)"** means machine-to-machine form factor (MFF2). It is soldered directly to the M2M device's motherboard, fully encased in the device. The eSIM is the hardware component of the SIM and a physical form that can be soldered into a solution. On the other hand, eUICC refers to the software component of eSIM that provides the capability to store multiple network profiles that can be provisioned and managed Over-the-Air (OTA).

2. **"Embedded SIM Remote Provisioning Architecture"** means the common global GSMA architecture framework which provides a single, de-facto standard mechanism for the remote provisioning and management of M2M connections, allowing the OTA remote provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another. The GSMA's remote provisioning architecture consists of various inter-related entities, viz. eUICC, eUICC Manufacturer (EUM), M2M Device, Mobile Network Operator (MNO), M2M Service Provider (M2M SP), Certificate Issuer (CI), Subscription Manager-Data Preparation (SM-DP) and Subscription Manager- Secure Routing (SM-SR).

3. **"Subscription Manager-Data Preparation (SM-DP)"** 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. It must be GSMA SAS-SM (Security Accreditation Scheme for Subscription Management) certified.

4. **"Subscription Manager-Secure Routing (SM-SR)"** obtains the platform management credentials of the eUICC from the EUM (in case of initial registration) or establishes 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 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.

5. **"Original Equipment Manufacturer (OEM)"** is an organization that makes devices containing M2M eSIM.

6. **"Communication Profile"** comprises of the mobile network operator data related to subscription, including the operator's credentials.

B. Additional eligibility conditions

7. An applicant, if it is an Indian company registered under the Indian Companies Act, may seek permission for owning and managing SM-SRs in India at the stage of submitting application for 'Registration of M2M Service Provider (M2MSP) & WPAN/ WLAN Connectivity Provider for M2M Services'.

8. Any existing M2MSP registrant, if it is an Indian company registered under the Indian Companies Act may separately seek permission for owning and managing SM-SRs in India.

9. A non-refundable processing fee of Rs. fifty thousand (Rs. 50,000/-) shall be payable separately at the time of seeking permission for owning and managing

SM-SRs in India.

C. Additional technical conditions

10. Each SM-SR site shall be GSMA Security Accreditation Scheme for Subscription Management (SAS-SM) certified. The Registrant shall submit a copy of the GSMA SAS-SM certificate to DoT before operationalizing any SM-SR in India.

11. The Registrant, whose SM-SR controls M2M eSIMs in India, shall not refuse integration of its SM-SR with the SM-DP of the licensed telecom service provider, whose communication profiles are to be added in such M2M eSIMs upon the request of the concerned OEM/ M2MSP. The integration of SM-SR with SM-DP shall be carried out in accordance with the GSMA's specifications and shall be completed within a period of three months from the date of receipt of the formal request from the concerned OEM/ M2MSP.

12. The Registrant, whose SM-SR controls M2M eSIMs in India, shall mandatorily facilitate switching of its SM-SR with the SM-SR of another entity, eligible to hold SM-SR in India, upon the request of the concerned OEM/ M2MSP. Such SM-SR switching shall be carried out as per the GSMA's specifications and shall be completed within a period of six months from the date of receipt of a formal request from the concerned OEM/ M2MSP.

13. The Registrant shall be allowed to communicate with SM-DPs and other SM-SRs only for profile management of the M2M eSIMs as per GSMA specifications.

D. Additional security conditions

14. The Registrant shall adhere to the instructions/ guidelines issued by the Government in respect of connecting Trusted Products in the network.

15. The Registrant shall adhere to the instructions/ directions of the Licensor (i.e., DoT) issued from time to time in the interest of national security.

LIST OF ACRONYMS

Acronyms	Description
3GPP	3rd Generation Partnership Project
APN	Access Point Name
CI	Certificate Issuer
CP	Consultation Paper
DoT	Department of Telecom
eUICC	Embedded Universal Integrated Circuit Card
EID	eUICC-ID
EUM	eUICC Manufacturer
GSMA	Groupe Speciale Mobile Association
ICCID	Integrated Circuit Card Identifier
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector
J&K	Jammu & Kashmir
KYC	Know Your Customer
LDS	Local Discovery Service
LoRa	Long Range
LPAD	Local Profile Agent in the Device
LPD	Local Profile Download
LSA	Licensed Service Area
LTE-M	Long Term Evolution for Machines
LUI	Local User Interface
M2M	Machine To Machine
M2MSP	M2M Service Provider
MCC	Mobile Country Code
MeitY	Ministry of Electronics and Information Technology

Acronyms	Description
MNOs	Mobile Network Operators
MoRTH	Ministry of Road Transport & Highways
NB-IoT	Narrowband IoT
OEMs	Original Equipment Manufacturer
OTA	Over The Air
P2P	Person to Person
PCB	Printed Circuit Board
QoS	Quality of Service
QR	Quick Response
RFID	Radio Frequency Identification
SAS-SM	Security Accreditation Scheme for Subscription Management
SAS-UP	Security Accreditation Scheme for UICC Production
SIM	Subscriber Identity Module
SM-DP	Subscription Manager Data Preparation
SM-DS	Subscription Manager Discovery Server
SMS	Short Message Service
SM-SR	Subscription Manager Secure Routing
SOP	Standard Operating Procedure
TEC	Telecommunication Engineering Center
TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UICC	Universal Integrated Circuit Card
UL	Unified License
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network