CONSULTATION PAPER ISSUED BY

THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

EMBEDDED SIM TECHNOLOGY

06 JUNE 2018

CONTENTS

1. INTRODUCTION

Physical SIM Cards

1.1 Secure and reliable mobile connectivity has become an indispensable part of our daily lives due to an increasing dependency on our mobile devices for work, life and play. It has also become an integral part in many countries' strategic roadmaps to achieving their vision of digitalising their economy and developing smart cities. According to the Global System for Mobile Communications Association ("**GSMA**") Intelligence, there are more than 5 billion unique mobile subscribers in the world, which means that more than two-thirds of the global population is connected to a mobile service. The development of the Subscriber Identity Module ("**SIM**") card and the technological advancements in this humble and inconspicuous card over the years, alongside the evolution of next generation mobile and communication devices, has facilitated the proliferation of mobile devices and subscriptions to a significant degree. The number of physical SIM cards in circulation today is significantly more than the 5 billion unique mobile subscribers estimated by GSMA Intelligence. In Singapore, there are approximately 8.4 million active mobile subscriptions, which translates to at least an equal number of SIM cards in circulation today.

1.2 The first SIM card was introduced in 1991. In that initial period, SIM cards were of the same size as credit cards and were designed to provide cellular connectivity on Global System for Mobile Communications or **GSM** networks. The primary role of the SIM card was two-fold, which continues to be relevant today:

i. **Identification** – the SIM card contains a unique reference number (Integrated Circuit Card Identifier or "**ICCID**") that identifies the SIM card and the subscription that accompanies the SIM card. This allows Mobile Network Operators ("**MNOs**") or Mobile Virtual Network Operators ("**MVNOs**") (hereinafter individually referred to as a "**mobile operator**" or collectively as "**mobile operators**") to recognise their subscribers on their respective networks and ensure accurate billing; and

ii. **Authentication** – the SIM card contains a security mechanism which allows end users to access the mobile operators' networks. Briefly, the authentication process between the network and the SIM card is achieved through the unique security key and other credentials stored in the SIM card. Once validated, access to the mobile operators' networks will be granted.

1.3 While the two key functions of SIM cards have remained unchanged over the years, both the form factor and technology applied in performing these functions

have evolved significantly. Over time, the size of the physical SIM cards has reduced significantly, largely driven by technological advancements. The shrinking of SIM cards has, in turn, freed up space in mobile devices and has paved the way for increased functionality. Currently, the fourth Form Factor ("**4FF**")[1] or Nano SIM (introduced in early 2012) is the smallest available size for SIM cards and has been used in a wide variety of mobile devices. With the advancement of mobile cellular technology from 2G, 3G and to 4G, SIM cards are also required to perform increasingly secured authentication processes to address emerging cybersecurity threats. In addition, SIM cards have also evolved to perform novel functions, e.g., Near-Field Communications.

New Technology Innovation – eSIMs and Remote Provisioning Functionality

1.4 The next development for SIM cards involves an evolution of the card form factor, where the circuitry of the physical SIM card is now physically and permanently integrated into different devices, i.e., it can no longer be removed from the device. This is known as an embedded SIM or **eSIM**. eSIMs are typically soldered directly into the devices during the manufacturing process by equipment manufacturers.

1.5 Alongside the introduction of eSIMs, Remote Provisioning of mobile operator profiles[2] for SIM cards has also been made possible. Remote Provisioning refers to the ability to remotely change a mobile operator's profile in a SIM card without having to physically change the SIM itself. While Remote Provisioning is a new function, it is also backwards compatible, i.e., it can be implemented on any SIM form factor, including physical SIM cards and eSIMs. Working together with operators and SIM hardware providers from around the world, GSMA has published technical specifications to facilitate Remote Provisioning of mobile operators' profiles.

1.6 The combination of eSIMs and Remote Provisioning functionality (hereinafter referred to as "**eSIM technology**") will enable over-the-air ("**OTA**") management of mobile operator profiles for more efficient service provisioning and switching between mobile operators. For example, end users will be able to switch between mobile operators without physically swapping their SIM cards, reducing visits to brick and mortar stores.

1.7 The development of eSIM technology will bring about benefits, in enabling greater choice of mobile operators and more competitive service plans, for both consumer devices including smart phones, tablets and wearables such as smart

[1] 1FF refers to the full size (i.e., credit card size) SIM; 2FF refers to the mini SIM; 3FF refers to the micro SIM.

[2] Mobile operators' profiles consist of file structure, application(s) and data (including information such as International Mobile Subscriber Identity ("**IMSI**"), Authentication Key ("**Ki**"), Integrated Circuit Card Identifier ("**ICCID**"), etc.), which allow access to a specific mobile network.

watches (hereinafter collectively referred to as "**Consumer"** devices), as well as Machine-to-Machine communication devices[3] and/or Internet of Things (hereinafter collectively referred to as "**M2M"** devices) typically deployed by enterprise users.

1.8 It is envisaged that M2M devices are likely to benefit more significantly from eSIM and Remote Provisioning developments, as some of these devices could be located across very diverse, unsupervised and inaccessible locations (e.g., sensors in storm drains or on lamp posts). Enabling M2M devices with SIM cards that require replacement of the physical cards when an enterprise wishes to change a mobile operator may be impractical and expensive. The adoption of eSIM technology in M2M devices will thus bring about significant benefits to enterprise users by allowing greater ease of switching mobile operators and availing themselves to more competitive service packages from different providers.

1.9 While physical SIM cards will continue to be the prevalent form factor for enabling mobile communication in the short to medium term, it is envisaged that eSIM technology will permeate more devices (both Consumer and M2M) and will become more prevalent over time. This technology will facilitate further business and service innovation in the mobile sector and other sectors of the economy with the increasing deployment of M2M devices.

1.10 At the same time, eSIM technology may disrupt the existing physical SIM card ecosystem, in areas such as the manufacturing, management and provisioning of services enabled by SIM cards.

1.11 In this vein, IMDA would like to seek views and comments from members of the public and the industry on IMDA's preliminary views and assessment of the impact of eSIM technology in Singapore's context. In this consultation, IMDA will not discuss the development of other low power wide area technologies for Internet of Things ("**IoT**") devices, such as LoRa[4], SigFox[5] and Wi-SUN[6], which are mainly used for localised or private networks.

1.12 This Consultation Document sets out the following for discussion:

---

[3] Machine-to-Machine communication devices enable automated communication between machines and devices (including voice communication within the scope of a pre-defined service feature and within a closed user group), and not for other purposes (such as voice communication with an external person).

[4] LoRa: **Lo**ng **Ra**nge, Low Power Wide-Area Network ("**LPWAN**") proprietary wireless data communication platform intended for IoT

[5] SigFox: another proprietary LPWAN communication platform for IoT

[6] Wi-SUN: **Wi**reless **S**mart **U**biquitous **N**etwork, a proprietary IoT communication platform that is typically deployed using mesh topology where each node relays data to the network for connectivity. In contrast, both SigFox and LoRa networks are typically deployed using a star topology, where devices are directly connected to gateways (similar to mobile phones' connectivity).

Section 2: No SIM-Lock Policy

Section 3: eSIM Technology

Section 4: eSIM Business and Operating Models

Section 5: Licensing and Regulation of eSIM Devices and Services

Section 6: Invitation to Comment

1.13 This consultation will be open for a period of six weeks, and will close by 12 noon on 18 July 2018.

2. NO SIM-LOCK POLICY

2.1 The No SIM-lock policy was introduced in 1997 in a physical SIM card and Consumer device only world. This policy states that mobile operators are not allowed to SIM-lock devices (i.e., lock the device to a specific mobile operator), such as mobile phones, tablets and wearables (e.g., smart watches) that are imported and sold in Singapore. This policy aimed to remove the barrier for end users to switch mobile operators, so as to facilitate competition and provide end users the freedom to choose and switch between mobile operators without the need to change their Consumer devices.

2.2 The eSIM technology involves an evolution of the form factor and facilitates more efficient switching between mobile operators. Therefore, as a matter of policy principle, the deployment of eSIM technology should be consistent with IMDA's existing policy on "No SIM-lock".

2.3 Today, in Singapore, the deployment of eSIMs is at a nascent phase. For Consumer devices, eSIMs have been deployed in a small number of mass market mobile devices such as wearables and tablets, e.g., the Apple iPad, Samsung's Gear S3 frontier edition and the Apple Watch Series 3 (GPS + Cellular). For enterprise use devices, examples of eSIM deployment include in vehicles, elevators, medical devices and mobile hotspots that require communication capabilities to allow the transmission of data such as device operating conditions and geo-location coordinates to the device manufacturer or enterprise users. While some of the eSIMs are provisioned by local mobile operators, others come embedded with overseas mobile operators' SIMs and roam on local mobile operators' networks. However, based on IMDA's understanding, few or none of these deployment examples have enabled the OTA Remote Provisioning functionality.

2.4 In view of these developments, IMDA is prepared to facilitate the adoption of eSIM technology to the extent where it is technically feasible and practicable, to give effect to the No SIM-lock policy in the most cost efficient and effective manner.

2.5 As a starting premise, the No SIM-lock policy should continue to apply to mobile operators for eSIM-enabled Consumer devices, such as mobile phones, tablets and wearables, whether they are purchased by consumers or enterprise end-users.

2.6 IMDA is cognisant that eSIMs are increasingly being used in M2M devices to facilitate automated communication between machines and devices, and often times within a closed, pre-defined network. The connectivity services are likely

to be bundled and sold as a package with the devices (e.g., cars with eSIM to trigger access to emergency services in the event of an accident) or are procured separately but intended primarily for enterprise use (e.g., industrial sensors with eSIM for monitoring equipment status). IMDA is prepared to allow the industry some flexibility in applying the No SIM-lock policy, as some of these enterprise users may choose to stay with a single mobile operator based on the terms negotiated for the provision of M2M services. However, where enterprise users request to switch mobile operators for the eSIM devices, the onus is on the mobile operators who are providing connectivity to the eSIMs to facilitate the switching of mobile operator profiles[7].

Question 1: *IMDA would like to seek views and comments on the policy principle of extending the No SIM-lock policy to eSIM devices.*

Question 2: *IMDA would like to seek views and comments on the application of the No SIM-lock policy on Consumer devices (e.g., mobile phones, tablets and wearables (such as smart watches and fitness trackers)) where they are eSIM-enabled.*

Question 3: *For M2M devices, IMDA would like to seek views and comments on placing the onus on mobile operators to facilitate switching of mobile operator profiles where consumer and enterprise end users request to switch* mobile operator*s.*

[7] Mobile operators can commercially decide whether to pass on reasonable costs of switching to their end users.

3. ESIM TECHNOLOGY

Introduction to GSMA Specifications

3.1 The GSMA has released two different technical specifications[8] for two categories of devices with eSIMs: Consumer devices and M2M devices (collectively to be known as "**eSIM devices**"). While both GSMA specifications enable the Remote Provisioning of mobile operator profiles, the approach and functional blocks defined to achieve this for Consumer devices and M2M devices are fundamentally different due to the typical uses of these devices. For Consumer devices, the downloading and switching of mobile operators' profiles are initiated by end users individually, i.e., 'pulled' by the devices directly. However, as most M2M devices operate with no or limited human intervention, the mobile operators' profiles are 'pushed' down centrally by mobile operators to the devices in batches instead, when the switching of the mobile operators' profiles has been initiated by enterprise users. The different architecture and functional roles used to provision the eSIM technology are broadly described below.

3.2 For Consumer devices, the key functional roles introduced by GSMA to provision the OTA subscription management are the Subscription Manager Discovery Server ("**SM-DS**"), Subscription Manager Data Preparation+ ("**SM-DP+**") and Local Profile Assistant ("**LPA**")[9]. The architecture is shown in **Figure 1**.

i. SM-DS
   a. Provides the Internet Protocol ("**IP**") address of the respective SM-DP+ to a Local Discovery Service ("**LDS**"), allowing the LPA to locate the SM-DP+ for profile downloading.

ii. SM-DP+
   a. Prepares mobile operators' profiles;
   b. Secures the profiles with profile protection keys;
   c. Stores profile protection keys;
   d. Stores the secured profiles in a repository; and
   e. Allocates the protected profiles to specified eSIM.

[8] The two GSMA Over-The-Air Subscription Management Specifications created for M2M and Consumer devices are SGP.02 and SGP.22 respectively.

[9] LPA can be located in either the device (**LPAd**) or eSIM (**LPAe**). The defined LPA functions are performed independently of the LPA's location.

iii. LPA

a. Allows end users to initiate the subscription management functions, such as downloading, activating and deactivating of mobile operators' profiles.

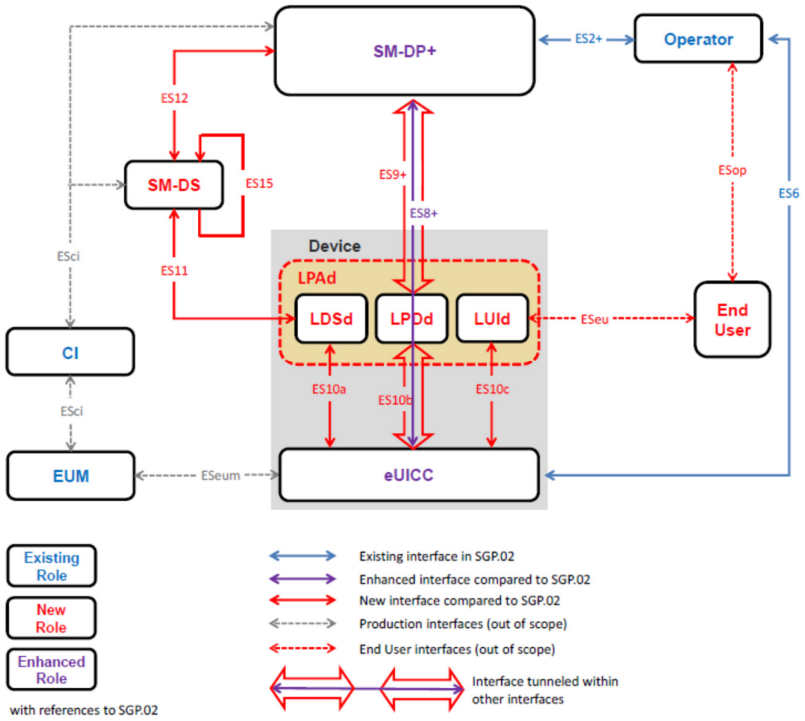

Figure 1: eSIM Technology Architecture for Consumer Devices (source: GSMA)

3.3 For M2M devices, the key functional roles introduced by GSMA to provision the OTA subscription management are the Subscription Manager Data Preparation ("**SM-DP**") and Subscription Manager Secure Routing ("**SM-SR**"). The architecture is shown in **Figure 2**.

i. SM-DP

a. Prepares mobile operators' profiles;
b. Secures the profiles with profile protection keys;
c. Stores profile protection keys;
d. Stores the secured profiles in a repository; and
e. Manages the secured download and installation of these mobile operators' profiles into the eSIM.

ii. SM-SR

a. Only entity allowed to establish a secure and authenticated transport channel to the eSIM; and

b. Executes commands of subscription management of the eSIM such as load, enable, disable, and delete mobile operators' profiles.

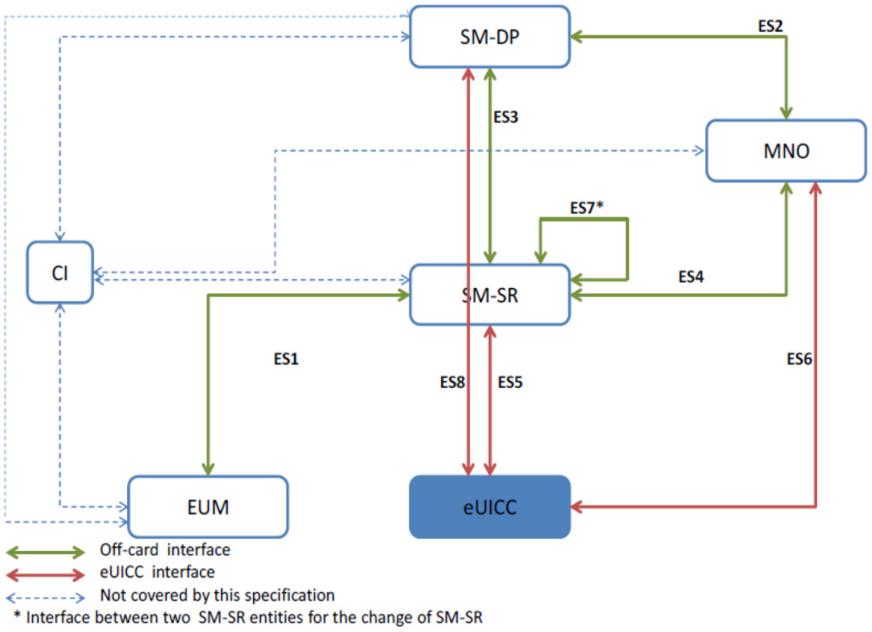

Figure 2: eSIM Technology Architecture for M2M Devices (source: GSMA)

3.4 To better understand the technical aspects of eSIM technology, IMDA completed a technical trial on Remote Provisioning for M2M devices based on the GSMA specifications in April 2017. The trial demonstrated that eSIM technology can be deployed with minimal changes to the existing local mobile operators' networks, with arrangements established between the mobile operators and the eSIM technology solution providers to ensure the secure deployment of this technology. The trial has also shown that it is possible to provision eSIM technology with eSIMs manufactured by different manufacturers, as long as the eSIMs comply with the GSMA specifications. While the trial results are positive, it is noted that not all M2M devices can support eSIM technology despite indications on the devices that purport to meet the requirements as published in the GSMA specifications. Hence, it would be important for organisations to conduct eSIM technology testing with their M2M devices prior to commercial deployment.

Adopting GSMA Specifications

3.5 Given that specifications have been set by GSMA, the global body of mobile operators and related vendors worldwide, IMDA expects eSIM devices that are brought into Singapore for sale and use in Singapore to conform to these GSMA specifications moving forward. IMDA is of the view that the adoption of GSMA specifications will enable the Remote Provisioning of mobile operators' profiles

regardless of the SIM manufacturers and solution providers, achieving the No-SIM lock policy intent.

3.6 While the adoption of the GSMA specifications will facilitate technical switching across mobile operators' networks, operational arrangements (e.g., Service Level Agreements) amongst mobile operators will need to be worked out in order to effect the switching, in particular for M2M devices. Although IMDA views that such operational arrangements are commercial in nature, which are to be discussed and agreed amongst mobile operators, IMDA is prepared to convene and facilitate these discussions.

Question 4: *IMDA would like to seek views and comments on the adoption of GSMA specifications for eSIM devices that are to be sold and used in Singapore to facilitate the deployment of OTA Remote Provisioning functionality.*

Security

3.7 In addition to the GSMA specifications outlined above, IMDA understands that there are global schemes and standards for security governance such as the GSMA Security Accreditation Schemes ("**SAS**") and the ISO 27001 Standards.

i. The GSMA operates the SAS and provides the Consolidated Security Requirements ("**CSR**") as well as the Consolidated Security Guidelines ("**CSG**"). The CSG provides SAS participants with practical guidance in relation to the design, implementation and operation of security controls that meet the CSR.

ii. ISO 27001 is a set of standards for an information security management system ("**ISMS**"). It includes all legal, physical and technical controls required in an organisation's information risk management framework. ISO27001 provides requirements required to establish, implement, maintain and continuously improve on ISMS.

3.8 Due to the maturity of physical SIM cards and their underlying technology, the security provided by physical SIM cards and their manufacturing processes have been generally viewed to be secure and reliable. While most of the manufacturing process (e.g., preparation and transport of mobile operators' profile data) for physical SIM cards is performed "offline", the same cannot be said for eSIMs, as Remote Provisioning allows mobile operator profile data to be packaged and transported "online". This key difference may potentially expose eSIM devices to new cyber security vulnerabilities.

3.9 IMDA is of the view that the various GSMA SAS and ISO 27001 standards are a useful starting point for ensuring that mobile operators and end users are

better protected from security vulnerabilities. For example, a Risk Treatment Plan is a key document in the ISO 27001 standard, which outlines the process for the risk treatment and management process (e.g., risk identification, assessment and treatment). If a new system and its associated eSIM Remote Provisioning functions are deployed without any risk treatment (e.g., a firewall to protect the eSIM's network was not installed), the risk of a security breach would likely be high. The security requirements from GSMA SAS and ISO 27001 Standards will also enhance service resilience and consumer confidence in eSIM, which will consequently increase market adoption.

3.10 IMDA thus proposes for Relevant Providers[10] to adopt the GSMA SAS and ISO 27001 standards as well as other related schemes from standards setting organisations such as the International Telecommunication Union ("**ITU**") and Internet Engineering Task Force ("**IETF**"). An eSIM service provider's eSIM infrastructure should also be GSMA SAS accredited and ISO 27001 certified for their facilities and functions for eSIM Remote Provisioning to safeguard against cyber-attacks. Mobile operators need to ensure that their eSIM service providers and their corresponding third party providers meet these requirements to protect mobile operators' interests. Mobile operators should request for their eSIM service providers to obtain the necessary certification from relevant certification bodies after conducting the necessary audits. As part of maintaining the certification process, regular audits will be necessary for the eSIM service providers to continue to be certified.

Question 5: *IMDA would like to seek views and comments on whether IMDA should require the mobile operators to adopt the GSMA SAS and ISO 27001 standards and secure the compliance of Relevant Providers in the eSIM OTA Remote Provisioning supply chain with the above-mentioned standards in the provisioning of eSIMs.*

Question 6*: Are there security gaps that GSMA SAS and ISO 27001 do not address, and if so, how should these gaps be plugged to facilitate trust and security in the provisioning of eSIMs, particularly in safeguarding the OTA profile management process.*

[10] Relevant Providers refer to eSIM manufacturers/suppliers, eSIM service providers, mobile operators, mobile device manufacturers and Subscription Managers ("**SM**").

4. ESIM BUSINESS AND OPERATING MODELS

4.1 IMDA is aware of several business models in the provisioning of eSIM-enabled services that are present in the market today. While mobile operators have traditionally managed, in-house, the end-to-end provisioning of SIM cards after the manufacturing process, several architectures, as described above, have been developed for eSIM service provisioning. Different players have also emerged to manage the provisioning process, such as the expanded role of the SIM manufacturer to become the eSIM OTA profile management solution provider, for example.

4.2 Some of the eSIM provisioning models include:

i. Fully outsourced model (most commonly observed model) – where the various functional blocks (i.e., SM-DS, SM-DP+, SM-SR and SM-DP) are fully managed by third parties (e.g., eSIM solution providers or manufacturers);

ii. Fully in-house model – where the various functional blocks (i.e., SM-DS, SM-DP+, SM-SR and SM-DP) are fully managed by mobile operators, either singly or collectively; and

iii. Hybrid model – a combination of either (i) or (ii) above, e.g., a mobile operator's profile packaging and management are managed by one party while services such as profile switching and service activation are managed by another party.

4.3 As provided for in the GSMA specifications, M2M devices will come pre-installed with a bootstrap mobile operator profile of the device manufacturers' choice at the point of device assembly. There are thus opportunities for entities traditionally not involved in the SIM provisioning process (e.g., device manufacturer) to participate in the eSIM ecosystem. The eSIM technology could result in new vertically integrated businesses where the device manufacturer would manufacture both the mobile devices as well as the SIM circuitry to be soldered to the device, and influence the choice of the bootstrap mobile operator.

***Question 7**: IMDA would like to seek views and comments on which eSIM provisioning model is best suited for mobile operator's needs, and why.*

***Question 8**: Do you see any further developments on the eSIM provisioning models, such as opportunities for business to vertically integrate and additional opportunities for third parties to participate in the eSIM ecosystem?*

***Question 9**: Given the changes to the SIM landscape, do you see any value capture opportunities for Singapore in relation to eSIM developments and adoption? These could be from a manufacturing or cyber-security function, for example.*

***Question 10**: As eSIM technology is still relatively nascent with few mass market devices using such technology, what additional support is required to encourage the development of the eSIM provisioning ecosystem in Singapore, in particular the OTA profile management function?*

***Question 11:** What would be the benefits and concerns for mobile operators to engage one trusted third party to provide services in support of OTA Remote Provisioning in Singapore, similar to the existing number porting arrangement.*

5. LICENSING AND REGULATION OF ESIM DEVICES AND SERVICES

Licensing Framework

5.1 Currently, all manufacturers, importers and sellers of SIM-enabled devices, and mobile operators who provide the connectivity for SIM-enabled devices, are required to apply for a Telecommunication Dealer's licence and telecommunication service provider's licence respectively from IMDA. Each model of the SIM-enabled device is also subject to equipment registration or approval by IMDA before the equipment can be imported and sold for use in Singapore. The type of licences and licence conditions applied depend on the communication capabilities of the device.

5.2 Consumer devices (e.g., mobile phones, tablets, and wearables) generally allow end users to interact with the devices and can be used for general voice communication and/or access to the Internet. M2M devices (e.g., telemetry sensors, smart meters and medical devices), on the other hand, are generally used only for automated communication between machines and devices with limited or no interactions with end users, and support restricted voice communication[11] (if any). Further, unlike Consumer devices, the connectivity service provider for M2M devices may not have a contractual relationship with the end users of the M2M devices.

5.3 Depending on the device capabilities and characteristics of the services provided, IMDA requires the manufacturer, importer and seller of Consumer devices, and the connectivity service provider for Consumer devices, to minimally obtain a Telecommunication Dealer's (Class) licence and a telecommunication operator licence[12] respectively. For M2M devices, the manufacturer, importer and seller is required to obtain a Telecommunication Dealer's (Individual) licence, and the connectivity service provider is required to obtain a telecommunication operator licence for the provision of M2M services[13]. These two latter licences have additional obligations for record keeping of the M2M SIM device information, as well as end users' information (see Annexes A1 and A2 for the relevant licence conditions). The licensing and regulatory framework is aimed at ensuring that the devices imported for use in Singapore comply with the relevant standards and technical requirements in

[11] Voice communication is enabled within the scope of a pre-defined service feature and within a closed user group, and not for other purposes (such as voice communication with an external person).

[12] For these services that provide any-to-any voice communication services, the connectivity service provider will require minimally a Services-Based Operations ("**SBO**") (Individual) licence to provision mobile subscription and call services.

[13] The connectivity service provider will require minimally an SBO (Individual) licence to provision M2M services.

the use of radio frequencies, to ensure public safety and security needs are met, and that consumer interests are protected (also see Annexes A1 and A2 for the relevant licence conditions).

5.4 As discussed in previous sections, M2M devices are likely to benefit more significantly from the developments of eSIM technology. The adoption of M2M devices is likely to accelerate in the next few years, especially with the maturity of eSIM technology. Gartner, in its forecasts, has estimated that there will be 20.4 billion connected devices worldwide by 2020[14], of which approximately 36% or 7.4 billion will be M2M devices

5.5 In Singapore, the M2M devices we see today are used by enterprises and in niche sectors, such as in smart vehicles, lift sensors and healthcare-related products. However, with eSIM technology becoming more mainstream, we will soon see eSIMs used in a variety of mass-market consumer devices, such as household appliances, toys and clothing. Hence, the current licensing approach for manufacturers, importers and sellers of M2M equipment and for M2M connectivity service providers may not be sustainable, with the wide-spread use of eSIMs in mass-market consumer devices.

5.6 IMDA thus proposes to maintain the current licensing framework only for M2M devices that support mobility and/or come with restricted voice communication features[15] for public safety reasons. In other words, the current licensing framework for M2M devices will continue to apply for M2M devices with or without restricted voice communication features that are used in motor vehicles and trains (amongst others), and M2M devices that come with restricted voice communication features. For all other M2M devices, e.g., those used in sensor or metering networks, or household appliances that are largely immobile, IMDA proposes to adopt a "light-touch" licensing approach where the device manufacturer, importer and seller is only required to register the M2M device and obtain a Telecommunication Dealer's (Class) licence, without additional record keeping licence obligations. A telecommunication operator licence is also not required for the entity providing the connectivity service to M2M devices that do not support mobility or have no voice communication features, if the entity (i) does not have a direct contractual relationship with the consumer or enterprise end user in Singapore, and (ii) the eSIMs are roaming on local mobile operators' network. In other words, a telecommunication operator licence will still be required for such M2M devices if the consumer or enterprise user is able to procure (i.e., through a direct contractual relationship) the connectivity services in Singapore.

[14] *Source: Gartner (January 2017)*

[15] For M2M devices that come with any-to-any voice communication features, the connectivity service provider will require minimally an SBO (Individual) licence to provision mobile subscription and call services.

Question 12: *Given the wide variety of applications for eSIM M2M devices, IMDA would like to seek views and comments on the proposed licensing framework and the proposed licence conditions for Consumer and M2M devices that are enabled with eSIM technology.*

Consumer Protection Measures

5.7 In the mobile sector, to safeguard consumers' interests, IMDA has established a list of codes of practice, guidelines and consumer protection measures related to the provision of mobile services to Consumer devices, which must be observed by mobile operators. The relevant codes of practice, guidelines and consumer protection measures are as follows:

i. The Code of Practice for Competition in the Provision of Telecommunication Services 2012 (Telecom Competition Code) which requires operators to provide services to end users on just, reasonable and non-discriminatory terms;

ii. The Code of Practice for Provision of Premium Rate Services (PRS Code) which protects the interest of end users by specifying the duties to be observed by the PRS providers and billing operators, as well as the PRS Barring service which enables end users to stop sending/receiving chargeable PRS offered by the PRS providers;

iii. The Contract Period and Early Termination Charges Guidelines which limits the maximum length of contracts to 24 months and requires the early termination charges to be graduated so that they are fair and reasonable to the end users;

iv. The Full Mobile Number Portability measure which enables end users the flexibility to switch to another mobile operator while retaining their numbers; and

v. The Data Roaming Bill Cap service which offers end users the option to limit their data roaming charges to a maximum of S$100 every billing month. The mobile operators are also required to obtain end users' express agreement before such services are provided, and provide end users the option to deactivate/reactivate their data roaming services at any time while in Singapore.

5.8 Considering that eSIM involves an evolution of the SIM card form factor and does not alter its core functions of identifying and authenticating users, IMDA is of the view that the existing codes of practice, guidelines and consumer

protection measures that apply to the mobile operators should remain applicable for mobile operators who offer telecommunication services via subscription contracts with end users for the use of eSIM-enabled Consumer devices.

***Question 13**: To the extent where they are relevant, do you agree that the codes of practice, guidelines and consumer protection measures established by IMDA for the provision of mobile services should remain applicable to the operators who offer telecommunication services for the use of eSIM-enabled Consumer devices?*

6. INVITATION TO COMMENT

6.1 IMDA would like to seek the views and comments from members of the public and the industry on the above issues.

6.2 Parties that submit comments on the issues identified in this Consultation Document should organise their submissions as follows:

i. Cover page (including their personal/company particulars and contact information);
ii. Table of contents;
iii. Summary of major points (structured to follow the individual Parts of the Consultation Document);
iv. Statement of interest;
v. Comments (in response to the Questions set out in the Consultation Document and any other comments); and
vi. Conclusion.

Supporting material may be placed in an Annex.

6.3 Where feasible, parties should identify the specific sections of the Consultation Document on which they are commenting and provide reasons for their proposals.

6.4 All submissions must reach IMDA by 12 noon on 18 July 2018. Softcopy of submissions in both Microsoft Word and Adobe PDF format should be provided. Parties submitting comments should include their personal/company particulars as well as the correspondence address, contact number and email addresses on the cover page of their submission. All comments should be addressed to:

Aileen Chia (Ms)
Deputy Chief Executive (Policy, Regulation & Competition Development),
Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Please submit your softcopy via email to: Consultation@imda.gov.sg

6.5 IMDA reserves the right to make public any written submissions and to disclose the identity of the source. Commenting parties may request confidential treatment of any part of the submission that the commenting party believes to

be proprietary, confidential or commercially sensitive, with supporting justification for IMDA's consideration. In such cases, the submission must be provided in a non-confidential form suitable for publication, with any confidential information redacted as necessary and placed instead in a separate annex.

6.6 If IMDA grants confidential treatment, it will consider, but will not publicly disclose the information. If IMDA rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider the information as part of its review. As far as possible, parties should limit any request for confidential information submitted. IMDA will not accept any submission that requests confidential treatment for the entire, or a substantial part of, the submission.