



GSMA Hong Kong
Suites 1207-10, 12/F
Great Eagle Centre
23 Harbour Road
Wan Chai
Hong Kong
Tel: +852 3960 5000
gsma.com

Ms Aileen Chia
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

14 August 2018

Dear Ms Chia,

Re: IMDA's preliminary views and assessment of the impact of eSIM technology in Singapore's context

The GSMA would like to thank the IMDA for the opportunity to submit its feedback and comments related to the above consultation.

Please do not hesitate to contact us if you have any questions regarding this submission or any other matter in which we might be of help to the IMDA.

Yours sincerely,

A handwritten signature in black ink, appearing to read "David Turkington".

Mr David Turkington

Head of Technology, APAC, GSMA

E: dturkington@gsma.com

T: +852 3960 5052

M: +852 6891 9569





Table of Contents	Page
Cover Letter	1
Summary	2
Statement of Interest	3
GSMA IMDA eSIM Consultation Responses	
Q1, 2, 3	4
Q4, 5, 6	5
Q7, 8	7
Q9, 10, 11	8
Q12, 13	9

Summary

eSIM is a global specification by the GSMA which enables remote SIM provisioning of any mobile device.

The GSMA eSIM specifications are written for global market, certain aspects of eSIM (e.g. SIM-lock) are local policy decisions depending on application and regulatory framework.

Many different eSIM provisioning methods will be possible and will depend greatly on operator/eSIM provider preference, device capability and application, GSMA suggests light touch regulation accordingly.

GSMA places great importance on eSIM security and has several procedures to assure protection all stages of provisioning and operations.

eSIM enables new business models, the flexibility of the specifications allows various commercial and regulatory requirements to address any arising issues.





Statement of Interest

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

The GSMA engages with policymakers and regulators to advance policy discourse, contribute market research and analysis, and convey the perspectives of the mobile industry across the wide range of issues that surround the digital economy and society.

GSMA has been deeply involved in the creation of the eSIM specification and has expertise in all aspects of eSIM technology, mobile networking, security, operations, telecom policy and regulation. GSMA is ready and willing to assist IMDA in any capacity to support deployment of eSIM in Singapore.

More information can be found here: <https://www.gsma.com/esim/>



GSMA IMDA eSIM Consultation Responses

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

The applicability of a 'No SIM-lock' policy is a purely local regulatory concern.

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.*

The GSMA eSIM specifications are written with the intent of global applicability, this means supporting operators required to adhere to a No SIM-lock policy. The policy rules defined in the specification and supported within devices make it possible for a mobile operator to implement a SIM lock, but there is no compulsion on any mobile operator to use them.

In a jurisdiction with a No SIM-lock policy, the regulator may need to amend the current regulation to stop mobile operators from invoking the eSIM Policy Rules to lock the device. Even where No-SIM lock policies exist there are often use cases where SIM-lock can be legitimately applied, examples include where the customer is an enterprise (such as for verticals: the customer is usually an OEM) or where the end-user does not own the device (e.g. short-term lease schemes).

Additionally, there may be low end devices that do not support remote provisioning or have some other limitations that prevent changing eSIMs.

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 operators.*

Placing the onus on mobile operators to facilitate switching of mobile operator profiles where consumer and enterprise end users request to switch mobile operators means the operators will need to absorb the cost of this activity. It is important to note that there is a difference between consumers devices and M2M devices.

If such an obligation is placed on the mobile operator, the mobile operator must be in control of the SM-SR platform.



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.*

GSMA would welcome the adoption of their specifications in the Singapore market and would be receptive to discussions with IMDA to facilitate such a decision.

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.*

The GSMA does not advocate for the imposition of mandatory rules. The mobile operators are to decide on a voluntary basis whether adoption is beneficial. Having said that, the GSMA SAS (and affiliated compliance procedures) exist to ensure interoperability, assure security and enable trust. GSMA would encourage their support by national regulators. The key document for eSIM compliance is the GSMA SGP.24, which includes references to additional compliance and certification schemes for eSIM from GlobalPlatform, Global Certification Forum and the PTCRB. It also references the applicable GSMA SAS procedures. Details of these schemes and relevant documents can be found at <https://www.gsma.com/esim/compliance/>.

ISO 27001 is a more generic information security standard and could be used as an indicator of good practice.

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.*

GSMA Security Accreditation Scheme (SAS) defines a standard for information and physical site security for SIM and eSIM production as well as for provisioning server operational sites. The SAS processes are constantly updated to address market needs such as new product type manufacturing processes. Actions are also in place to permit disassociating a full production line into different sections, allowing audited companies' accreditation for only the necessary part of the production chain.

GSMA and security companies are aware for the need to be continually vigilant and adapt to an ever-changing security threat landscape. For this reason, GSMA has taken the following measures around security while specifying eSIM:



- Involving independent external security experts in the review of every public major release of the eSIM specifications.
- Involving GSMA Fraud and Security (FASG) experts in each approved version of the specification.
- GSMA runs an official Coordinated Vulnerability Disclosure (CVD) program designed to handle potential security vulnerability disclosures that could affect the industry and its customers (this program has already received CVD inputs on eSIM).
- GSMA works closely with leading security experts across all stakeholders on eSIM security requirements and associated Common Criteria process (known as Protection Profiles) at the level of EAL4+ AVA_VAN.5 created together with German Federal Office for Information Security and approved by Common Criteria as well as recognised by SOG-IS in Europe to ensure the security assurance level and robustness of the eSIM where the operator credentials are stored.
- GSMA has a process in place for issuance of PKI certificates to entities able to ensure functional and security compliance to the GSMA specifications to enable a trusted ecosystem.
- GSMA has a process of certificate revocation in place in case of security threats over a GSMA certified product.
- Every GSMA specification has a maintenance process in place to address market needs and potential security threats as soon as they are identified.

It is worth observing that the security threats with eSIM differ to those with physical removable SIMs, one of the positive security aspects of eSIM is that vulnerabilities discovered within the SIM themselves are more rapidly addressed through OTA updates of the operator profile, or of the eSIM software.

GSMA continually strives to improve the GSMA processes, should there be areas of concern the GSMA would welcome discussions on these, if any, with IMDA on a confidential basis.



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.*

The GSMA specifications are written to enable flexibility in deployment models. However, mobile operators must be responsible for the management of operator credentials. This is because profile settings (Network Authentication Algorithms etc.) are highly specific to an individual mobile operator and an incorrect setting can have catastrophic consequences for customer service.

The flexibility in the GSMA specifications is also intended to cope with both regulatory and commercial steps related to Know Your Customer (KYC) and credit risk checks.

In addition, whole new eSIM device types (M2M, IoT, wearables etc) are expected that may require new provisioning processes and procedures, so it is not possible to suggest a 'best' eSIM provisioning model at this time.

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?*

With the emergence of eSIM technology there is likely to be innovation from operators, SIM vendors, OEMs, other vertical manufacturers and retail organisations to integrate provisioning of collections of devices to a subscribers accounts. The GSMA specifications facilitate innovation in the enablement of cellular connectivity to consumers. As such, it is likely that new roles will emerge as part of the eSIM ecosystem, and these include:

- Operators will have simpler means to expand their businesses into emerging markets; for example, automotive, wearables, consumer electronics. SIM card distribution costs will be eliminated, logistics simplified, and eSIM will enable new distribution models for devices and for marketing of subscriptions;
- Device Manufacturers, can exploit the reduced space within their products to make smaller devices. Their products could also be made more tolerant to environmental factors such as dampness, temperature and vibration as they can be hermetically sealed. Manufacturers can also leverage eSIM to optimise supply chain processes

The GSMA has published an eSIM Whitepaper in which these developments, and the benefits for many players in the digital ecosystem are explored further. The Whitepaper can be downloaded here: <https://www.gsma.com/esim/wp-content/uploads/2018/06/eSIM-Whitepaper-v4.11.pdf>



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.*

The changes in business models described above should provide an opportunity for businesses to support the services that an eSIM ecosystem requires to enable global interoperability and trust. Progressive government regulators can only further enable such change.

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?*

We agree with IMDA that eSIM technology is still in its infancy and that regulatory intervention at such an early stage may be premature.

Having said that, clear and transparent light-touch regulatory rules on eSIM technology should help to encourage the development of the eSIM provisioning ecosystem in Singapore. As the eSIM business models/market are still emerging, thought should be given to enabling sufficient flexibility to enable successful models to emerge.

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?*

The GSMA specifications are supported by capabilities to enable an eSIM ecosystem and for local mobile operators to launch eSIM services. Additional services would be a local market consideration. Unlike number portability, eSIM provisioning is internal to the operator so 3rd party involvement is unnecessary.



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.*

GSMA considers that no change is required to the existing licensing arrangements. Although disruptive in some senses, eSIM should be seen as merely changing the way a SIM is delivered. Obligations for service licensing and device type approvals should not be impacted, likewise obligations and ability to fulfil them for Know Your Customer, Lawful Interception and Number Portability are not impacted.

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?*

For the same reason explained above (Q12) GSMA would see no need for a change.