IMPLEMENTATION GUIDE FOR ELECTRONIC KNOW YOUR CUSTOMER ("eKYC") SOLUTION

1 Scope

1.1 This implementation guide prescribes the requirements to deploy remote registration of subscribers for postpaid and prepaid cellular mobile telecommunication services (**Mobile Service**), using the eKYC solution.

1.2 Licensed Mobile Network Operators or Mobile Virtual Network Operators (herein collectively referred to as the **Operators**) adopting this approach would be able to fulfil the existing terms and conditions for the provision of Mobile Service[1] with the use of advanced technologies for documentation verification and biometric authentication. While the choice of the eKYC technology and solution provider are left to the Operators' decisions, the Operators must ensure that the eKYC solution deployed meets the requirements stipulated in this document and is at least as effective as (and not worse off than) the measures to obtain the information and particulars of the subscriber in a face-to-face customer verification. The necessary requirements described for the deployment of eKYC solutions are summarised in **Annex A**.

1.3 In the event that the eKYC solution fails to comply any of the requirements stipulated in this Implementation Guide at any time, the registration of any affected subscribers may be deemed invalid. The Operators must take measures to remedy the non-compliance quickly and may be required to re-register the affected subscribers.

2 Definitions, Abbreviations and Acronyms

2.1 Terms and Definitions

For the purpose of this implementation guide, the following terms and definitions apply.

2.1.1 False-Acceptance Rate

False-Acceptance Rate refers to the percentage of incorrect/bogus registrants that are successfully registered.

[1] For Mobile Network Operators, please refer to the specific terms and conditions for the provision of (i) prepaid public cellular mobile telecommunication service, and (ii) postpaid public cellular mobile telecommunication service, incorporated in the Facilities-Based Operations licence. For Mobile Virtual Network Operators, please refer to the specific terms and conditions for the provision of mobile virtual network operation, incorporated in the Facilities-Based Operations or Services-Based Operations (Individual) licence, where applicable.

2.1.2 IDV Template

IDV template refers to a document layout standardised with security identifier(s) for enabling graphical verification techniques to be applied to validate data integrity and authenticity of the document. An example is the IDV template standardised for passports according to the ICAO Document 9303 that has been endorsed by ISO and IEC and published as the ISO/IEC 7501-1 standard.

2.1.3 MyInfo

All SingPass users will have a MyInfo Profile. Non-permanent residents who are eligible for SingPass will also have their own MyInfo Profile. MyInfo is a service that allows SingPass users to manage their personal data and pre-fill forms in digital services transactions. This includes government-verified data that is retrieved across participating Government agencies and data users contributed to form their Profile.

2.1.4 Positive-Acceptance Rate

Positive-Acceptance Rate refers to the percentage of correct/actual registrants that are successfully registered.

2.1.5 Postpaid Mobile Service

Postpaid Mobile Service refers to a cellular mobile telecommunication service provided by an Operator in Singapore, which involves the collection of payments from subscribers according to their use of mobile services at the end of each billing cycle.

2.1.6 Prepaid Mobile Service

Prepaid Mobile Service refers to a cellular mobile telecommunication service provided by an Operator in Singapore, which involves the collection of advance payments from subscribers prior to, upon or after the supply of a SIM card or other access device/code, and before their use of the subscribed mobile service.

2.1.7 Prescribed Limit

Prescribed limit refers to the Prepaid Mobile Service card limit where each customer can only register up to three (3) prepaid SIM cards across all Operators in Singapore.

2.1.8 QR Code

QR code refers to the trademark for a type of matrix barcode (or two-dimensional barcode). It consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using Reed-Solomon error correction until the image can be appropriately interpreted. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image.

2.1.9 Reed-Solomon Error Correction

Reed-Solomon error correction refers to a group of error-correcting codes introduced by Irving S. Reed and Gustave Solomon in 1960. The most prominent applications include consumer technologies such as CDs, DVDs, Blu-ray Discs, QR Codes, data transmission technologies such as DSL and WiMAX, broadcast systems such as DVB and ATSC, and storage system such as RAID 6.

2.1.10 Registration Information

Registration information refers to all information collected during the registration process, including particulars of the Mobile Service subscriber, videos of liveness detection, photos taken, and scanned photo identity document.

2.1.11 Trusted Databases

Trusted databases are databases that contain registrants' personal information, which have been verified by the databases' owners. The trusted databases include MyInfo, Monetary Authority of Singapore licensed banks' databases and the Operators' databases.

2.2 Abbreviations and Acronyms

ATSC	Advanced Television Systems Committee
CD	Compact Disc
dpi	Dots Per Inch
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
DVD	Digital Video Disc
eKYC	electronic Know Your Customer
ICAO	International Civil Aviation Organisation
IDV	Identification Verification
IEC	International Electrotechnical Commission
iOS	Apple Mobile Operating System
ISO	International Organisation for Standardisation
Mobile Service	Cellular Mobile Telecommunication Services
MRZ	Machine Readable Zone
OCR	Optical Character recognition
OTA	Over-The-Air
QR	Quick Response
RAID 6	Redundant Array of Independent Disks 6
SIM	Subscriber Identity Module
SMS	Short Message Service
VIZ	Visual Inspection Zone
WiMAX	Worldwide Interoperability for Microwave Access

3 Characteristics of eKYC

3.1 Introduction

This implementation guide defines the requirements where Operators shall comply with when implementing an eKYC solution for remote registration of the Mobile Services. Adoption of the eKYC technologies enable the digital transformation of the Operators' business operations, which shall minimally encompass the following aspects:

(i) Subscriber acceptance and identification procedure;

(ii) Monitoring of transactions; and

(iii) Risk management.

3.2 Subscriber Acceptance and Identification Procedure

The eKYC process can be a fully automated identification flow process which determines the subscriber's eligibility, minimises customers' risk (e.g. identity theft), and ensures compliance with business obligations and regulatory requirements, before completing the registration process and approving the service provision. The eKYC process removes the hassle of manual registration, where subscriber's presence is required to verify his identity against the identification document presented, as well as consent to the disclosure of personal data. It also removes any possible human error in data entry and visual checks with the use of technologies such as OCR and biometric authentication.

The Operator must implement the following minimum measures in the eKYC solution to identify and verify a subscriber's identity:

(a) collecting the subscriber's information for the purposes of validating the subscriber's identity, which includes;

(i) performing a live scan of the allowed subscriber's identity document; and

(ii) taking live photos (or live video) of the subscriber,

or

(b) establishing that information about the subscriber's identity is provided from a trusted database.

If information about the subscriber's identity is not provided from a trusted database, the eKYC solution must perform documentation verification and biometric authentication.

3.2.1 Performance Requirement

Technologies such as facial recognition and OCR used for eKYC have advanced rapidly over the years. While it is understood that Operators are incentivised to deploy an accurate eKYC system, it is still important to establish a minimal performance requirement for the deployed eKYC systems. Hence, the eKYC solution deployed must achieve at least 85% positive-acceptance rate, and not more than 2% false-acceptance rate.

3.2.2 Types of Identification Documentation

The types of identification documents required for validating subscribers are dependent on the eKYC solution. However, the Operator must ensure the deployed eKYC solution accepts only the types of documents listed in the relevant licence conditions[2]. A passport used as an identification document in eKYC shall be an ICAO-compliant passport.

3.2.3 Registration Information

The Operators must maintain a register containing subscriber's registration information obtained during the registration process, which includes any video and live photos taken for liveness detection, and of any photo identity document for registration, for a period of not less than twelve (12) calendar months from the date of termination of the service subscription.

3.2.4 Access to eKYC for Registration

3.2.4.1 Subscribers' access to eKYC systems for service registration may be via mobile phone applications developed for iOS and Android platforms (**Mobile Apps**), service providers' web portals or self-service kiosks. As the eKYC aspect of subscriber acceptance and identification relies on photo shots of identification documents and facial recognition, it is recommended that these modes of access are equipped with cameras of preferably 8 mega pixel resolution or higher, capability to produce scanned images preferably 200dpi or higher, and broadband connections for live transmission of facial live captures back to the eKYC systems. While the recommendations on the specifications of cameras and resolutions of images captured are for Operators' consideration, it should be noted that a better image resolution will help reduce the margin of error, allowing Operators to better meet the requirements stated in clause 3.2.1.

[2] For Mobile Network Operators, please refer to the specific terms and conditions for the provision of (i) prepaid public cellular mobile telecommunication service, and (ii) postpaid public cellular mobile telecommunication service, incorporated in the Facilities-Based Operations licence. For Mobile Virtual Network Operators, please refer to the specific terms and conditions for the provision of mobile virtual network operation, incorporated in the Facilities-Based Operations or Services-Based Operations (Individual) licence, where applicable.

3.2.4.2 The Operators must put in place measures and restrictions in the eKYC solution for registration to be initiated only within Singapore. This may be implemented through identifying local IP addresses, geo-fencing Mobile App, using mobile network information, or other solutions. Operators can also deploy self-service kiosk for electronic registration.

3.2.5 Automated Identification Flow Process

The eKYC process presupposes a subscriber's consent to disclose personal data. This includes mobile number and/ or location information where Mobile Apps, Kiosks or online web portals are used, as well as images of the subscriber and identification document (mentioned in clause 3.2.2) taken for security feature checks. The Operators must ensure that the eKYC solution does not allow or enable the information readout[3] (including photos taken) and analysis of the document verification and biometric authentication obtained during the registration to be modified by the subscriber.

3.2.6 Documentation Verification

Operators shall ascertain the validity and authenticity of the uploaded identification documents, fulfilling the same requirements for today's physical face-to-face mobile customer verification and registrations.

If the Operator decides not to obtain the subscriber's information from a trusted database, the eKYC solution must implement graphical verification techniques, which includes but not limited to visual patterns and photo replacement detection techniques, to verify the authenticity of the identification documents. Depending on the type of identification document used for registration, the following graphical verification techniques could also be applied:

(i) Data integrity check of content readout from the VIZ with OCR techniques versus content readout from the MRZ

(ii) Validity check by means of QR code

[3] A visual record or display of the output from a computer and displaying it in an understandable form.

3.2.7 Biometric Authentication

If the Operator decides not to obtain the subscriber's information from a trusted database, the eKYC solution must implement biometric authentication techniques, which includes but not limited to the use of facial recognition to verify that the identification documents belongs to the subscriber. Facial recognition is one of the most common biometric authentication techniques deployed today to compare a photo image in the uploaded identification document with live facial capture of the subscriber's face. If the Operator uses facial recognition as a biometric authentication technique, live photos or video of the subscriber must be taken during the registration via the eKYC solution to verify against the photo identification documents. The Operator must not allow still images to be uploaded by subscriber to avoid digital fraud, such as the use of Photoshop. In addition, the Operator must require the subscriber to perform certain actions in real time in front of the camera (i.e. liveness detection), e.g. tilting the head to the left and the right; nodding the head up and down a number of times; or moving the eyeballs to different locations of the screen. This is to prevent fraud and avoid identity theft by means of a still image of the subscriber or animated videos.

3.2.8 Use of Trusted Databases

Operators may use subscriber's information obtained via trusted databases with the subscriber's consent, for the registration of Mobile Services. Alternatively, if the subscriber is an existing customer of the Operator, the Operator may re-use the subscriber's information stored for the registration of additional Mobile Services.

As there is no need for subscriber to upload identification document if the required subscriber's information is obtained via trusted databases, Operators will not be required to deploy facial recognition and/or other biometric authentication techniques for the validation of identification document. Hence, the performance requirement, i.e., positive-acceptance rate and false-acceptance rate, is not applicable. However, for existing customers of the Operator, the Operator must put in place sufficient checks, such as 2 factor authentication (2FA), to validate that the subscriber during registration is indeed the Operator's existing customer. The Operator must also ensure that the registration information of the subscriber, such as passport numbers, remain current and up-to-date. For avoidance of doubt, the Operator must ensure that the eKYC solution deployed comply with the other requirements and guidelines under the Operator's existing licence conditions. For example, the Operator must not provide the Prepaid Mobile Service to any subscriber below the minimum age requirement, and not sell more than the prescribed limits of the Prepaid Mobile Service, with the use of the eKYC solution.

3.3 Monitoring of Transactions

3.3.1 The Operators must put in place security controls against unauthorised registration or access for the kiosk-based eKYC solution. Physical access control is particularly important for network connections to subscribers (users) who are accessing service applications in higher-risk locations, e.g. public or external areas outside the information security management control of the Operators.

3.3.2 The eKYC solution must be able to detect any fault during the registration process, and prompt the Operator to handle or deal with the fault. A subscriber could be directed by the eKYC system to proceed to any of the Operator's retail outlets for service registration. The Operators must also employ security features in the eKYC solution, e.g., to block the subscriber from trying to register remotely after a number of unsuccessful attempts, and to apply check-sum functions, where applicable, to ensure the authenticity of an identity number.

3.3.3 The registration of a Prepaid Mobile Service through the eKYC solution is counted towards the prescribed limit of a subscriber. The Operators must not permit additional registrations through eKYC solution which will exceed the prescribed limit of the Prepaid Mobile Service to a subscriber. Consequently, the subscriber may be directed by the eKYC system to proceed to the Operator's retail outlets for service registration. The Operators must adopt measures in the eKYC solution to verify the authenticity of an identity number. This includes check-sum functions.

3.4 Risk Management

3.4.1 The Operators must ensure that the eKYC solution is secure and robust to protect the subscribers' information from unauthorised access, use and disclosure at all times. The Operators must ensure the eKYC solution deployed are at least in compliance with the ISO/IEC 27002: 2013 Code of Practice for Information Security Controls including all amendments and revisions thereto from time to time in force.

3.4.2 The Operators should consider adopting International standards such as ISO/IEC 27001 framework for Information Security Management Systems, and ISO/IEC 27005 standard for Information Security Risk Management for the deployment of the eKYC systems. In addition to the adoption of International standards, the following controls may be necessary for the deployment of eKYC systems for remote registration for Mobile Services (but may not be limited to):

(i) Controls for formal registration and de-registration of subscribers, e.g., Mobile Services will only be activated after the successful completion of the subscriber acceptance and identification procedure, where no abnormality is detected.

(ii) Cryptographic controls to protect confidentiality, authenticity and integrity of information, and the level of protection required should be based on risk treatment plan, e.g., use of encryption for protection of information transported by mobile phones and across communications lines.

(iii) Controls for network security management to ensure adequate protection of information in the network and its information processing facilities.

(iv) Controls for communications security to safeguard the confidentiality and integrity of information that is being transferred over public or wireless networks.

(v) Controls for segregation of duties to ensure that no single person can access, modify or use information without authorisation and detection.

(vi) Controls for physical and environmental security when setting up self-service kiosks, e.g., may need to tamper proof the kiosks to deter against and/or recover from vandalism and hacking.

3.4.3 While the adoption of above-mentioned International standards and controls will help Operators better conform to the clauses of the Personal Data Protection Act ("PDPA") and any cyber security requirements imposed by IMDA and Cyber Security Agency ("CSA"), it shall not be inferred that such adoptions would automatically ensure compliance. Operators are still responsible for taking necessary measures to comply with the respective legislations and regulations.

3.5 Mobile Service Delivery

After the subscriber has successfully completed the subscriber acceptance and identification procedure without any abnormality detected, and the eKYC system has properly registered the subscriber and uploaded the subscriber's record, the Operators must ensure that the SIM card is delivered directly to and/or activated by the same subscriber who has registered for the Mobile Service through the eKYC solution. The Operators may employ any method, including the following options for delivery of the SIM card:

(i) The subscriber may request for registered mail delivery of the SIM card:

a. Delivery man to validate the subscriber against his/her original identification document visually; and/or

b. Activation code for the SIM card to be delivered to the subscriber separately.

(ii) If the subscriber is using a self-service kiosk for the registration, the SIM card may be dispensed immediately and the Mobile Service may be activated upon validating all registered personal information. In the case of prepaid service, Operators are to also ensure that the total number of SIM cards subscribed does not exceed the prescribed limit.

(iii) The subscriber may bring along the original identification document and a softcopy acknowledgement of the successful eKYC registration to collect the SIM card personally at the Operator's retail outlet.

3.6 Implementation of eKYC Solution

Operators who are interested to deploy eKYC solutions are required to submit an application to IMDA, to seek IMDA's written approval prior to the implementation of eKYC solution. In the application, please include a detailed description of the proposed eKYC solution, including the technical information, and a declaration of compliance with the requirements in Annex A of the Guide. The application should be submitted to IMDA via ILO@imda.gov.sg, and addressed to:

> Director-General (Telecoms & Post)/ Deputy CE (Policy, Regulation & Competition Development)
> Attention: Industry Liaison Officer

Where required, Operators may be requested to provide clarifications and justify how their proposed solutions meet the implementation guide requirements, including a demonstration of the proposed eKYC solution. Please note that any approval for the implementation of eKYC solution shall be given subject to terms and conditions which IMDA may impose.