ANNEX A

Section	Necessary Requirements under the Implementation Guide of eKYC solution for Mobile Service	Compliance (Yes/No)	Remarks
	Overview		
1.2	The Operator must ensure that the eKYC solution deployed 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.		
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 will be deemed invalid. The Operator must take measures to remedy the non-compliance quickly and may be required to re-register the affected subscribers.		
3.2	***Subscriber Acceptance and Identification Procedure***		
3.2	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.		

Section	Necessary Requirements under the Implementation Guide of eKYC solution for Mobile Service	Compliance (Yes/No)	Remarks
3.2.1	The eKYC solution deployed must achieve at least 85% positive-acceptance rate (of correct/actual registrants that are successfully registered), and not more than 2% false-acceptance rate (of incorrect/bogus registrants that are successfully registered).		
3.2.2	The Operators must ensure the eKYC solution accepts only the types of identification document listed in the relevant licence conditions, if information about the subscriber's identity is not provided from a trusted database.		
	If a passport is used as an identification document for validating the subscriber in the eKYC solution deployed, the passport must be an ICAO-compliant passport.		
3.2.3	The Operator must maintain a register containing records of all the information and particulars of the subscribers obtained during the registration, including any photo identification document for registration, and of any live photos or video taken for liveness detection, for a period of not less than twelve (12) calendar months from the date of termination of the service subscription.		
3.2.4.2	The Operator must put in place measures and restrictions in the eKYC solution for registration to be initiated only within Singapore.		
3.2.5	The Operator must ensure that the eKYC solution does not allow or enable the information readout (including photos taken) and analysis of the document verification and biometric authentication obtained during the registration to be modified by the subscriber.		

Section	Necessary Requirements under the Implementation Guide of eKYC solution for Mobile Service	Compliance (Yes/No)	Remarks
3.2.6	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.		
3.2.7	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 belong to the subscriber.		
	If the Operator uses facial recognition as a biometric authentication technique to verify the same against the photo identification documents for its eKYC solution, live photos or video of the subscriber must be taken during the registration via the ekYC solution. The Operator must not allow still images to be uploaded by subscriber to avoid digital fraud.		
	In addition, if a live video of the subscriber is taken during the registration via the eKYC solution, the Operator must require the subscriber to perform certain actions in real time in front of the camera (i.e. liveness detection), to prevent fraud and avoid identity theft.		
3.2.8	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.		

Section	Necessary Requirements under the Implementation Guide of eKYC solution for Mobile Service	Compliance (Yes/No)	Remarks
	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 (see below), with the use of the eKYC solution.		
3.3	***Monitoring of Transactions***		
3.3.1	The Operator must put in place security controls against unauthorised registration or access for the kiosk-based eKYC solution.		
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.		
	The Operator 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 Operator must not permit additional registrations through eKYC solution which will exceed the prescribed limit of the Prepaid Mobile Service to a subscriber. (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.)		

Section	Necessary Requirements under the Implementation Guide of eKYC solution for Mobile Service	Compliance (Yes/No)	Remarks
	The Operator must adopt measures in the eKYC solution, such as check-sum functions, to verify the authenticity of an identity number. This includes check-sum functions.		
3.4	***Risk Management***		
3.4.1	The Operator 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 Operator must ensure the eKYC solution deployed are at least in compliance with the ISO/IEC27002: 2013 Code of Practice for Information Security Controls including all amendments and revisions thereto from time to time in force.		
3.5	***Mobile Service Delivery***		
3.5	The Operator 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.		