CLARIFICATION NOTE ON ELECTRONIC KNOW-YOUR-CUSTOMER (E-KYC)

1.0 Preamble

1.1 This Clarification Note is issued pursuant to section 4A of the Labuan Financial Services Authority Act 1996 to provide clarity on Electronic Know-Your-Customer requirements pertaining to the Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Labuan Key Reporting Institutions (the Guidelines) issued on 21 May 2024.

2.0 Electronic Know-Your-Customer (e-KYC)[1]

Role and responsibility of the Board

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.1
>
> *"A Labuan KRI shall obtain the Board's approval on the overall risk appetite and internal framework governing the implementation to e-KYC."*

2.1 The framework also needs to address internal processes, mitigating controls and triggers for escalation to the Board where there may be potential concerns on the effectiveness of the e-KYC solution's performance and its related processes (e.g. change of technology provider, review of e-KYC results, sufficiency of reporting).

2.2 The Board is responsible for ensuring satisfactory measures are undertaken by the Labuan KRI such that an appropriate level of performance of the e-KYC solution is maintained at all times. The Board's responsibilities should include but are not limited to ensuring improvements are undertaken by Labuan KRI to

[1] Refer to paragraph B.6 of the Guidelines.

enhance the e-KYC solution in a regular and timely manner, and that the Board is satisfied that the performance of the e-KYC solution does not undermine the intended effectiveness of the identification and verification process.

Identification and verification of customers through e-KYC

A. General requirements

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.3
>
> *"A Labuan KRI shall ensure and be able to demonstrate on a continuing basis that appropriate measures for the identification and verification of a customer's identity through e-KYC are secure and effective."*

2.3 In line with the requirements under paragraph B.5 of the Guidelines, a Labuan KRI must ensure and be able to demonstrate on a continuous basis that appropriate measures for the identification and verification of a customer's identity through e-KYC are secured and remain effective. Measures for identification and verification shall be commensurate to the risk dimensions of e-KYC and its capabilities.

2.4 Where reference is made to face-to-face processes, this should mainly serve as guidance on the minimum expected baseline.

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.5
>
> *"In respect of paragraph 11.4, a Labuan KRI should have regard to the three basic authentication factors…"*

2.5 In respect of paragraph 11.4, a Labuan KRI may consider the key basic authentication factors, which include:

(i) Personal information that the customer possesses (e.g. national identity document such as an identity card, registered mobile number, company's certificate of incorporation);

(ii) Personal information that the customer knows (e.g. PIN, personal information, transaction history); and

(iii) Item that is uniquely identifiable only to the customer (e.g. biometric characteristics).

An e-KYC solution that depends on more than one factor is typically more difficult to compromise than a single factor system.

B. Identification and verification through e-KYC for individuals

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.6
>
> *"In identifying and verifying a customer's identity through e-KYC, a Labuan KRI may undertake measures including but not limited to the following…"*

2.6 In identifying and verifying an individual's identity through e-KYC, a Labuan KRI may undertake measures which at the minimum include:

(i) Document verification – i.e. ensuring that the government issued ID to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms;

(ii) Biometric matching – i.e. verifying the customer against a government issued ID[2] by utilising biometric technology; and/or

(iii) Liveness detection – i.e. ensuring the customer is a live subject and not an impersonator (e.g. through use of photos, videos, synthetic human face masks[3]) by utilising liveness detection.

C. Identification and verification through e-KYC for legal person

2.7 A Labuan KRI may implement e-KYC to identify and verify legal persons, subject to meeting the requirements in this Clarification Note and the CDD requirements for legal persons under paragraph B.5 of the Guidelines.

[2] I.e. National Registration Identity Card (NRIC), passport, or any other official documents.

[3] Synthetic human face masks are designed to impersonate real human faces and made from materials such as silicone or otherwise. For purposes of e-KYC, such masks may be used to defraud facial recognition software.

2.8 A Labuan KRI may wish to undertake one or more verification methods to establish business legitimacy, which may at the minimum include those under **Appendix 1**.

2.9 Where the identification and verification of the authorised person is conducted via electronic means, a Labuan KRI must ensure that:

(i) Electronic communication or documents that capture collective decision making by the directors of the legal person (e.g. digital forms of Directors Resolution or Letter of Authority) to appoint the authorised person and establish business relations, are maintained in accordance with relevant record keeping requirements under paragraph B.14 of the Guidelines;

(ii) Such electronic means adopted to identify and verify the authorised person are within the legal person's constitution or any other document which sets out the powers of the legal person; and

(iii) The authorised person is identified and verified through e-KYC as an individual, having due regard to the measures listed under paragraph 2.6 in this Clarification Note.

2.10 In respect of paragraph 2.9(i), such electronic means to capture collective decision making by the directors of the legal persons on the appointment of the authorised person may include at the minimum the following matters:

(i) Utilising electronic technologies that identify and verify the directors, and subsequently capture evidence of directors' consent (e.g. audited/ circulated email trails, providing agreement or disagreement through personal secure authentication links for directors to consent, video-conferencing to verify consent, digital signatures, use of secure electronic voting platforms, etc); and/or

(ii) Using third parties (e.g. Digital Company Secretaries) that may provide confirmation on the legitimacy of relevant evidence such as the Directors Resolution or Letter of Authority.

2.11 A Labuan KRI must undertake their own risk assessment to clearly define parameters for classifying potential legal persons that are not allowed to establish business relations through e-KYC.

Ensuring effective e-KYC implementation

2.12 A Labuan KRI must ensure that the appointed technology provider that provides the e-KYC solution conducts the following:

(i) Ensure that the e-KYC solution, encompassing the three (3) e-KYC modules comprising document verification, biometric matching and liveness detection under paragraph 2.6 in this Clarification Note:

(a) Has been assessed by a credible[4] external independent assessor in accordance with the scope and criteria as outlined in **Appendix 2**; and

(b) The technology provider has put measures in place to address the gaps or weaknesses identified from such assessment in a timely manner; and

(ii) Ensure that the relevant certification(s) is obtained for the various modules of the e-KYC solution, where such certification is available[5].

2.13 A Labuan KRI that have yet to implement e-KYC or wish to change the e-KYC solution or technology provider used, are required to ensure that:

(ii) A Labuan KRI must perform due diligence on the identified technology provider and the e-KYC solution. The due diligence, which need to be validated by an independent party, must include the following assessment areas:

(a) Whether the technology provider has a good track record, experience and expertise in offering solution involving regulated entities and products; and

(b) The technical capabilities of the e-KYC solution (e.g. parameters, methodology of models used); and

(ii) Prior to implementing the e-KYC solution, a Labuan KRI must fulfil the requirements in paragraph 2.12[6].

[4] Credible external independent assessor refers to an assessor who has the capability and expertise in conducting assessments on identity verification solutions.

[5] The modules are biometric matching/facial recognition, liveness test and ID verification. For example, ISO 197945 for facial recognition and ISO 30107-3 for liveness test (presentation attack detection) module.

[6] This requirement must be completed prior to implementation of the e-KYC solution unless:

(i) Such assessment has already been conducted by the technology provider within the past two (2) years; or

(ii) Where the technology provider has experience in applying the e-KYC solution effectively for other Labuan KRIs and has established a good track record, this requirement may be completed no later than one (1) year from the date of the Labuan KRI's e-KYC implementation.

2.14 A Labuan KRI must review or reassess requirements under paragraph 2.12 to ensure continuous relevancy of at least once every three (3) years, or where there are any material changes made to the e-KYC solution.

2.15 Notwithstanding the requirements of paragraphs 2.12 and 2.13, to ensure an effective overall implementation of e-KYC, a Labuan KRI must:

(i) Conduct an independent assessment on the Labuan KRI's own processes, procedures and controls prior to first-time implementation of an e-KYC solution; and

(ii) Undertake a review of the independent assessment on a regular basis, as may be determined by the Labuan KRI based on its own risk assessment.

Addressing ongoing vulnerabilities

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.14
>
> *"A Labuan KRI shall continuously identify and address potential vulnerabilities in the e-KYC solution.*

2.16 Where potential vulnerabilities[7] in the e-KYC solution are detected, a Labuan KRI must identify and adopt immediate mitigation measures where necessary, including for higher risk products.

[7] Potential vulnerabilities include exposures to IT, operational and ML/TF/PF related risks.

> ***Excerpt from the Guidelines:***
>
> Paragraph 11.15
>
> *"In respect of paragraph 11.14, actions to address potential vulnerabilities shall include conducting reviews on the e-KYC solution and, where applicable, submitting periodical feedback to technology providers with the aim of improving effectiveness of the underlying technology used for customer identification and verification."*

2.17 Actions to address potential vulnerabilities must also include risk considerations, trigger mechanisms and rectification measures as listed in **Appendix V** of the Guidelines.

2.18 The appendices in this Clarification Note may be updated from time to time to take account of the latest market developments. Updates on the appendices can be referred to Labuan FSA's website at https://www.labuanfsa.gov.my/amlcft/guidelines-directives-circulars.

Labuan Financial Services Authority

13 June 2024

APPENDICES

Appendix 1: Examples of verification methods to establish business legitimacy

1. In developing e-KYC methods for legal persons, a Labuan KRI may wish to consider undertaking at least one or more verification methods that is relevant to the nature or business model of the legal person. This aims to provide heightened assurance on the legitimacy of the legal person's business.

2. Such verification measures may at the minimum include:
   (i) make video calls to the CEO, directors, or authorised person assigned to the legal person. During the video call, Labuan KRI may request the person to show proof of business existence such as signboard or inventories (if any). A Labuan KRI may consider making unannounced video calls depending on the ML/TF/PF risk identified on a particular customer. Such unannounced call may be effective in identifying circumstances where a fraudulent business had staged its premise in advance of the call;
   (ii) identify and verify the location of legal person to ensure that the location matches the registered or business address of the legal person via methods that provide high levels of assurance and are legally permissible[8]. A Labuan KRI may also verify location of the CEO, directors, or authorised person during the video call;
   (iii) verify the legal person's information against a database maintained by credible independent sources such as relevant regulatory authorities, government agencies or associations of the regulated sectors. A Labuan KRI may also request for the legal person's active bank account statement or audited financial statement as proof of on-going business activity; and/or
   (iv) any other credible verification methods as proposed by Labuan KRI to Labuan FSA.

[8] Examples of such methods, which at the minimum include video calls, use of internet map/location services, drones, or visits by the Labuan KRI's agent network.

Appendix 2: Minimum scope and criteria for external independent assessment

Introduction

1. The Guidelines requires a Labuan KRI to ensure the systems and technology deployed for the purpose of establishing a business relationship using non-face-to-face channels (including e-KYC) have the capabilities to support an effective AML/CFT/CPF compliance programme.

2. Hence, the objective of the external independent assessment under paragraph 2.12 in this Clarification Note is to identify the overall effectiveness[9] and robustness of the e-KYC solution in detecting and mitigating ML/TF/PF and fraud risks at the point of customer on-boarding. The assessment must include any identified gaps/weaknesses in the e-KYC solution, areas for improvement and recommendations to address such gaps/weaknesses.

Scope

3. The assessment must cover the three (3) modules of an e-KYC solution, namely facial recognition, liveness detection (presentation attack detection) and Identity Document (ID) verification (which includes MyKad, international passports or any other common IDs used).

Criteria of assessment

4. The assessment must be conducted in accordance with an appropriate methodology that is clear, structured and effective in delivering the intended objectives.

5. The assessment must be conducted on a risk-based approach and must ensure areas of higher risk are given an appropriate level of focus and intensity.

6. The assessment must:

[9] Effectiveness is defined as the overall ability of the e-KYC solution to detect identity fraud and not deemed as indicating whether a particular e-KYC solution is being endorsed and/or more effective than others.

(i) Determine whether the e-KYC solution fulfils the requirements in relevant established standards and practices, if any;

(ii) Evaluate effectiveness of the methodology and key parameters used in the relevant modules of the e-KYC solution, to the extent possible;

(iii) Take into consideration any certifications and tests results/outcome on the e-KYC solution by credible independent bodies; and

(iv) Ensure breakthrough testing is conducted in accordance with the minimum requirements under paragraph 7 of this Appendix.

7. Breakthrough testing are tests conducted on the e-KYC solution from end-to-end to mimic a malicious attacker. Specific requirements for breakthrough testing on the e-KYC solution are as follows:

(i) The tests must be conducted in a comprehensive and effective manner, in line with emerging fraud techniques;

(ii) The tests must consist of various test scenarios for each module under the e-KYC solution, including the following as well as any other alternative but equally robust test scenarios:

Module	Test Scenarios
ID verification	(i) Physical tampering of ID (ii) Digital tampering of ID (iii) Use of fake ID (a) Low quality fakes (e.g., self-generated) (b) Medium quality fakes (e.g., ID that may be produced by printing shops) (c) If possible, use of high quality fakes
Facial recognition	(i) Tampering of selfie image but not ID (ii) Tampering of ID but not selfie image (iii) Tampering of both selfie image and ID (iv) Use of different person's selfie vs ID (e.g. Mr. A's selfie against Mr. B's ID)
Liveness test	Presentation attack detection test may be done in conformance to ISO/IEC 30107-3 standards, where there is increasing degree of sophistication as commercially

	available technology solution to product biometric artefacts become more readily available. This must include at the minimum the following: (i) Use of simple artefacts produced with equipment readily available in a normal home e.g., 2D mask; (ii) Use of 3D mask; (iii) Use of falsified biometric traits e.g. facial image using software readily available in the market 'ShallowFake' application; (iv) If possible, use of falsified biometric traits created using artificial intelligence technology "DeepFake" application; and (v) Coverage of the test scenarios must reflect the latest identity impersonation and cyber-attack techniques.

(iii) The tests must be done using an adequate sample size in accordance with the various test scenarios for each module. The number of test samples should be risk-based (for instance, a smaller number of test samples can be prepared for a module that has undergone credible tests or met a known benchmarked, whereas more vigorous testing is required with higher sample size for a module which has not undergone any credible test or benchmark).

(iv) Test samples must be representative of and adequately reflect the demographics of a Labuan KRI's customers (e.g., coverage of race, gender, age, etc).

(v) Test samples must consist of low, medium and high quality of samples[10].

(vi) The tests must include replay attacks test (e.g., resubmission of identical images test, man-in-the-middle attack via network layer packet transmission approach), where at least two rounds of random re-tests must be conducted.

[10] For example, low quality test samples are simple, fast and cheap to produce. Medium quality test samples are moderately difficult to produce, takes longer time (eg.1-3 days) and involves moderate investment. Where else high quality test samples are generally difficult/requires more expertise to produce, takes longer time and can be expensive.

(vii) For ID verification, it is recommended that the testing include the elements below:

(a) Detection of tampered personal data e.g. name, address;

(b) Detection and verification of micro print (e.g., existence and features of micro print, font type and size, unique colour);

(c) Detection and verification of hologram image (i.e., comparison of hologram image against ID image and selfie);

(d) Official markings (e.g., the Malaysian flag, MyKad logo, font type and size); and

(e) Identity card number (e.g., consistency of presented MyKad with existing numbering and format conventions, for passport the machine-readable zone (MRZ) bit-check number and format conventions); and

(viii) ID verification must include verification of passports that are compliant with International Civil Aviation Organisation (ICAO) standards. The ID verification on international passports must focus more on passports from countries where the Labuan KRI's customers are commonly from.

8. The outcome of the assessment must be adequately and clearly documented and must be submitted to the technology providers and subsequently submitted to the relevant Labuan KRIs. The outcome of the assessment must include the following:

(i) areas of gaps/weaknesses and areas for improvement; and

(ii) recommendations to address any weaknesses or gaps detected. This must also include recommendation on any certifications required.