BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Electronic Know-Your-Customer (e-KYC)

Exposure Draft

Applicable to:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed life insurers
5. Licensed family takaful operators
6. Prescribed development financial institutions
7. Licensed money-changing operators
8. Licensed remittance service providers
9. Approved non-bank issuers of designated payment instruments and designated Islamic payment instruments

`

Issued on: 16 December 2019 BNM/RH/ED 030-2

This exposure draft sets out the proposed requirements and guidance in implementing electronic Know-Your-Customer (e-KYC) solutions for the on-boarding of individuals to the financial sector.

The proposals in this exposure draft seek to accommodate advancements in technology to facilitate secure and safe adoption of e-KYC solutions, while preserving integrity the of the financial system.

Bank Negara Malaysia invites written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified and alternative proposals that the Bank should consider. The written feedback should be supported with clear rationale, accompanying evidence or appropriate illustrations to facilitate an effective review of this exposure draft.

Responses must be submitted by **17 February 2020** to:

Pengarah,
Jabatan Pembangunan dan Inovasi Kewangan
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: e-kycpolicy@bnm.gov.my

Electronic submission is encouraged. Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of preparing your feedback, you may direct any queries to the following officers at 03-26988044-

(i) Muhamad Faisal Khairol Anuar (ext. 7258); or
(ii) Ian Lee Wei Xiung (ext. 7381).

Issued on: 16 December 2019

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 The digitalisation of on-boarding processes is an important enabler to increase the convenience and reach, as well as lower the costs of financial services. A key aspect of digitalisation entails the delivery of end-to-end financial solutions through online and mobile channels, supported by the adoption of financial technology.

1.2 The digitalisation process, if not effectively managed, can become a source of risk to a financial institution and can undermine the integrity of financial transactions. The Bank expects the outcome of e-KYC technology adoption in the financial sector to include uncompromised accuracy in customer identification and verification, along with an on-going assessment of the robustness of the technology application.

1.3 This document sets out the minimum requirements and standards that a financial institution, as defined in paragraph 5.2, must observe in implementing e-KYC for the on-boarding of individuals. The requirements outlined in this policy document are aimed at-

(i) Enabling safe and secure application of e-KYC technology in the financial sector;
(ii) Facilitating the Bank's continued ability to carry out effective supervisory oversight over financial institutions; and
(iii) Ensuring effective Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) control measures.

2 Applicability

2.1 This document is applicable to all financial institutions as defined in paragraph 5.2.

2.2 This policy document shall not apply to agent banking channels governed under the Agent Banking policy document dated 30 April 2015.

3 Legal provisions

3.1 This policy document is issued pursuant to-

(i) sections 47(1) and 261(1) of the Financial Services Act 2013 (FSA);
(ii) sections 57(1) and 272 of the Islamic Financial Services Act 2013 (IFSA);
(iii) sections 41(1),126 and 123A of the Development Financial Institutions Act 2002 (DFIA);
(iv) sections 74 of the Money Services Business Act 2011 (MSBA); and
(v) sections 16 and 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities 2001 (AMLATFPUAA).

4 Effective date

4.1 This policy document comes into effect on [DD MM YYYY]

5 Interpretation

5.1 The terms and expressions in this policy document shall have the same meaning assigned to them in the FSA, IFSA, DFIA and MSBA unless otherwise stated.

5.2 For the purposes of this document-

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.

"**G"** denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted.

"the Bank" means Bank Negara Malaysia.

"financial institution" refers to-
(i) a licensed bank, investment bank and life insurer under the FSA;
(ii) a licensed Islamic bank and licensed family takaful operator under the IFSA;
(iii) a prescribed development financial institution under the DFIA;
(iv) an approved non-bank issuer of designated payment instruments under the FSA;
(v) an approved non-bank issuer of designated Islamic payment instruments under the IFSA; and
(vi) a licensed money-changing operator and/or a licensed remittance service provider under the MSBA.

"biometric" refers to a unique physical feature of a person based on a certain aspect of the person's biology. These include facial features, fingerprints or retinal patterns.

"Board" in relation to a company, refers to-
(i) directors of the company who number not less than the required quorum acting as a board of directors; or
(ii) if the company has only one director, that director.

"customer" refers to any individual who uses, has used or may be intending to use, any financial service or product offered by a financial institution.

"electronic Know-Your-Customer (e-KYC)" means establishing business relationships and conducting customer due diligence by way of electronic means, including online channel and mobile channel.

"False Positive" refers to the number of identity verification cases processed under e-KYC solutions for customer on-boarding purposes in which the solution accepted and verified an identity when said identity should have been rejected.

These include cases of false or unclear identities, forged or tampered documents and unclear images that were wrongly accepted.

"False Negative" refers to the number of identity verification cases processed under e-KYC solutions for customer on-boarding purposes in which the solution wrongly rejected and did not verify an identity when it should have been accepted. These include cases of genuine identities or documents that were wrongly rejected.

"True Positive" refers to the number of identity verification cases processed under e-KYC solutions for customer on-boarding purposes in which the solution rightly accepted and verified an identity. These include cases of genuine identities or documents that were rightly accepted.

"True Negative" refers to the number of identity verification cases processed under e-KYC solutions for customer on-boarding purposes in which the solution rightly rejected and did not verify an identity. These include cases of false or unclear identities, forged or tampered documents and unclear images that were rightly rejected.

Question 1:
The terms False Positive, False Negative, True Positive and True Negative form an essential component in measuring the accuracy of e-KYC solutions, as detailed further in paragraph 7.9 and Appendix 1 of this policy document. Kindly provide feedback on whether the definitions sufficiently cover the intended use cases for e-KYC in the industry.

6 Related legal instruments and policy documents

6.1 Where applicable, this policy document must be read together with any relevant legal instruments, policy documents and guidelines issued by the Bank, in particular-

(i) Exposure Draft on Anti Money Laundering, Counter Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) and any relevant policy document issued thereafter;
(ii) Risk Management in Technology (RMiT) dated 18 July 2019;
(iii) Outsourcing dated 28 December 2018;
(iv) Management of Customer Information and Permitted Disclosures dated 17 October 2017;
(v) Introduction of New Products dated 7 March 2014; and
(vi) Introduction of New Products by Insurers and Takaful Operators dated 15 May 2015.

PART B POLICY REQUIREMENTS

7 e-KYC implementation

Role and responsibility of the Board

S 7.1 A financial institution shall obtain approval from its Board prior to implementing e-KYC for each type of financial product or service.

> Question 2:
> Please provide feedback on the proposal to require the Board to give approval for each type of product or service.

S 7.2 The Board of a financial institution shall set and ensure the effective implementation of appropriate policies and procedures to address any risks associated with the implementation of e-KYC. These include operational, information technology (IT) and money laundering and terrorism financing (ML/TF) risks.

Identification and verification through e-KYC

S 7.3 A financial institution 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.

S 7.4 A financial institution shall adopt an appropriate combination of authentication factors when establishing measures to verify the identity of a customer being on-boarded through e-KYC. The strength and combination of the authentication factors shall be commensurate to the risks associated with inaccurate identification for a particular product or service.

G 7.5 In respect of paragraph 7.4, a financial institution should have regard to the three basic authentication factors, namely, something the customer possesses (e.g. identity card, registered mobile number), something the customer knows (e.g. PIN, personal information) and something the customer is (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.

G 7.6 In identifying and verifying a customer's identity through e-KYC as required by the Exposure Draft on AML/CFT and TFS for FIs, a financial institution may undertake measures including but not limited to the following-

(i) utilise biometric technology to verify the customer against a government issued ID;

(ii) utilise fraud detection technology to ensure that the government issued ID used to support e-KYC customer verification is authentic; and

(iii) utilise liveness detection technology to ensure the customer is a live subject and to detect impersonation attempts (e.g. use of photos, videos, facial masks).

Question 3:
Please suggest any other key considerations that are relevant in identifying and verifying a customer's identity.

Ensuring effective e-KYC implementation

G 7.7 e-KYC solutions may utilise artificial intelligence, machine learning or other forms of predictive algorithms to ensure accurate identification and verification. This may result in automation of the decision-making process for customer on-boarding, thus reducing the need for human intervention.

S 7.8 Where the decision to verify a customer's identity through e-KYC is automated with the use of artificial intelligence, machine learning or other forms of predictive algorithms, whether in whole or in part, a financial institution shall ensure that the e-KYC solution is capable of accurately distinguishing between genuine and non-genuine cases of customer on-boarding.

S 7.9 For the purposes of paragraph 7.8, in ensuring accuracy of the e-KYC solution, a financial institution shall take steps to minimise the False Acceptance Rates (FAR), defined as $\frac{False\ Positive}{(False\ Positive + True\ Negative)}\ x\ 100$. In measuring and assessing the FAR, a financial institution shall observe the considerations and requirements listed in Appendix 1[1].

Question 4:
Please provide feedback on the following:
- Potential challenges in implementing the requirements for FAR specified in Appendix 1; and
- Alternative suggestions on the collection or measurement of FAR.

S 7.10 A financial institution shall continuously identify and address potential vulnerabilities[2] in the e-KYC solution.

S 7.11 In respect of paragraph 7.10, 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.

[1] For avoidance of doubt, requirements for FAR within this policy document, do not apply to e-KYC solutions where verification of customer identity is automated without the use of artificial intelligence, machine learning or other similar forms of predictive algorithms.
[2] Potential vulnerabilities include exposures to IT, operational and ML/TF related risks.

Additional safeguards to facilitate deployment

G 7.12 The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification.

S 7.13 Where there are limited data points to determine accuracy of the e-KYC solution in the initial deployment stage, a financial institution shall consider additional safeguards, particularly for products that pose higher risks arising from inaccurate identification.

S 7.14 To facilitate deployment of e-KYC solutions for products with higher risks arising from inaccurate identification, a financial institution shall observe the considerations and safeguards specified in Appendix 2. This list may be updated as and when there are developments in the e-KYC landscape, including availability of better performance data on the effectiveness of particular e-KYC methods.

Question 5:

- What would be the challenges, if any, to comply with the considerations and safeguards specified in Appendix 2?
- While more secure, the credit transfer safeguard limits the deployment of e-KYC solutions in the first phase to those with an existing bank account. What are possible measures to facilitate e-KYC for new-to-market customers? In lieu of the credit transfer safeguard, are there other safeguards that are equally or more effective?
- How should the credit transfer safeguard be applied in the case of a joint account holder?

8 Reporting requirements

S 8.1 In monitoring the effectiveness and accuracy of e-KYC solutions utilising artificial intelligence, machine learning or other forms of predictive algorithms, a financial institution shall maintain a record of the performance of the e-KYC solution segregated on a monthly basis in accordance with the reporting template specified in Appendix 3.

S 8.2 A financial institution shall submit the record in relation to paragraph 8.1 to the Pengarah, Jabatan Pembangunan dan Inovasi Kewangan, Bank Negara Malaysia on half year basis according to the following arrangement-

(i) For the period of January to June of each year, the record shall be submitted no later than 15 July of the same year; and

(ii) For the period of July to December each year, the record shall be submitted no later than 15 January the following year.

Question 6:
What would be the challenges, if any, to comply with the reporting requirements in paragraphs 8.1 – 8.2?

PART C REGULATORY PROCESS

9 "File-and-use" system for licensed persons and prescribed development financial institutions

S 9.1 Subject to paragraph 7.1 and 7.2, a licensed person [3] or a prescribed development financial institution[4] that meets the requirements stipulated in this policy document may proceed to implement e-KYC upon the submission of a complete list of information as set out in Appendix 4. This process shall be referred to as the "file-and-use" system. The submission of information to the Bank shall be made to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be and shall be signed off by the Chief Executive Officer, Chief Risk Officer or Chief Operating Officer who has the responsibility to ensure that the information submitted pursuant to this paragraph is complete and accurate.

S 9.2 In respect of paragraph 9.1, a licensed person or a prescribed development financial institution shall proceed to implement and utilise e-KYC after 14 working days from the date of receipt by the relevant Departments of the Bank of the complete submission of information set out in Appendix 4.

Question 7:
Please provide feedback on the proposed "file-and-use" system approach for licensed persons and prescribed development financial institutions.

G 9.3 Where a licensed person or a prescribed development financial institution intends to offer, through e-KYC, a new product as defined under the Introduction of New Products policy document[5], the information required under the aforementioned policy document and this policy document may be submitted together to the Bank.

S 9.4 Prior to submission through the "file-and-use" system, a licensed person or a prescribed development financial institution, where relevant, shall ensure compliance to the Bank's RMiT and Outsourcing policy documents.

Question 8:
Please provide feedback on the proposal to require compliance with Outsourcing and RMiT prior to submission to implement e-KYC.

[3] As defined under the FSA or IFSA.
[4] As defined under the DFIA.
[5] Or in the case of life insurers and family takaful operators, the Introduction of New Products by Insurers and Takaful Operators policy document.

10 Approval for licensed money-changing operators, licensed remittance service providers, approved non-bank issuers of designated payment instruments and approved non-bank issuers of designated Islamic payment instruments

S 10.1 Subject to paragraphs 7.1 and 7.2 and as required under the Exposure Draft on AML/CFT and TFS for FIs, licensed money-changing operators, licensed remittance service providers, approved non-bank issuers of designated payment instruments and approved non-bank issuers of designated Islamic payment instruments shall obtain a written approval from the Bank prior to implementing e-KYC.

S 10.2 In respect of paragraph, 10.1, application for approval shall include a complete list of information as set out in Appendix 4.

11 Enforcement

S 11.1 Where the Bank deems that the requirements in this document have not been complied with, the Bank may take appropriate enforcement action against the financial institution, including the directors, officers and employees with any provision marked as “S” in this document or direct a financial institution to-

(i) undertake corrective action to address any identified shortcomings; and/or

(ii) suspend or discontinue implementation of e-KYC.

APPENDICES

Appendix 1: False Acceptance Rate

1. In measuring the accuracy and effectiveness of e-KYC solutions, the FAR may be considered a useful measurement as it captures the capability of the solution to identify non-genuine on-boarding cases. Generally, a lower FAR indicates that the e-KYC solution has correctly identified non-genuine or fraudulent on-boarding cases on a regular basis.

2. FAR shall be based on the number of on-boarding attempt cases.

3. In determining FAR, a financial institution shall conduct manual reviews to classify on-boarding cases into genuine and non-genuine cases. Where it is not feasible for a financial institution to review every single on-boarding case facilitated through e-KYC, a financial institution may adopt a sampling approach. In doing so, a financial institution shall ensure that the data used to determine FAR is random, unbiased and representative of the customer base.

4. A financial institution shall aim to ensure that the overall FAR for the e-KYC solution does not exceed 5%. However, the level of FAR should also take into consideration the number of on-boarding cases and the risks associated with inaccurate identification for a particular product or service offered through e-KYC.

5. Generally, for e-KYC solutions leveraging the use of artificial intelligence, FAR should reduce with the increase in on-boarding cases processed.

6. Where the overall FAR for any type of product is measured to be more than 5% for three consecutive months, a financial institution shall notify Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan, Jabatan Penyeliaan Insurans dan Takaful, Jabatan Pengawalan Perniagaan Perkhidmatan Wang or Jabatan Pemantauan Pembayaran, as the case may be, in writing. The notification shall be made within seven working days and include the following-
   (i) An assessment on the current performance of the e-KYC solution, including reasons for the observed level of FAR;
   (ii) Proposed action plan to reduce the FAR going forward; and
   (iii) Proposed mitigating actions or additional controls to safeguard the effectiveness of the e-KYC solution. These mitigating actions or additional controls may be withdrawn should the FAR be no higher than 5% for 3 consecutive months.

7. In respect of paragraph 6 of this Appendix, the mitigating actions and/or additional controls may include but are not limited to the following-
   (i) Enhanced monitoring of customers on-boarded through e-KYC; and/or
   (ii) Conducting manual reviews for on-boarding cases prior to opening an account.

Appendix 2: e-KYC safeguards to be adopted by financial Institutions offering higher risk financial products

1. List of products subjected to e-KYC safeguards-
   (i) Current account; and
   (ii) Savings account.

2. A financial institution offering the financial products in paragraph 1 of this Appendix through e-KYC for the purpose of customer on-boarding shall at minimum include the following-
   (i) utilise biometric technology to verify the customer against a government issued ID;
   (ii) utilise fraud detection technology to ensure that the government issued ID used to support e-KYC customer verification is authentic;
   (iii) utilise liveness detection technology to ensure the customer is a live subject and to detect impersonation attempts (e.g. use of photos, videos, facial masks); and
   (iv) require a customer to perform a credit transfer from the customer's existing bank account with another licensed person and ensure the customer details (e.g. name) returned on said transfer is consistent with the initial details supplied by the customer.

Appendix 3: Reporting Template

1. The performance data below shall be recorded when reporting e-KYC on-boarding cases performed by a financial institution-

	(Year)			
Data	**January**	**…**	**June**	**Total**
Total on-boarding attempt cases performed				
Total on-boarding attempt cases that was cleared by solution				
Total sample size for on-boarding attempts reviewed				
True Positive (no. of cases)				
True Negative (no. of cases)				
False Positive (no. of cases)				
False Negative (no. of cases)				
False Acceptance Rate (%)				
False Rejection Rate (%), defined as $\frac{False\ Negative}{(False\ Negative + True\ Positve)}\ x\ 100$				

2. A robust e-KYC solution may consist of a series of e-KYC checks (e.g. document authenticity and liveness checks as outlined in paragraph 7.6) in identifying and verifying a customer. Where a financial institution utilises a series of e-KYC checks in the solution, the performance data below shall be recorded for each e-KYC check-

	(Year)			
Type of e-KYC checks	**January**	**…**	**June**	**Total**
Document authenticity, segregated by-				
a) *MyKad*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
b) *Passport*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
c) *Other official identity documents*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
Liveness detection				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
Biometric matching				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				

3. Other relevant metrics to be reported-

Optical Character Recognition (OCR) rate, defined as: $1 - \frac{Number\ of\ cases\ with\ at\ least\ 1\ misidentified\ character}{Total\ number\ of\ cases}$	
Average time taken for completion of e-KYC process: Average time taken from start of application to: a) Completion of application (minutes); b) Account opening (hours); and c) Account activation (hours).	

Appendix 4: Information Required for Submission

1. A detailed product description, including its features, structure and target market or customers. Product illustrations shall also be included where appropriate.

2. Sample product term sheet.

3. Detailed information on the key features of the e-KYC solution. This may include types of checks, customer information captured and any other material information.

4. A written assessment on the effectiveness of the e-KYC solution. The written assessment may consider technology functions, types of checks included and any other relevant information that may attest for the effectiveness of the underlying technology. Where a financial institution chooses to engage a technology provider, this may include company background and track record in other jurisdictions or industries.

5. Description of key inherent risks of the e-KYC solution and arrangements in place to manage those risks. Where a financial institution deems it necessary, plans for implementation of enhanced monitoring and reporting mechanisms to identify potential ML/TF activities should also be included in the description.

6. Detailed end-to-end process flow of the e-KYC solution. This may include but is not limited to an illustration of the customer journey from on-boarding to account opening.

7. Any other relevant information to demonstrate a financial institution's ability to comply with the standards in this document and any other related policy documents issued by the Bank, including, where applicable-
   (i) RMiT policy document; and
   (ii) Outsourcing policy document.

8. Any additional documents or information as may be specified by the Bank.