4.3.5 Use of electronic identification (E-ID)

B

Overview

E

66. With the ongoing development of remote working and circumstances where *customers* are not able to be met face-to-face, *relevant persons* are increasingly making use of smart phone and tablet applications to capture information, copy documents and take images, liveness checks (including micro streaming) or video recordings of *customers* as part of their *CDD* processes (defined in this Handbook as *E-ID*). This Section will set out provide guidance and (where relevant) set out *AML/CFT Codes of Practice* in respect of:

    - The relevant legal and regulatory obligations in relation to *CDD*
    - The relevant legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers
    - Risk factors inherently associated with the use of *E-ID* applications
    - Examples of risk mitigants to consider when assessing the potential use of a particular *E-ID* method or application and
    - *E-ID* methods which are not permitted.

67. The FATF has issued guidance on Digital Identity, March 2020 which *relevant persons* may find useful in developing their own procedures and controls.

68. The guidance in this Section may also be relevant in situations where similar processes are undertaken but carried out through means other than smart phone and tablet applications, e.g. the use of self-service kiosks with similar document and image capturing and verification technology.

69. In order to adequately consider the risks associated with *E-ID*, the *relevant person's* Board/*senior management* should clearly identify, fully understand and document what the *E-ID* application does and does not do. For example:

    - Is it to be used only to collect information about an individual (**finding out identity**)?
    - Is it to be used to obtain **evidence** of that individual's identity?
    - Is it to be used to collect more general relationship information about an individual from that individual, e.g. *source of funds*?
    - Is it to be used to collect information about an individual from reliable and independent data sources? If so, where do these data sources originate and have they been assessed as to their reliability and/or independence?

70. Where it is identified that an *E-ID* application does not cover particular elements of *identification measures* (or more general *CDD* measures) then, in line with Article 13 of the Money Laundering Order, those elements should continue to be applied using a *relevant person's* existing *systems and controls* (including *policies and procedures*). For example, a *relevant person* could decide to use an *E-ID* application to find out and evidence identity, whilst, at the same time, employ a more traditional method to establish and verify a *customer's* address.

Deleted: <#>Guidance on Products and Services¶ <#>¶ <#>E-ID¶

Deleted: The purpose

Deleted: this section is

Deleted: assist

Deleted: who

Deleted: considering the

Deleted: photographs

Deleted: referred to hereafter

Deleted: "

Deleted: "). It

Deleted: explains

Deleted: ;

Deleted: explains

Deleted: ;

Deleted: highlights

Deleted: smart phone and tablet

Deleted: to capture information, copy documents and take photographs; and

Deleted: provides some

Deleted: smart phone and tablet

Deleted: .

Deleted: This guidance

Deleted: , risks and potential mitigants are present (for example in assessing the risks presented by

Deleted:).

Deleted: <#>Background¶

Deleted: <#>properly

Deleted: <#>it will be necessary for

Deleted: <#>to be very clear about

Deleted: <#>smart phone and tablet

Deleted: <#>what it

Deleted: from that individual?

Deleted: also

Deleted: To the extent

Deleted: a smart phone and tablet

Deleted:),

Deleted: these

71. The *JFSC* is aware that a range of *E-ID* applications are commercially available for use by *relevant persons*. *Relevant persons* might also make use of *E-ID* applications which have been developed in-house or within their wider corporate group. The guidance provided in this section is not intended to express any preference or favour towards any particular method of *E-ID*, or any particular *E-ID* application. The *JFSC* does not endorse nor advise on specific methods or providers available to *relevant persons*. It remains the decision of the *relevant person* whether *E-ID* should be utilised in any given circumstance, and/or whether the *relevant person* will develop its own *E-ID* application for these purposes, or select an *E-ID* application that is commercially available. This choice may be determined, for example, based on the *relevant person's customer* base and how the *relevant person* conducts its business.

4.3.5.1 Legal and regulatory obligations relevant to E-ID

B

Statutory Requirements (paraphrased wording)

C

72. *Article 3(4) of the Money Laundering Order explains that identification of a person means:*

- ***Finding out the identity*** *of that person, including that person's name and legal status and*
- ***Obtaining evidence*** *on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who they are said to be, and satisfies the person responsible for the identification that the evidence does establish that fact.*

Overview

E

73. Using an *E-ID* application is one way of obtaining evidence of identity. Section 4.3.2 of this Handbook explains how a *relevant person* may demonstrate that it has **obtained evidence** that is reasonably capable of verifying that an individual to be identified is who they are said to be. Among other things, it states that use of the following documentary evidence will be reasonably capable of verifying an individual's identity:

- A current passport, or copy of such a passport certified by a suitable certifier
- A current national identity card, or copy of such a national identity card certified by a suitable certifier or
- A current driving licence, or copy of such a driving licence certified by a suitable certifier.

For the avoidance of doubt, there is no regulatory requirement to use either original or "wet ink" /certified documents.

74. As an alternative to using documentary evidence, Section 4.3.4 of this Handbook permits, in certain circumstances, the use of **independent data sources** to verify that the person to be identified is who they are said to be. In practice, it may be possible to demonstrate compliance with Article 3(4) of the Money Laundering Order through a combination of documentary evidence and independent data sources.

75. A *relevant person* may use other tools and/or methods (including *E-ID* applications) to undertake *CDD* measures, so long as such methods comply with Article 3(4) of the Money Laundering Order.

Deleted: in relation

Deleted: CDD

Deleted: ;

Deleted: the person is

Deleted: of a person

Deleted: the AML/CFT

Deleted: the individual is

Deleted: Inter alia

Deleted: ;

Deleted: ;

Deleted: the AML/CFT

Deleted: the person is

Deleted: customer due diligence

Statutory Requirements (paraphrased wording)

C

76. *Article 11 of the Money Laundering Order requires a relevant person to have policies and procedures for the identification and assessment of risks that arise in relation to the use of new or developing technologies for new or existing products or services.*

77. *Article 15(3) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures when the customer has not been physically present for identification purposes.*

AML/CFT Codes of Practice

D

78. The requirements under Articles 11 and 15(3) of the *Money Laundering Order* and the *AML/CFT Code of Practice* set out at Section 2.4.4 will apply in any circumstances where a part of the *CDD* process is undertaken by an independent third party via the use of *E-ID* applications, where the *customer* is not present. Accordingly, when deciding whether to make use of a particular *E-ID* application, a *relevant person* must undertake a risk assessment comprising of the following:

    - Consider the risks involved in the use of the *E-ID* application and record the reasons why its use is appropriate
    - Consider the risks involved in outsourcing any part of the *CDD* process to an independent third party using the *E-ID* application and record the reasons why such outsourcing is appropriate
    - Consider whether the features of the *E-ID* application effectively mitigate the risks identified
    - Apply any additional measures to ensure that all risks are effectively managed
    - Apply, on a risk-sensitive basis, *enhanced CDD measures* to take account of the particular risks arising due to the fact that the *customer* has not been physically present for identification purposes.

79. A risk assessment as described in the paragraph above is not required to be undertaken by the *relevant person* on each occasion that the particular *E-ID* application is used, but rather when considering whether to incorporate the use of that *E-ID* application into its *CDD* measures.

80. When using technology to on-board a *customer* remotely, i.e. when there is no face-to-face interaction because the parties are not in the same physical location and conduct activities by digital or other non-physical present means, for example when interacting via a video call, mail or telephone, *enhanced CDD measures* must be applied.

81. The approval by a *relevant person* of the use of one *E-ID* application must not be taken to constitute approval of the use of all *E-ID* applications. Each *E-ID* application must be risk-assessed separately and on its own merits.

82. The *relevant person* must ensure that adequate and effective *policies and procedures* are supporting the use of the *E-ID* application, and are catering for the technology that is being used, as well as for the *relevant person's* business practices.

83. The *relevant person* must ensure appropriate training is in place.

4.3.5.2 Risk of using E-ID

Deleted: <#>Legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers¶

Deleted: <#>An AML/CFT Code in Section 2.4.4 of the AML/CFT Handbook (and other Handbooks) requires a relevant person to assess, record and monitor risk when any element of the CDD process is outsourced to another party.¶
<#>The Commission considers that all three requirements

Deleted: new technologies

Deleted: smart phone or tablet

Deleted: is required to

Deleted: smart phone or tablet

Deleted: .

Deleted: smart phone or tablet

Deleted: .

Deleted: smart phone or tablet

Deleted: work to

Deleted: .

Deleted: .

Deleted: For the avoidance of doubt,

Deleted: this

Deleted: smart phone or tablet

Deleted: deciding

Deleted: the

Deleted: <#>Risks¶

Deleted: smart phone and tablet

B

Overview

E

84. The use of *E-ID* applications to apply *identification measures* presents a number of inherent risks. Typically, an *E-ID* application will do one or more of the following:

    - Capture information, copy documents and capture an image (e.g. take a photograph) of the *customer* (for instance by way of a camera on a smart phone or tablet)
    - Transmit the information, documents or image (either to the *relevant person* or another party)
    - Compare the information, documents and image captured
    - Verify the information or documents against external data sources.

Guidance Notes

E

85. A *relevant person* may demonstrate that it has considered the particular risks that arise when using *E-ID* applications to copy documents and take photographs for *CDD* purposes when it considers the risks set out below.

86. Risk: Documents are tampered with or forged:

    - When original documents are not physically presented, it is more difficult for a *relevant person* to detect that documents have been tampered with or forged. For example, it may be difficult to detect that another individual's photograph has been fraudulently inserted into a passport when simply viewing an electronic copy of that document.
    - Similarly, it may be difficult to detect the presence or absence of watermarks or other built-in security features on an identity document when simply viewing an electronic copy of the document.

87. Risk: Captured copies of documents or images are tampered with before or during transmission:

    - When an electronic copy of a document or an image has been captured there may be opportunities for the *customer* (or another party) to use software to alter the copy of the document or image before transmitting it. For example, it may be possible for a *customer* to alter details (such as name and date of birth) on the copy of the passport prior to transmission. Similarly, it may be possible to use software to alter the photograph and other biometric data on a copy of an identity document.

88. Risk: Documents presented are stolen or their use unauthorised:

    - When a *customer* is not physically presenting identification documents, it is more difficult for a *relevant person* to detect that the documents do not belong to the *customer*. For example, a customer may present stolen documentation when using the *E-ID* application.

Deleted: may

Deleted:);

Deleted: photograph

Deleted:);

Deleted: photograph

Deleted: ;

Deleted: smart phone and tablet

Deleted: at sections to .

Deleted: The risk that identification

Deleted: a

Deleted: ,

Deleted: the passport

Deleted: The risk that

Deleted: photographs

Deleted: or photograph has been taken,

Deleted: photograph

Deleted: from the smart phone or tablet.

Deleted: when a customer is merely transmitting a scanned copy of a passport,

Deleted: ,

Deleted: <#>Similarly, it may be possible to alter the biometric data (such as a photograph) on a copy of an identity document.¶
<#>The risk that

4.3.5.3 Factors to consider when assessing E-ID applications

B

Overview

E

89. This section lists some potential features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risks listed at Section 4.3.5.2 above. Where the *E-ID* application (or connected system) does not sufficiently mitigate the risk, the *relevant person* will need to ensure that its *CDD systems and controls* (including *policies and procedures*) incorporate measures specifically designed to do so.

90. The features described in the *Guidance Notes* below do not represent an exhaustive list. A *relevant person* may consider other features, *systems and controls* (including *policies and procedures*) appropriate.

Guidance Notes

E

91. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents have been tampered with or forged may include:

    - The copy of the document is of a very high level of clarity and resolution, such that its contents can be adequately reviewed without undue difficulty (i.e. the clarity and resolution is still sufficient when zooming in to view a particular element of the document)
    - The copy of the document is automatically matched to a pre-defined "template" for the particular form of identity document used to compare the security features ingrained in the document presented
    - The data in the main body of the document is compared to biometric or other data stored in the document's machine readable zone (MRZ) code
    - Data on the document is automatically examined for use of unauthorised print fonts and unexpected character spacing
    - The copy of the document is automatically examined to enable detection of fraudulent documents on the basis of that documents' security features (e.g. watermarks, biographical data, photographs, lamination, UV sensitive ink lines holograms, micro-text, etc.) and the location of various elements in the document (i.e. optical character recognition).
    - The copy of the document is examined by individuals specifically trained to detect tampering/forgery (e.g. ex-border agents) or to spot situations where the person on screen looks different from the person within the document.

92. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that a copy of a document or photograph has been tampered with or forged before or during transmission may include:

Deleted: Considerations for

Deleted: smart phone and tablet

Deleted: .

Deleted: smart phone or tablet

Deleted: include

Deleted: list of

Deleted: is

Deleted: and

Deleted: or

Deleted: may be

Deleted: <#>Risk that identification documents are tampered with or forged¶

Deleted: smart phone and tablet

Deleted: viewed and/or enlarged to aid review;

Deleted: "template'

Deleted: ;

Deleted: Data on

Deleted: and

Deleted: on

Deleted: /algorithm on the document;

Deleted: ;

Deleted: confirm

Deleted: existence

Deleted: .);

Deleted: individual(s)

Deleted:).¶
Risk that captured documents

Deleted: photographs are tampered with before or during transmission

Deleted: smart phone and tablet

- The *E-ID* application itself controls the process of copying the document, taking photographs and transmitting the same, allowing no opportunity to tamper with or manipulate documents or photographs. This is in contrast with, for example, a prospective *customer* taking a photograph of a document and transmitting the PDF by e-mail, which presents multiple opportunities for interference
- A highly secure connection is used to transmit copies of documents and photographs
- The *E-ID* application's security is regularly tested in order to guard against hacking or other security breaches.

93. Features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents presented are stolen (or their use unauthorised) may include:
    - A "selfie" photograph of the *customer* is taken **and** biometrically compared/matched to the photograph on the identity document presented, in order to verify that they relate to the same individual
    - A video or a "micro-stream" of photographs is taken in order to identify facial movements, which may help to confirm that the *customer* is present at the time that the video/stream of photographs is taken. Use of anti-impersonation measures such as requiring the user to verbally repeat a word or phrase as dictated by the relevant person during a video or "micro-stream". This may also help to prevent the use of a video/stream of photographs which may have been stolen or use of which is unauthorised
    - A code or password is sent to the *customer* who, immediately before the application of E-*ID*, is photographed while displaying the code or password - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised
    - Use of location matching, where the *E-ID* application determines that information and copies of documents are captured and photographs taken at a location that is consistent with the *customer's* place (or country) of residence.
    - The requirement that any image taken is adequately illumined when using the E-ID solution.

4.3.5.4 Record-keeping requirements relevant to the use of E-ID

B

Guidance Notes

F

94. Where a *relevant person* uses *E-ID* applications to capture information, copy documents and take photographs of *customers* as part of their *CDD* processes, adequate records must be kept in line with the record-keeping requirements set out in Part 4 of the Money Laundering Order.
95. Detailed *AML/CFT Codes of Practice* and *Guidance Notes* are provided at Section 10 of this Handbook regarding the requirements of Part 4 of the Money Laundering Order.

Deleted: smart phone or tablet
Deleted: of
Deleted: photography, and transmission process
Deleted: ,
Deleted: ,
Deleted: (Compared to
Deleted: instance
Deleted:);
Deleted: ;
Deleted: Application
Deleted: <#>Risk that documents presented are stolen or their use unauthorised¶
Deleted: <#>smart phone and tablet
Deleted: -
Deleted: person;
Deleted: "
Deleted: -
Deleted: photograph
Deleted: -
Deleted: avoid a photograph being taken of
Deleted: photograph
Deleted: ;
Deleted: ;
Deleted: a
Deleted: match –
Deleted: smart phone or tablet

4.3.5.5 E-ID Methods not permitted by this Handbook

B

Overview

E

96. Whilst there are a range of *E-ID* applications which incorporate features that the *JFSC* considers may allow a *relevant person* to comply with Article 3(4) of the Money Laundering Order, some other methods are not currently deemed to sufficiently address the risks listed at Section 4.3.5.2 and are therefore **not** permitted.

97. Biometric and similar matching/checking technology is referred to in the *AML/CFT Code of Practice* below. The *FATF* describes biometrics as an individual's personal biological or behavioural characteristics. *E-ID* applications may make use of the following biometrics as part of their verification processes:

    - Biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints and facial recognition
    - Biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system
    - Behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, for example, an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns.

AML/CFT Codes of Practice

D

98. Use of video calls where an identity document is produced during the call for comparison, but no biometric or similar matching/checking technology is employed, e.g. the *customer* just holds up their passport during a video call. This method must not be used due to:

    - There being no independent authentication process alongside the identification document being produced, hence the process is not adequately robust.
    - The risk of 'deep fake' technology being utilised, whereby the video image and voice of an individual can be manipulated to look and sound like another individual. Again, biometric and similar matching/checking technology is considered necessary for this risk to be adequately mitigated.

    Whilst a *relevant person* may wish to hold a video call in order to meet a potential customer and discuss elements of the proposed *business relationship* (including **finding out identity** or other customer information), the video call must not be used for the purposes of obtaining **evidence of identity**. An *E-ID* application, or other alternative method, may be used for that purpose, enabling the independent authentication process.

99. Using scanned copies of documents in themselves as evidence of identity – this method must not be used due to:

› The risk that an identity document has been tampered with or forged not being mitigated through the use of specialist checks. The scanned copies in this case are in effect non-certified and non-authenticated. If scanned copies are to be used as evidence, they must be independently verified/authenticated. That verification process may include, for example, the use of third party data sources or the use of an *E-ID* application in instances when such technology utilises automated verification technology in a robust and appropriate way. It may, for example, verify data embedded in the scanned document (barcodes, micro-lettering etc.).

100. Using a "selfie" photograph of the *customer* **without** it being biometrically compared/matched to the photograph on the identity document presented in order to verify that they relate to the same individual, e.g. the *customer* taking a "selfie" photograph of themselves holding up their passport – this method must not be used due to:

› The risk that an identity document has been tampered with or forged not being mitigated through the use of specialist checks.

If, however, such a "selfie" photograph is being uploaded to an *E-ID* application which then undertakes authenticity checks to verify identity, for example by extracting machine-readable text or hologram data, and verifying the data in an appropriate, independent way to ensure it is robust, then this is an acceptable method to evidence identity.