INTERNATIONAL STANDARD

ISO 5158

First edition
2023-01

Mobile financial services — Customer identification guidelines

Services financiers mobiles — Lignes directrices relatives à l'identification des clients

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

Reference number
ISO 5158:2023(E)

© ISO 2023

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2023 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Introduction

With the rapid penetration of mobile devices into every aspect of people's daily lives, mobile financial services (MFS) have emerged as a result of the convergence of financial industry and ICT technologies. MFS provide people with convenient access to basic financial services, such as payments, and are therefore a great attraction for financial inclusion.

Much effort has been made to use financial technologies (fintech) to reduce the cost and improve the efficiency of financial services. "Electronic know your customer (eKYC)" is a typical example of such fintech, and market demand is growing rapidly due to MFS. Traditional KYC procedures, which usually require customers to visit a bank branch to enrol for financial services in person, are time-consuming, inconvenient and not suitable for lightweight MFS. In contrast, eKYC can provide a more competitive alternative, giving end users more convenient access to financial services and helping financial service providers attract more users.

Customer identification is at the core of eKYC. A mobile device can provide access to a number of information sources which can be used for customer identification, such as:

— text message;

— phone call;

— location-based services (LBS);

— microphone (voice print);

— camera (photo identity document, human face, motions);

— various sensors (fingerprint, motions);

— contact and contactless local interfaces (to external credential carriers); and

— internet connection (to third-party identity providers).

However, KYC requirements and practices, especially online or remote eKYC, vary widely in different jurisdictions. The identity evidence collected through a mobile device and the identity established based on this evidence can differ greatly in terms of trustworthiness and assurance. The industry needs a commonly-agreed standard to guide it on how to choose proper customer identification solutions for MFS according to different KYC requirements. This document establishes such a common standard by defining assurance levels (ALs) for identity evidence and corresponding identities in the context of MFS.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

Mobile financial services — Customer identification guidelines

1 Scope

This document provides guidelines for customer identification in mobile financial services (MFS), including:

— a general framework of customer identification for MFS;

— the multi-dimensional overall identity assurance level (AL) of an MFS customer and its evaluation criteria;

— security and privacy considerations.

This document also contains annexes which demonstrate how to apply the ALs in practice, through (e) KYC use cases in different regions, for example.

This document is applicable to various kinds of MFS providers, including but not limited to commercial banks and third-party payment service providers.

This document is applicable to identifying natural persons. Identifying legal entities, known as (e)KYB, is out of the scope of this document.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12812-1, *Core banking — Mobile financial services — Part 1: General framework*

ISO/IEC 24760-1, *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12812-1, ISO/IEC 24760-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
assurance level
AL
amount of assurance obtained according to the specific scale used by the assurance method

[SOURCE: ISO/IEC 19792:2009, 4.1.1, modified — Note 1 to entry removed.]

© ISO 2023 – All rights reserved

3.2
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 19784-1:2018, 4.17]

3.3
customer
person or business that has contracted with a mobile financial services provider (MFSP) in order to use mobile financial services (MFS)

Note 1 to entry: Only customers who are natural persons are covered by this document.

[SOURCE: ISO 12812-1:2017, 3.12, modified — Note 1 to entry added.]

3.4
evidence issuer
identity information provider or *identity information authority* (3.7) which issues the identity evidence

3.5
identity
set of attributes related to an entity

Note 1 to entry: The entity is a natural person in this document.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2, modified — Notes to entry replaced.]

3.6
identity assurance level
IAL
parameter used to describe the amount of assurance in a subscriber's *identity* (3.5) obtained by a credential service provider

Note 1 to entry: IAL1 indicates that there is no requirement to link the applicant to a specific real-life identity.

Note 2 to entry: IAL2 indicates that evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity.

Note 3 to entry: IAL3 requires physical presence.

[SOURCE: NIST SP-800-63A:2019, 2.2, modified.]

3.7
identity information authority
IIA
entity related to a particular domain responsible for the life cycle management of trusted identities, which can make provable statements on the validity and/or correctness of one or more attribute values in an *identity* (3.5)

Note 1 to entry: An identity information authority is typically associated with the domain, for instance the domain of origin, in which the attributes, which the identity information authority can make assertions on, have a particular significance.

Note 2 to entry: The activity of an identity information authority is usually subject to a policy on privacy protection.

Note 3 to entry: An entity can combine the functions of identity information provider and identity information authority.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.3, modified — Definition and Note 2 to entry revised.]

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

4 Abbreviated terms

AI	artificial intelligence
AL_E	assurance level of existence
AL_IDx	overall identity assurance level of customer x
AL_P	assurance level of presence
AL_R	assurance level of reachability
AL_U	assurance level of uniqueness
AL_W	assurance level of willingness
AML	anti-money laundering
BR	biometric reference
CDD	customer due diligence
CRM	customer relationship management
eKYC	electronic know your customer
FAR	false acceptance rate
FRR	false rejection rate
IC	integrated circuit
IIP	identity information provider
KBV	knowledge-based verification
KYC	know your customer
LoIP	level of identity proofing
MFS	mobile financial services
MFSP	mobile financial services provider
MNO	mobile network operator
NPI	natural person identifier
OTP	one-time password
PII	personal identifiable information
REE	rich execution environment
SE	secure element
TEE	trusted execution environment

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

5 General framework of customer identification for MFS

5.1 Identity of an MFS customer

Identity is the representation of an entity (natural person) in the form of one or more information elements (known as "attributes") which allow the entity to be sufficiently distinguished within a context.

The identity attributes can consist of something that:

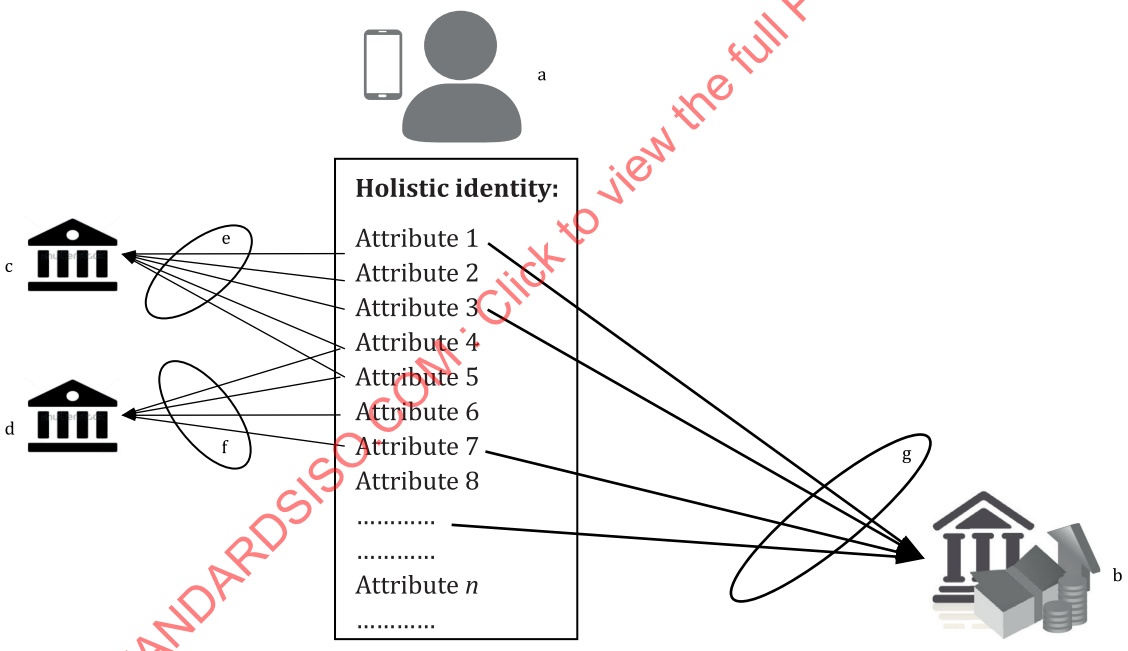
— characterizes the entity, for example biometric characteristics;

— the entity chooses, for example an email address;

— the entity has been assigned, for example an identity number assigned by the national authority;

— constitutes other personal information associated with the entity (natural person), for example geolocation.

The combination of all attributes of the entity (unlimited number) is called a "holistic identity". In the context of MFS, the identity of an MFS customer should be regarded as a "contextual identity", which consists of a limited set of attributes which are sufficient for verifying that the entity who is applying for a service is the one who was enrolled previously, as depicted in Figure 1.



Key

a MFS customer.

b MFS provider.

c IIP/IIA which can provide Attributes 1 to 5.

d IIP/IIA which can provide Attributes 4 to 7.

e MFS customer's identity as of key reference [c].

f MFS customer's identity as of key reference [d].

g MFS customer's identity as of key reference [b].

Figure 1 — Identity and attributes

A contextual identity, once established, should be able to be confirmed or verified using authentication methods, such as something that the MFS customer possesses, knows, or is (inherence such as biometrics). Identity authentication methods are out of the scope of this document.

The natural person identifier (NPI) and its data record, as defined in ISO 24366, is recommended as the reference when the MFS providers select the set of attributes to identify their customers. An NPI issuer

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

can be regarded as an identity information provider (IIP) or an identity information authority (IIA), depending on local regulations.

Local KYC and anti-money laundering (AML) regulations usually define several mandatory attributes for initial identification of the financial customers. See Annex B for examples.

Depending on the nature of specific financial services, it is possible that additional identity attributes will be needed, for example geolocation (home address or office address), employment status or emergency contacts.

5.2 Identification of an MFS customer

Identification of a financial services customer, known as (e)KYC in the financial sector, includes identity proofing, enrolment and continuous maintenance of the customer's identity attributes required to provide certain financial services. General concepts of identity proofing and enrolment can be found in ISO/IEC TS 29003.

The identification process for an MFS customer should be composed of the following basic steps.

a) The MFS customer provides core verifiable attributes as required by the MFS provider and/or provides eligible identity evidence to support the claimed attributes.

b) The MFS provider validates, by all possible means, the authenticity, validity and eligibility of the identity attributes and evidence provided by the MFS customer.

c) The MFS provider verifies, by all possible means, the links between the MFS customer and the provided identity attributes and evidence, as well as the willingness of the MFS customer to apply for the specified services.

d) The MFS provider enrols the MFS customer after successful initial verification of required identity attributes and continuously maintains (adding, removing or updating) the MFS customer's identity attributes according to the business and compliance requirements.

In step a), there are different ways to collect identity attributes, for example:

— self-claimed by the customer, for example:
  — ask the customer to fill in a table (text attributes);
  — ask the customer to upload a selfie (facial image);
— retrieval from an identity document presented by the customer, for example:
  — ask the customer to upload a photo of an identity card (usually equipment with certain anti-forgery measures);
  — ask the customer to present a digital identity document containing certain identity attributes (usually with a digital signature);
— retrieval from a database, for example:
  — retrieve identity attributes from a specialized third-party IIP;
  — retrieve identity attributes from a domain-specific IIA.

NOTE 1 Additional information can be requested from the customer in order to allow the retrieval of attributes from a database and to link the relevant attributes, for instance by pressing a finger on a fingerprint sensor (e.g. fingerprint database on VISA information systems or the Indian Aadhaar eKYC use case; see Annex B).

In step b) and step c), the MFS provider should, by all possible means, confirm the following aspects:

— the authenticity, validity and eligibility of the identity attributes and evidence provided by the MFS customer;

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

— the links between the MFS customer and the provided identity attributes and evidence;

— the willingness of the MFS customer to apply for the specified services.

Depending on the different ways to confirm these three aspects, the MFS provider can achieve different levels of assurance in the identity of an MFS customer.

NOTE 2 Although the customer is aiming to access some MFS, the identity proofing process can occur partially, entirely or not at all on mobile devices.

5.3 Assurance levels

The overall assurance level of an MFS customer's identity should be defined as a multi-dimensional vector. In particular, this document defines the following dimensions.

— Assurance on uniqueness: AL_U

  How confident the MFS provider can be that the customer identity is unique in the specific MFS provider's domain.

— Assurance on existence: AL_E

  How confident the MFS provider can be that the customer identity corresponds to a real-life subject, i.e. the genuineness of the identity attributes and/or evidence.

— Assurance on presence: AL_P

  How confident the MFS provider can be of the links between the present MFS customer and the provided identity attributes and/or evidence.

— Assurance on willingness by consent: AL_W

  How confident the MFS provider can be of the willingness of the MFS customer to apply for the specified services.

— Assurance on reachability: AL_R

  How confident the MFS provider can be that the customer can be contacted when necessary. This is an additional criterion, not directly bound to the identity but used to manage the overall risk related to the MFS customer.

These dimensions may be tailored and other dimensions may be added according to the jurisdictional AML or related requirements. The willingness and reachability dimensions are included as example dimensions to group some identity attributes which are not directly used to identify a customer, but which are indispensable for the MFS provider to make business decisions.

The overall identity assurance level of an MFS customer, "x", should be noted as follows:

$$AL\_IDx = (AL\_U, AL\_E, AL\_P, AL\_W, AL\_R, \ldots)$$

Each dimension should be evaluated against the criteria which are commonly agreed upon and recognized within the MFS provider's domain. Details are provided in Clause 6.

NOTE AL_IDx is intended as a vector, not a simple score. But if the MFS provider needs to calculate a simple score, the weighting of each dimension can be defined according to its KYC policy and a weighted sum can be calculated and assigned to AL_IDx.

It is recommended that the AL value of each dimension ranges from 0 to 1, both included. But other kinds of value domain are also acceptable according to the needs of the MFS providers.

Based on the different identity ALs, the MFS provider can grant differentiated services to its customers. Examples are provided in Annex B.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

 © ISO 2023 – All rights reserved

As part of the customer due diligence (CDD) requirements, the MFS provider can increase or decrease the AL(s) in one dimension or more for a specific customer over time, for example when the contact information is no longer valid, the AL_R is decreased. The MFS provider can also ask the customer to increase the AL(s) in one dimension or more if the customer wants to apply for a service which requires higher AL(s).

6 Evaluation of multi-dimension identity AL

6.1 Evaluation criteria for AL_U

Table 1 shows the recommended evaluation criteria for AL_U. A brief risk analysis is also provided.

Table 1 — Recommended evaluation criteria and risk analysis for AL_U

AL_U value	Description	Criteria	Risk analysis
0	No assurance of uniqueness	The MFS customer does not need to enrol or log in to access a service, for example to browse the real-time foreign exchange rates.	When a security incident arises with a customer, it cannot be traced back to a particular customer.
(0, 1)	Ambiguous	The MFS customer needs to provide certain identity attribute(s), such as age or geolocation, to access a service.	When a security incident arises with a customer, it cannot be traced back to a particular customer but can be traced back to a subset of possible customers, for instance when first name and surname have been recorded without additional identifying attributes.
1	Uniqueness assured	The MFS customer needs to provide adequate identity attribute(s) so that they can be uniquely identified by the MFS provider in the specific MFS provider's domain by: — a single attribute (e.g. a national identity number or unique biometric characteristic); or — an adequate set of attributes (e.g. a combination of name, date of birth and facial image).	None.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

6.2 Evaluation criteria for AL_E

6.2.1 General

The recommended evaluation criteria for AL_E is as follows.

Step 1: Determine the AL of an identity evidence according to Table 2 by the overall AL or eligibility of the evidence issuer, and the security and risk-control measures which are leveraged during evidence validation:

— physical evidence: anti-forgery measures;

— digital evidence and online IIP database: security measures such as digital signature.

More details are provided in 6.2.2 and 6.2.3.

© ISO 2023 – All rights reserved

Step 2: Determine the AL of an identity attribute by the maximum AL, as in Formula (1), or a weighted sum of the ALs of its supporting identity evidence(s), as in Formula (2):

$$L_{\mathrm{a}} = \max(L_{\mathrm{e1}}, L_{\mathrm{e2}}, \ldots, L_{\mathrm{e}n}) \tag{1}$$

where

L_{a} is the AL of the identity attribute, a;

L_{e1} is the AL of the first identity evidence to support this attribute;

L_{e2} is the AL of the second identity evidence to support this attribute;

$L_{\mathrm{e}n}$ is the AL of the last identity evidence to support this attribute.

$$L_{\mathrm{a}} = \frac{1}{n}\sum_{i=1}^{n} w_i \times L_{\mathrm{e}i} \tag{2}$$

where

L_{a} is the AL of the identity attribute, a;

n is the total amount of collected evidence to support this attribute;

$L_{\mathrm{e}i}$ is the AL of the ith identity evidence to support this attribute;

w_i is the weight assigned to the ith identity evidence to support this attribute, with the constraint that $\sum_{i=1}^{n} w_i = 1$ and $w_i \in [0,1]$;

Step 3: Determine the AL of customer existence by the minimum AL of its mandatory attributes, as in Formula (3):

$$L_{\mathrm{E}} = \min(L_{\mathrm{a1}}, L_{\mathrm{a2}}, \ldots, L_{\mathrm{a}m}) \tag{3}$$

where

L_{E} is the AL of customer existence (AL_E);

L_{a1} is the AL of the first mandatory attribute;

L_{a2} is the AL of the second mandatory attribute;

$L_{\mathrm{a}m}$ is the AL of the last mandatory attribute.

6.2.2 Identity evidences used in MFS environment

Identity evidence used in MFS environments can be classified as follows.

— Digitalized physical evidence, for example a photo of a driving licence (containing a facial image), a photo of a bank card.

— Digital identity, for example a digital certificate containing the owner's identity information and related attributes (e.g. fingerprints) held on a physical token such as an identity integrated circuit (IC) card, which can generate a digital signature for identification, or in software.

— Online identity information database, for example an interface to access the mobile network operator (MNO) customer relationship management (CRM) database or an interface to access a governmental IIA.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

In particular, biometrics are very commonly used as part of the identity evidence. There are three ways that a person can be identified using biometrics:

— identification based on the biometric information on the facial image in an identity document;

— identification based on biometric information stored in the IC chip of an identity document;

— identification based on biometric information stored in a central database.

6.2.3 Evaluation criteria of identity evidence ALs

Table 2 shows the recommended evaluation criteria for identity evidence. A brief risk analysis is also provided.

Table 2 — Recommended evaluation criteria and risk analysis for identity evidence ALs

Evidence AL value	Description	Criteria	Risk analysis
0	Evidence is not dependable	The evidence is revoked, or the evidence issuer is: — not eligible according to the MFS provider's KYC policies; or — evaluated as IAL 1 (NIST), LoIP 1 (ISO/IEC TS 29003) or equivalent.	The evidence cannot be linked to a real life individual.
(0, 0,9)	Evidence is partly dependable	The evidence issuer is: — eligible according to the MFS provider's KYC policies; or — evaluated as IAL 2/3 (NIST), LoIP 2/3 (ISO/IEC TS 29003) or equivalent; and the evidence issuer provides certain levels of: — anti-forgery measures to protect the physical evidence which can be verified remotely; or — security measures such as digital signature which can be leveraged to verify the authenticity and integrity of the digital evidence.	The evidence can potentially be forged or tampered with, depending on the strength of the protection measures.
(0,9, 1)[a]	Evidence is believed to be genuine and valid	The evidence issuer is: — eligible according to the MFS provider's KYC policies; or — evaluated as IAL2/3 (NIST), LoIP 2/3 (ISO/IEC TS 29003) or equivalent; and digital evidence or online IIP database is provided, protected by security measures such as digital signature and/or secure communication protocol and verified as genuine and valid at the time of the verification based on a revocation check mechanism	Low risk.

[a] In practice, there is no way to guarantee 100 % confidence in a piece of identity evidence, so the evidence AL value is always lower than "1" in spite of all the security measures. The corresponding risk is "low" but not "none".

Once the mandatory attributes of a customer are selected, the evidence of each attribute should be evaluated according to Table 2 and the overall AL_E value should be computed according to the rules defined in 6.2.1.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

6.3 Evaluation criteria for AL_P

There are different ways to confirm the presence of a customer, for example:

— knowledge-based verification (KBV) challenges, such as a payment history;

— biometric verifications, such as facial image, fingerprint, voiceprint;

— physical presence over the counter or by a visited MFS employee, during which the presentation of a possession is verified, for example a passport, an identity card or a phone registered to the customer.

In the MFS environment, biometric verifications are the most recommended way to confirm the presence of a customer. The ALs of biometric verifications are dependent on two major factors:

— the AL of the biometric reference (BR), usually contained in a piece of identity evidence (see Table 2 for details);

— the security and risk-control measures, such as:

  — the intrinsic risks of a specific biometric modality;

  — the capability to detect a presentation attack (see the ISO/IEC 30107 series for details);

  — the false acceptance rate (FAR) and false rejection rate (FRR) of a biometric implementation.

To evaluate the security of biometric authentication technologies and systems, see ISO/IEC 19792. To evaluate the performance of biometric technologies and systems, see the ISO/IEC 19795 series.

Table 3 shows the recommended evaluation criteria for AL_P. A brief risk analysis is also provided.

Table 3 — Recommended evaluation criteria and risk analysis for AL_P

AL_P value	Description	Criteria	Risk analysis
(0, 0,1)	Low assurance that the present applicant is the intended MFS customer to be enrolled	One of the following verifications is performed: — KBV challenges, e.g. a payment history; — biometric verifications[a] where the BR is at least partly dependable (evidence AL>0) but the security and risk-control measures are not in place.	The knowledge-based information can potentially be controlled by an attacker. The BR can potentially not belong to the intended customer.
(0,1, 0,9)	Medium assurance that the present applicant is the intended MFS customer to be enrolled	One of the following verifications is performed: — KBV challenges, for example a payment history, and proper risk-control measures are in place, for example verification of applicant's location or operation habits; — biometric verifications[a] where the BR is at least partly dependable (evidence AL>0) and a certain level of security and risk-control measures are in place.	Presentation attacks, false acceptance and false rejections.

[a] For countermeasures to biometric attacks, see ISO 19092.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Table 3 *(continued)*

AL_P value	Description	Criteria	Risk analysis
(0,9, 1)	The applicant's presence is highly assured.	Any means equivalent to in-person verification, for example: — high-level assurance process is performed, such as biometric verifications[a] where the BR is dependable (evidence AL>=0,9) and the security and risk-control measures are sufficient, for example artificial intelligence (AI) enabled strong liveness detection; — physical presence over the counter or by a visited MFS provider employee.	Low risk.
[a] For countermeasures to biometric attacks, see ISO 19092.			

6.4 Evaluation criteria for AL_W

There are different ways to confirm the willingness of a customer by consent, for example:

— asking to confirm consent by reading the terms and conditions;

— asking explicitly to fill in a specific sentence;

— remote video interactions, for example asking the applicant to answer "yes" to some questions regarding the applied MFS service;

— physical presence over the counter or by a visited MFS employee and directly asking questions to confirm consent.

Table 4 shows the recommended evaluation criteria for AL_W. A brief risk analysis is also provided.

Table 4 — Recommended evaluation criteria and risk analysis for AL_W

AL_W value	Description	Criteria	Risk or residual risk analysis
(0, 0,1)	The applicant provides consent implicitly	Validation of terms and conditions.	The applicant can potentially give consent without confirming the terms and conditions.
(0,1, 0,5)	The applicant provides consent explicitly	Confirm by writing an explicit message.	The applicant can potentially not have understood the applied service correctly.
(0,5, 0,9)	The applicant provides an answer in live interactions	Remote video interactions with dedicated questions.	The applicant can potentially be under coercion or decoy.
(0,9, 1)	Assured physically	Physical presence over the counter or by a visited MFS provider employee with dedicated questions.	Low risk.

6.5 Evaluation criteria for AL_R

Table 5 shows the recommended evaluation criteria for AL_R. A brief risk analysis is also provided.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Table 5 — Recommended evaluation criteria and risk analysis for AL_R

AL_R value	Description	Criteria	Risk analysis
0	No assurance	No physical address, phone number, email or other contact information is verified.	There is no way to contact a particular customer if there is such a need.
(0, 0,9)	Assured online	Assured by means of, for example, email one-time password (OTP), mobile OTP or phone call, and/or physical address verified against an identity evidence.	The customer can be contacted online but cannot be reached in person. The online contact information becomes outdated. The customer provides fraudulent contact information or an attacker impersonates the customer through technical means (e.g. leveraging the vulnerability of signalling system).
(0,9, 1)	Assured offline	a) The customer provides a physical address which is verified by postal mail or other means. b) The MFS provider employee visits the customer in person.	The physical address becomes outdated. The customer provides fraudulent contact information.

7 Security and privacy considerations

7.1 Personal data protection of customer information

7.1.1 General privacy issues

The principles of ISO/IEC 29100 should be followed to ensure that the applicable privacy properties are fulfilled and that the specific context of personal information collection and processing are handled accordingly.

7.1.2 Biometrics-related vulnerabilities and privacy issues

Biometric data is vulnerable during transmission between different components. It can be intercepted, recorded or tampered with. When biometric data is used for financial services, the key is to protect data against such attacks. Data integrity should be protected during transmission.

When it comes to privacy, only necessary biometric information is collected to reflect personal identifiable information (PII) requirements.

When biometric information is collected during the identification process, it should be protected in accordance with ISO/IEC 24745. If it is no longer necessary after the identification, any biometric information should be securely deleted. If it is kept for auditability, recovery or any other reason, it should be protected in accordance with ISO/IEC 24745.

ISO 19092 provides more information on a security framework for using biometrics in financial services. The list of biometric security controls should be followed when using biometrics for customer identification in MFS.

7.2 Device side security

One of the standardization challenges is the understanding of the role(s) of the mobile device in an MFS. Depending on the implementation, the mobile device can be seen as a channel for using a

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

payment instrument or for accessing a banking service, or as a tool for customer identification and/or authentication.

In the MFS environment, many security- and privacy-sensitive operations are carried out on mobile devices, for example the collecting and processing of customers' personal information for KYC purposes. The MFS provider can leverage the security capabilities provided by a mobile device, for example trusted execution environment (TEE) and/or secure element (SE), during the customer identification process to raise the assurance levels of eKYC (see Clause 6) or to protect customer privacy (see 7.1).

See Annex A for more information about device side security capabilities and ISO/TS 12812-2:2017, 8.1 for detailed requirements.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Annex A
(informative)

Security capabilities of mobile devices related to customer identification

A.1 Overview

This annex describes the framework of the mobile device environment as well as the security capabilities which can be leveraged by the MFS provider to raise the assurance levels of eKYC.

The environment of mobile device is generally formed of the rich execution environment (REE), TEE, SE and various hardware.

A.2 Rich execution environment (REE)

The REE refers to the standard operating system that the device is running. It provides the environment to run the applications related to, for example, payments, communication, entertainment, games and social media. It includes the following:

— Application level: general applications, such as bank applications and wallet applications.

— System software level: mobile operating system, hardware drivers for cameras, flash memory, universal serial bus (USB), and touch screen. It also provides the system service, application service and management framework for the development and deployment of different applications. For those mobile devices which support access to the TEE, it should provide the communication driver to access the TEE and external application program interface (API) for the TEE.

A.3 Trusted execution environment (TEE)

A TEE is an execution environment inside the mobile device that runs alongside but is isolated from the environment provided by the operating system (OS) of the mobile device. A TEE has security capabilities and meets certain security-related requirements. It protects some assets from general software attacks, defines rigid safeguards as to data and functions that an application can access, and resists a set of defined threats.

The TEE's ability to offer safe execution of authorized security software, known as "trusted applications" (TAs), enables it to provide end-to-end security by protecting the execution of authenticated codes, confidentiality, authenticity, privacy, system integrity and data access rights.

The TEE objective is to prevent the financial application from being executed by the generic OS of the mobile device as the OS will possibly not be a sufficiently secure environment for the application. The TEE offers an API to applications residing in the mobile device.

There are multiple technologies that can be used to implement a TEE and the level of security achieved varies accordingly. It can be implemented by the mobile device manufacturer.

It can be implemented by different techniques, including the following.

— Application level: security-related applications will generally combine with the applications running in the REE to provide a convenient and secure user experience. These applications include fingerprint authentication, payment and identity certifications.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

— System software level: hardware resources such as the central processing unit (CPU), random-access memory (RAM), and flash memory are utilized to provide the hardware-level isolated environment. This can be used to provide the following functions:

  — secure encode or decode, secure storage, trusted user interface, trusted identification certification and other system-level services;

  — system and application security of secret key;

  — secure communication mechanisms for REE, SE and external devices, including the related access control;

  — provide trusted virtual level to support multiple trusted operating systems.

A TEE can be used together with a SE hosting the application. This configuration provides a trusted user interface (display and keypad) and thus the transaction data displayed on the mobile device are those generated and/or transmitted by the SE.

A.4 Secure element (SE)

An SE is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (e.g. cryptographic keys) in accordance with the rules and security requirements set out by well-identified trusted authorities. There are different form factors of SE, including embedded and integrated SEs, subscriber identity module (SIM) or universal IC cards, smart microSD and smart cards. SEs exist in different form factors to address the requirements of different business implementations and market needs.

The SE can be used to prevent hardware- and software-level attacks. The applications running in the SE have high security needs, including the following.

— Application level: security-related application, such as financial, public transport, social security or telecommunications, which should be deployed via pre-setting or under the TSM control.

— System software level: card operating system, mainly providing functions such as secure encoding or decoding and secret key storage.

A.5 Peripheral hardware

Additional hardware sensors or readers, such as fingerprint, iris and near field communication (NFC) can also be found on mobile devices. However, not all mobile devices support all sensors or readers.

In some instances, these sensors or readers can be controlled by the TEE.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Annex B
(informative)

Case study of (e)KYC practices

B.1 General

This annex is based on publicly available information. It aims to demonstrate how an MFS provider can "translate" the regulatory requirements into technical policies based on the framework and criteria specified in Clauses 5 and 6.

B.2 (e)KYC practices for banking accounts

B.2.1 Overview

Generally, the (e)KYC requirements for banking accounts are stricter than those for payment accounts. Table B.1 gives some examples.

Table B.1 — (e)KYC requirements for banking accounts

Country	Level	KYC requirement	Restrictions
China (personal banking accounts)	Class I	Face-to-face verified	Can be used for deposit, cash withdrawal, financial investment, money transfer, consumption payment and bill payment. There is no limit to account balance or transaction amount.
	Class II	Option 1: Face-to-face verified. Option 2: At least the following attributes are verified remotely: — name, — national ID number, — cell phone number, — class I personal banking account to be bound with. Biometrics verification is encouraged.	Can be used for deposit, financial investment, consumption payment and bill payment. Account payment cannot exceed CNY 10 000 daily.
	Class III	Same as Class II.	Can only be used for consumption payment and bill payment. Account balance cannot exceed CNY 1 000.
India	n/a	— Permanent account number (PAN) card. — Aadhaar[a] verified.	Most common savings account.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved

Table B.1 *(continued)*

Country	Level	KYC requirement	Restrictions
Malaysia	n/a	— Valid national identity card[b] or passport (for foreigners). — Resident permit or Malaysia my second home (MM2H) visa documents (foreigners only). — Employment details.	n/a
Singapore	n/a	Face-to-face verified or SingPass.[c]	n/a
Sweden	n/a	Information needed to open a bank account: — personal identity number issued at the time of resident registration; — identification card with personal identity number (identity card). Information required to obtain BankID[e]: — personal identity number; — bank account that can issue a BankID.	n/a

Key

n/a = not applicable

NOTE All information is correct as of 2020.

[a] Aadhaar is an Indian program which provides a unique identifier (a random 12-digit number) to residents and provides authentication and an eKYC service to its RPs. When registering an Aadhaar number, not only basic information but also biometric information is registered. Biometric information is used to check for double registration. In the context of MFS, the Aadhaar e-KYC service plays the role of an IIA for an MFS provider, which can provide a digital identity document and online identity information database as the identity evidence. The MFS provider can verify a customer's identity using the customer's Aadhaar number and a fingerprint and/or iris scan.

[b] MyKad, a government-issued multipurpose smart card in Malaysia.

[c] Singpass is government-operated identity that is available to all Singapore residents who are at least 15 years old. The National Registration Identification Cards (NRIC) are distributed to all Singapore residents who are at least 15 years old. The Foreign Identification Numbers (FIN) are unique identification numbers issued by the Immigration & Checkpoints Authority (ICA) and government agencies to foreigners who are working, studying, or residing in Singapore. SingPass allows users to use NRIC or FIN numbers and passwords to access government services online.

[d] A personal identity number is a combination of a six-digit number for the date of birth and a four-digit number that varies from person to person. All personal records, from birth to school attendance to tax payments, are managed based on personal identity numbers. Resident registration is required to obtain a personal identity number. Under-age persons must always have parental consent.

[e] BankID used in mobile banking is managed by a bank consortium in Sweden. More than half of banking transactions conducted by BankID users are internet banking transactions.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

B.2.2 Mapping of (e)KYC requirements to AL_ID

An MFS provider can "translate" the regulatory (e)KYC requirements into technical ALs based on the framework and criteria specified in Clauses 5 and 6. An example is given in Table B.2.

© ISO 2023 – All rights reserved

Table B.2 — Mapping of (e)KYC requirements to AL_ID

Account levels	KYC requirements	AL_ID
Class I	Face-to-face verified.	AL_U=1[a] AL_E=[0,9, 1) AL_P=[0,9, 1) AL_W=[0,9, 1) AL_R=[0, 1)
Class II	Can be verified remotely and one Class I bank account with the same name needs to be bound with it. Biometrics verification is encouraged.	AL_U=1[a] AL_E=[0,9, 1) AL_P=[0,1, 1) AL_W=[0,1, 1) AL_R=[0, 1)
Class III	Can be verified remotely and one Class I bank account with the same name needs to be bound with it. Biometrics verification is encouraged.	AL_U=1[a] AL_E=[0,9, 1) AL_P=[0,1, 1) AL_W=[0,1, 1) AL_R=[0, 1)

[a] According to the AML requirements on the financial institutions in China, the basic identity information of a natural person customer includes the customer's:

— name,

— gender,

— nationality,

— occupation,

— address of residence or working place,

— contact information,

— type, number and validity period of the identity evidence.

According to Table 1, these nine identity attributes compose an identity which can achieve AL_U=1. The MFS provider can define their own set of attributes to identity a customer based on the needs of different services, but they are not allowed to provide AML-risky financial services to a customer whose AL_U is lower than 1.

During enrolment, the MFS provider can select proper (e)KYC mechanisms based on Tables 1 to 5 according to the services a customer applies. During the account life cycle management, the MFS provider can assign or adjust the customer's AL_ID dynamically based on Tables 1 to 5 and use this as a factor in deciding which services can be provided to the customer.

B.3 (e)KYC practices for payment accounts

B.3.1 Overview

Payment accounts are different from banking accounts. They are provided by non-banking payment institutions and used mainly for payment purposes. It is possible that a payment account is or is not bound to one or more banking accounts.

In some practices, the (e)KYC requirements on payment accounts are classified into different levels, which in turn result in different restrictions. Some examples are given in Table B.3.

STANDARDSISO.COM : Click to view the full PDF of ISO 5158:2023

© ISO 2023 – All rights reserved