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

Reference number
ISO 5158:2023(E)

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

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 General framework of customer identification for MFS **4**
5.1 Identity of an MFS customer 4
5.2 Identification of an MFS customer 5
5.3 Assurance levels 6
6 Evaluation of multi-dimension identity AL **7**
6.1 Evaluation criteria for AL_U 7
6.2 Evaluation criteria for AL_E 7
6.2.1 General 7
6.2.2 Identity evidences used in MFS environment 8
6.2.3 Evaluation criteria of identity evidence ALs 9
6.3 Evaluation criteria for AL_P 10
6.4 Evaluation criteria for AL_W 11
6.5 Evaluation criteria for AL_R 11
7 Security and privacy considerations **12**
7.1 Personal data protection of customer information 12
7.1.1 General privacy issues 12
7.1.2 Biometrics-related vulnerabilities and privacy issues 12
7.2 Device side security 12
Annex A (informative) **Security capabilities of mobile devices related to customer identification** **14**
Annex B (informative) **Case study of (e)KYC practices** **16**
Bibliography **22**

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.

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.

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.

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.]

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.]

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

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:

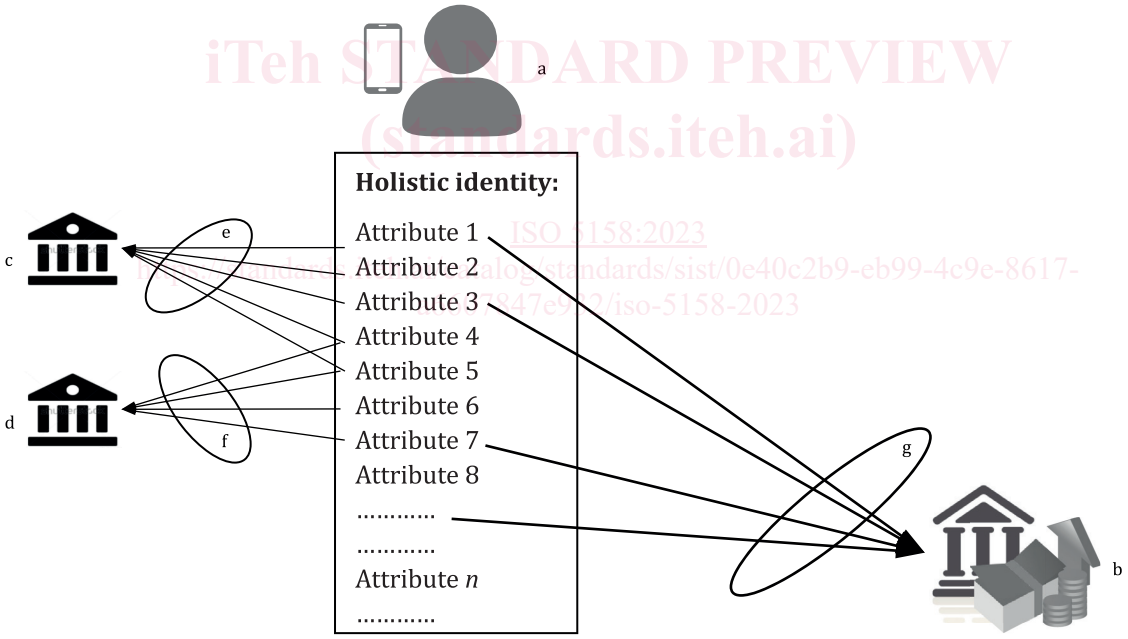
— characterizes the entity, for example biometric characteristics;

— 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

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;

— 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.

