INTERNATIONAL STANDARD

ISO 12812-1

First edition
2017-03

Core banking — Mobile financial services —

Part 1: General framework

Opérations bancaires de base — Services financiers mobiles —

Partie 1: Cadre général

Reference number
ISO 12812-1:2017(E)

© ISO 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **8**

5 Concept of interoperability **9**
5.1 General 9
5.2 Concept of interoperability for payments: the business layer 9
5.3 Concept of interoperability for payments: the technical layer 9
5.4 Interoperability objectives 9

6 Relationships between customers and MFSPs **10**
6.1 General 10
6.2 Legal status of the customer 10
6.3 Role played by the customer 10
6.4 Contractual relationship between the customer and the institution 11
6.5 Choice of wording for ISO 12812 (all parts) 11

7 Rationale for ISO 12812 (all parts) **11**
7.1 General 11
7.2 Environment description 11
7.2.1 General 11
7.2.2 Increased dematerialization of financial services 12
7.2.3 Increased use of financial services 12
7.2.4 Increased cross-border payments 12
7.2.5 Remote management of applications 12
7.2.6 Enhanced proximate functionalities 12
7.2.7 Enhanced multi-application environment 13
7.3 Standardization challenges 13
7.3.1 General 13
7.3.2 Adaptation of mobile financial services to a fast evolving technology 13
7.3.3 Complexity of ecosystems 13
7.3.4 Complexity of regulatory systems 13
7.3.5 Consumer expectation for accessing all services using the same device 13
7.3.6 Risk management in the mobile environment 14
7.3.7 Certification programs 14
7.3.8 Role of the mobile device 14

8 Mobile payments **14**
8.1 General payment functions 14
8.1.1 General 14
8.1.2 Payment service issuance 14
8.1.3 Payment service activation 14
8.1.4 Payment service selection by the payer 15
8.1.5 Application selection by the POI or the payment gateway 15
8.1.6 Application data retrieval 15
8.1.7 Customer identification 15
8.1.8 Payer authentication 15
8.1.9 Application authentication 15
8.1.10 Payer authorization/confirmation 15
8.1.11 Transaction data authentication 15
8.1.12 MFSP authorization 15
8.1.13 Completion of the transaction 16

© ISO 2017 – All rights reserved

8.1.14 Clearing and settlement 16
8.1.15 End of service 16
8.2 Mobile proximate payment 16
8.2.1 General 16
8.2.2 Mobile contactless payment 16
8.2.3 Mobile proximate payment based on bar code 17
8.3 Mobile remote payment 17
8.3.1 General 17
8.3.2 Payment to businesses 17
8.3.3 Payment to persons 18

9 Mobile banking 19
9.1 General 19
9.2 General mobile banking functions 19
9.2.1 General 19
9.2.2 Enrolment 19
9.2.3 Customer profile management 20
9.2.4 Banking service issuance 20
9.2.5 Customer identification 20
9.2.6 Customer authentication 20
9.2.7 Customer authorization/confirmation 20
9.2.8 Transaction data authentication 20
9.2.9 Financial institution authorization 20
9.2.10 Completion of the banking operation 20
9.2.11 End of service 20
9.3 Channels for mobile banking 20
9.3.1 General 20
9.3.2 Mobile Internet browser 21
9.3.3 Mobile application 21
9.3.4 Short Messaging Service (SMS) 21

10 Mobile financial services supporting technologies 21
10.1 Mobile device 21
10.2 Mobile communication 22
10.3 Mobile device local interface 22
10.4 Applications 22
10.5 Mobile wallet 22
10.6 Secure element 23
10.7 User interface 24
10.8 Trusted execution environment 24
10.9 Secured server 24
10.10 Service management 25

11 Stakeholders involved in the mobile payment ecosystems 25

12 Implementations of ISO 12812 (all parts) 26

Annex A (informative) **Organizations involved in mobile standardization and guidance 27**

Annex B (informative) **Mobile payment ecosystems and related business models for MFSPs 28**

Annex C (informative) **Payment instruments 30**

Bibliography 33

 © ISO 2017 – 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 on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 7, *Core banking*.

A list of all the parts in the ISO 12812 series can be found on the ISO website.

© ISO 2017 – All rights reserved

Introduction

The use of mobile devices to conduct financial services (i.e. payments and banking) is occurring following the steady rise in the number of customers using the Internet for these services. As an evolving market, mobile financial services are being developed and implemented on various bases throughout the different regions of the world and also among the various providers of such services. In these conditions, the purpose of the ISO 12812 (all parts) is to facilitate and promote interoperability, security and quality of mobile financial services. At the same time, it is important that stakeholders in the services can benefit from the evolution and service providers remain commercially free and competitive in order to pursue their own business strategies. ISO 12812 (all parts) addresses the interoperability only at the technical layer by considering the impact of new components and/or interfaces induced by the introduction of a mobile device in financial services. The intentions of ISO 12812 (all parts) are as follows.

a) To advance interoperability of mobile financial services globally by defining requirements based on a common terminology and basic principles for the design and operation of mobile financial services.

b) To define technical components and their interfaces, as well as roles that may be performed by different actors in addition to mobile financial service providers (e.g. mobile network operators, trusted service managers). These components and their interfaces, as well as roles, are defined according to identified use cases. Future use cases may be considered during the maintenance of ISO 12812 (all parts).

c) To identify existing standards on which mobile financial services should be based, as well as possible gaps.

Standardization in this area is beneficial for the sound development of the mobile financial services market because it will:

— facilitate and promote interoperability between the different components or functions building mobile financial services;

— build a safe environment so that consumers and merchants can trust the service and allow the mobile financial service providers to manage their risks;

— promote consumer protection mechanisms including fair contract terms, rules on transparency of charges, clarification of liability, complaints mechanisms and dispute resolution;

— enable the consumer to choose from different providers of devices or mobile financial services including the possibility to contract with several mobile financial service providers for services on the same device;

— enable the consumer to transfer a mobile financial service from one device to another one (portability);

— promote a consistent consumer experience among various mobile financial services and mobile financial service providers with easy-to-use interfaces.

To achieve these objectives, each part of ISO 12812 (all parts) will specify the necessary technical mechanisms and, when relevant, refer to existing standards as appropriate.

ISO 12812 (all parts) provides a framework flexible enough to accommodate new mobile device technologies, as well as to allow various business models. At the same time, it enables compliance with applicable regulations including data privacy, protection of personally-identifiable data, consumer protection, anti-money laundering and prevention of financial crime.

It is not the intention of ISO 12812 (all parts) to duplicate or to seek to replace any existing standard in the area of mobile financial services (e.g. communication protocols, mobile devices). It is also not the intention to drive technology to any specific application or to restrict the development of future

 © ISO 2017 – All rights reserved

technologies or solutions. Messages and data elements to be exchanged at the interfaces between the different components or actors of the system may be those already specified [e.g. ISO 20022, ISO 8583 (all parts)].

ISO 12812 (all parts) recognizes the need for unbanked or under-banked consumers to access mobile financial services. It also recognizes that these services may be provided by diverse types of institutions in accordance with the applicable regulation(s).

The ISO 12812 series consists of the following parts:

— *Part 1: General framework* — The introduction of the standard with descriptions of some fundamental bases on which the other parts are built;

— *Part 2: Security and data protection for mobile financial services* — Definition of a general framework for the secure execution of mobile financial services;

— *Part 3: Financial application lifecycle management* — The lifecycle of the application including roles and infrastructure for secure provisioning;

— *Part 4: Mobile payments to persons* — Use cases and requirements for interoperability;

— *Part 5: Mobile payments to businesses* — Use cases and requirements for interoperability.

© ISO 2017 – All rights reserved

Core banking — Mobile financial services —

Part 1: General framework

1 Scope

This document defines the general framework of mobile financial services (payment and banking services involving a mobile device), with a focus on:

a) a set of definitions commonly agreed by the international financial industry;

b) the opportunities offered by mobile devices for the development of such services;

c) the promotion of an environment that reduces or minimizes obstacles for mobile financial service providers who wish to provide a sustainable and reliable service to a wide range of customers (persons and businesses), while ensuring that customers' interests are protected;

d) the different types of mobile financial services accessed through a mobile device including mobile proximate payments, mobile remote payments and mobile banking, which are detailed in other parts of ISO 12812;

e) the mobile financial services supporting technologies;

f) the stakeholders involved in the mobile payment ecosystems.

This document includes the following informative annexes:

— an overview of other standardization initiatives in mobile financial services (Annex A);

— a description of possible mobile payment business models (Annex B);

— a description of typical payment instruments which may be used (Annex C).

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
acquirer
institution (3.17) that has contracted with the *merchant* (3.19)/*payee* (3.38) in order to process the *payment transaction* (3.40) data and transmit onwards in the *payment system* (3.45)

Note 1 to entry: This role might or might not be performed by the merchant/payee institution.

© ISO 2017 – All rights reserved

3.2
alias
pseudonym for the *payer* (3.39) and/or the *payee* (3.38) uniquely linked to the name and account associated to the *payment instrument* (3.43)

EXAMPLE Mobile phone number.

3.3
application
set of program modules (application software) and/or data (application data) needed to provide functionality for a *mobile financial service* (3.25)

EXAMPLE Payment application, authentication application, user interface application, *mobile wallet* (3.35).

3.4
authentication
provision of assurance that a claimed characteristic of an entity is correct

Note 1 to entry: The provision of assurance may be given by verifying the identity of an individual, device or process.

[SOURCE: ISO/IEC 27000:2016, 2.7, modified —Note 1 to entry has been added.]

3.5
authentication credential
data provided by the *mobile financial service provider (MFSP)* (3.27) to the *customer* (3.12) in order to allow the authentication of the customer

EXAMPLE PIN, mobile code.

3.6
bar code
optical machine-readable representation of data

Note 1 to entry: Bar codes include QR codes (ISO/IEC 18004), Data Matrix (ISO/IEC 16022) and MaxiCode (ISO/IEC 16023).

3.7
cardholder verification method
CVM
particular case of *user verification method (UVM)* (3.63) when the *payment instrument* (3.43) is a card

3.8
consumer
person using a *mobile device* (3.24) to purchase goods or services and who is acting for purposes other than trade, business or profession

3.9
contactless
radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them

Note 1 to entry: Contactless is not to be confused with wireless which is a more general term.

Note 2 to entry: Contactless technology is specified in ISO/IEC 14443.

3.10
credential
data provided to the *customer* (3.12) for identification/authentication purposes

© ISO 2017 – All rights reserved

3.11
credit transfer
payment initiated by the *payer* (3.39) which results in transferring an amount of money from a payer's account to a *payee's* (3.38) account

3.12
customer
person or business that has contracted with an MFSP in order to use *mobile financial services* (3.25)

3.13
direct debit
payment initiated by the *payee* (3.38) which results in transferring an amount of money from a *payer's* (3.39) account to a payee's account

Note 1 to entry: A direct debit is usually pre-authorized in the form of a mandate between the payer and the payee.

3.14
electronic money
electronically stored monetary value measured in currency and stored on a device, such as a *mobile device* (3.24), or at a server remotely and that can be purchased by a *consumer* (3.8) and used for payment

3.15
host card emulation
HCE
implementation of *contactless* (3.9) payments where the payment application is held in the *mobile device* (3.24) host

3.16
identification credential
data provided by an *institution* (3.17) to the *customer* (3.12) in order to allow the identification of the customer

3.17
institution
entity authorized to provide financial services under the applicable regulation(s)

3.18
know your customer
KYC
process to verify the identity of a *customer* (3.12) in order to prevent financial crime, money laundering and terrorism financing

3.19
merchant
business that accepts *mobile payments* (3.29) for the goods or services purchased by a *consumer* (3.8)

3.20
mobile banking
access to and execution of online banking services through a *mobile device* (3.24)

3.21
mobile card payment
mobile payment (3.29) using a card *payment credential* (3.41) and a card infrastructure for authorization and settlement

3.22
mobile code
authentication credential (3.5) used as UVM and entered via the *mobile device* (3.24)

© ISO 2017 – All rights reserved

3.23
mobile contactless payment
mobile proximate payment where the *payer* (3.39) and the *payee* (3.38) communicate directly using *contactless* (3.9) technologies

3.24
mobile device
personal device with mobile communication

EXAMPLE Mobile phone, *smartphone* (3.56), tablet.

Note 1 to entry: A mobile device can have an NFC capability.

3.25
mobile financial service
MFS
mobile payment (3.29) (including retail payment) and *mobile banking* (3.20) service

3.26
mobile financial service program
MFS program
set of rules, practices and standards agreed between the MFSPs participating in the program for the functioning of the MFS

3.27
mobile financial service provider
MFSP
institution (3.17) that has contracted with the *customer* (3.12) and that is responsible for providing the *mobile financial service* (3.25) to that customer

3.28
mobile network operator
MNO
mobile telecommunication operator that provides a range of mobile communication services, including *over the air* (3.37) connectivity

3.29
mobile payment
payment involving a *mobile device* (3.24) and using a *payment instrument* (3.43) and associated infrastructures

3.30
mobile payment ecosystem
set of stakeholders which interact to form a stable functioning *payment system* (3.45) in the mobile environment

3.31
mobile proximate payment
mobile payment (3.29) where the *payer* (3.39) and *payee* (3.38) (and/or his/her equipment) are in the same location

Note 1 to entry: This terminology is preferred to mobile proximity payment as the wording proximity has a specific meaning for *contactless* (3.9) standards (ISO/IEC 14443).

Note 2 to entry: Mobile proximate payments include, but are not limited to, *mobile contactless payments* (3.23).

3.32
mobile remote payment
mobile payment (3.29) whereby the transaction is conducted over a mobile communication network and which can be made independently from the *payee's* (3.38) location (and/or his/her equipment)

© ISO 2017 – All rights reserved

3.33
mobile service
service accessed through a *mobile device* (3.24)

EXAMPLE *Mobile financial service* (3.25), transit/public transport, shopping, loyalty and information.

3.34
mobile service provider
entity providing a *mobile service* (3.33) to the end-user

Note 1 to entry: For *mobile financial service* (3.25), the service provider is called a *mobile financial service provider (MFSP)* (3.27).

Note 2 to entry: The definition does not include suppliers (vendors) to the mobile service providers and which are not known by the end-user.

3.35
mobile wallet
digital container accessed by the *mobile device* (3.24) that allows a *consumer* (3.8) to store applications and *credentials* (3.10) being used for mobile financial and non-financial services

Note 1 to entry: This container may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a server (or a combination thereof) or on a *merchant* (3.19) website.

3.36
near field communication
NFC
contactless (3.9) communication interface and protocol specified by ISO/IEC 18092 and ISO/IEC 21481

3.37
over the air
OTA
data channel operated by a *mobile network operator* (3.28) for the remote management of components resident in the *mobile device* (3.24)

3.38
payee
person or legal entity who is the intended recipient of funds which have been the subject of a *payment transaction* (3.40)

3.39
payer
person or legal entity who authorizes a *payment transaction* (3.40)

3.40
payment
payment transaction
act of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the *payer* (3.39) and the *payee* (3.38)

3.41
payment credential
data provided by the MFSP to the *customer* (3.12) in order to allow the identification of the customer account associated to the *payment instrument* (3.43)

EXAMPLE IBAN, PAN.

3.42
payment gateway
service located on a distant server for the acceptance of *mobile remote payments* (3.32)

© ISO 2017 – All rights reserved

3.43
payment instrument
personalized device and/or set of procedures agreed between the *payer* (3.39) and the *institution* (3.17) and used by the payer in order to conduct a *payment transaction* (3.40)

EXAMPLE *Credit transfer* (3.11), card payment and *electronic money* (3.14).

3.44
payment scheme
set of rules, practices, standards and/or implementation guidelines agreed between scheme participants for the functioning of payment services and which is separated from any infrastructure or *payment system* (3.45) that supports its operation

3.45
payment system
funds transfer system with formal and standardized arrangements and common rules for the processing, clearing and/or settlement of *payment transactions* (3.40)

3.46
payment to business
payment transaction (3.40) where the *payee* (3.38) is a business

3.47
payment to person
payment transaction (3.40) where the *payee* (3.38) is a person

3.48
point of interaction
POI
device used for the acceptance of *mobile payments* (3.29)

EXAMPLE POS, vending machine, ATM for proximate payments and *payment gateway* (3.42) for remote payments.

Note 1 to entry: The POI may be a *mobile device* (3.24).

3.49
remittance
transfer of an amount of money between two persons

Note 1 to entry: In the context of ISO 12812 (all parts), remittance includes domestic and cross-border transfer of money.

3.50
secure element
SE
tamper-resistant platform in the *mobile device* (3.24) capable of securely hosting and executing applications and associated confidential and cryptographic data (e.g. key management)

EXAMPLE UICC, embedded secure elements, chip cards and SD cards.

3.51
SE provider
entity that owns the original access rights to the SE

3.52
secured server
secure environment (3.53) located on a server

© ISO 2017 – All rights reserved

3.53
secure environment
system that implements the controlled storage and processing of information in order to protect personal and/or confidential data

Note 1 to entry: In the context of *mobile financial services* (3.25), it can be located in the *mobile device* (3.24), such as a *secure element* (3.50), a *trusted execution environment* (3.60) or software with supplementary *security controls* (3.54), or in a remote *secured server* (3.52).

3.54
security controls
management, operational and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information

3.55
short message service
SMS
service that enables a mobile phone or a server to send messages of limited length to one or several mobile phone(s)

3.56
smartphone
mobile device (3.24) that performs functions of a computer such as data storage, capability to run downloadable applications and Internet access

3.57
strong authentication
authentication procedure using a minimum of two independent (from the security point of view) authentication mechanisms, with at least one of them being dynamic

3.58
third party
party who is not one of the parties primarily involved in a transaction

3.59
tokenization
process by which a *payment credential* (3.41) is replaced with a surrogate value called a payment token

Note 1 to entry: Tokenization can be undertaken to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

3.60
trusted execution environment
TEE
aspect of the *mobile device* (3.24) comprising hardware and/or software which provides security services to the mobile device computing environment, protects data against general software attacks and isolates hardware and software security resources from the operating system

3.61
trusted service manager
TSM
trusted third party (3.62) acting on behalf of the *secure environment* (3.53) provider and/or the *mobile financial service provider* (3.27) in order to perform the provisioning and management of the application

3.62
trusted third party
third party (3.58) trusted by other entities with respect to security-related activities

© ISO 2017 – All rights reserved

3.63
user verification method
UVM
method verifying that the person who uses the *mobile financial service* (3.25) is the legitimate *customer* (3.12) of the *mobile financial service provider* (3.27)

Note 1 to entry: A UVM can be based on the processing of *authentication credentials* (3.5).

3.64
unstructured supplementary services data
USSD
functionality built into the GSM standard to support transmitting information over the signalling channels of the GSM network

4 Abbreviated terms

ATM	Automated Teller Machine
CVM	Cardholder Verification Method
IBAN	International Bank Account Number
HCE	Host Card Emulation
KYC	Know Your Customer
MFS	Mobile Financial Service
MFSP	Mobile Financial Service Provider
MNO	Mobile Network Operator
NFC	Near Field Communication
OS	Operating System
OTA	Over The Air
PAN	Primary Account Number
PIN	Personal Identification Number
POI	Point Of Interaction
POS	Point Of Sale
QR	Quick Response
SE	Secure Element
SMS	Short Message Service
TEE	Trusted Execution Environment
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Services Data
UVM	User Verification Method

© ISO 2017 – All rights reserved