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 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

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.

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

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.

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.

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

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)

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)

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)

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

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

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

5 Concept of interoperability

5.1 General

Numerous definitions exist for the term interoperability. Some limit the concept at a technical level such that interoperability is the ability of systems to provide services to and accept services from other systems and to enable them to operate effectively together.

NOTE According to ISO/IEC 2382, interoperability is defined as "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units".

Other definitions include the role of organizations in deciding to work together by using systems able to operate together. In that context, interoperability is the ability for systems and organizations to work together (inter-operate).

Payments generally involve several parties forming a chain of technical components or systems. In that context, the concept of interoperability includes two layers: a business layer and a technical layer.

5.2 Concept of interoperability for payments: the business layer

In payments, the business layer of the interoperability concept is essential so that any two organizations in the payment chain have decided to work together by agreeing terms and conditions of their cooperation. This is typically the case of the relationship between a merchant and its acquirer/institution. The merchant may only offer the consumer means of payments provided by that given acquirer/institution (or several acquirers/institutions if the merchant has contracted with several of them). The consumer may have subscribed to some means of payment with one or several payment service providers. The consequence of business interoperability is that a consumer may use one of these means of payment which are accepted by the merchant.

5.3 Concept of interoperability for payments: the technical layer

For the technical layer, interoperability means that an organization may easily operate with several other entities for a given service attributable to systems that are compatible. In information technologies, and particularly for payments, this principle implies that the interfaces between two successive components of the payment chain are standardized allowing solutions to be implemented by several vendors. For some interfaces, more than one standard may exist, impacting the level of interoperability with less efficient processes within the entities being involved at that interface if several standards are implemented. Interoperability does not necessary imply that a single standard exists at a given interface.

The term compatibility is equivalent to the technical layer of the concept of interoperability.

NOTE In daily life, when a consumer has to substitute a component of a device by a new one, compatibility is required. This is, for example, the case for a supply power adapter of a mobile device. A new supply power adapter is compatible with the device on the conditions that both power supplied and plug fit the features of the device.

For payment, a solution of a vendor is compatible with the system of an organization if it may easily substitute an already installed compatible solution of another vendor. This compatibility is facilitated if both solutions are compliant with a common standard.

The technical layer of the interoperability concept includes different aspects such as implementations of application, function, security, communication, protocol, data element and operation.

5.4 Interoperability objectives

The objective of ISO 12812 (all parts) is to address interoperability only at the technical layer. ISO 12812 (all parts) considers the impact of new components and/or interfaces created by the introduction of a mobile device in the payment chain. It does not address interoperability of existing

components and/or interfaces of payment chains reused in MFS (e.g. already existing payment instruments). ISO 12812 (all parts) is not intended to duplicate existing standards that may be used in the mobile environment. The relevant standards are quoted for the different interfaces between components of the mobile payment chains (see Annex A for examples of standardization organizations involved in mobile financial services).

6 Relationships between customers and MFSPs

6.1 General

The term mobile financial service provider (MFSP) is used in ISO 12812 (all parts) for designating an institution having built an MFS offer accessed by their customers via a mobile device. When an institution is inserted in a MFS value chain without providing the service via a mobile device, this institution is not named an MFSP. This is the case of a payee institution, for example. Figure 1 represents the different expressions related to institutions being used in ISO 12812 (all parts) for both mobile payment and banking.

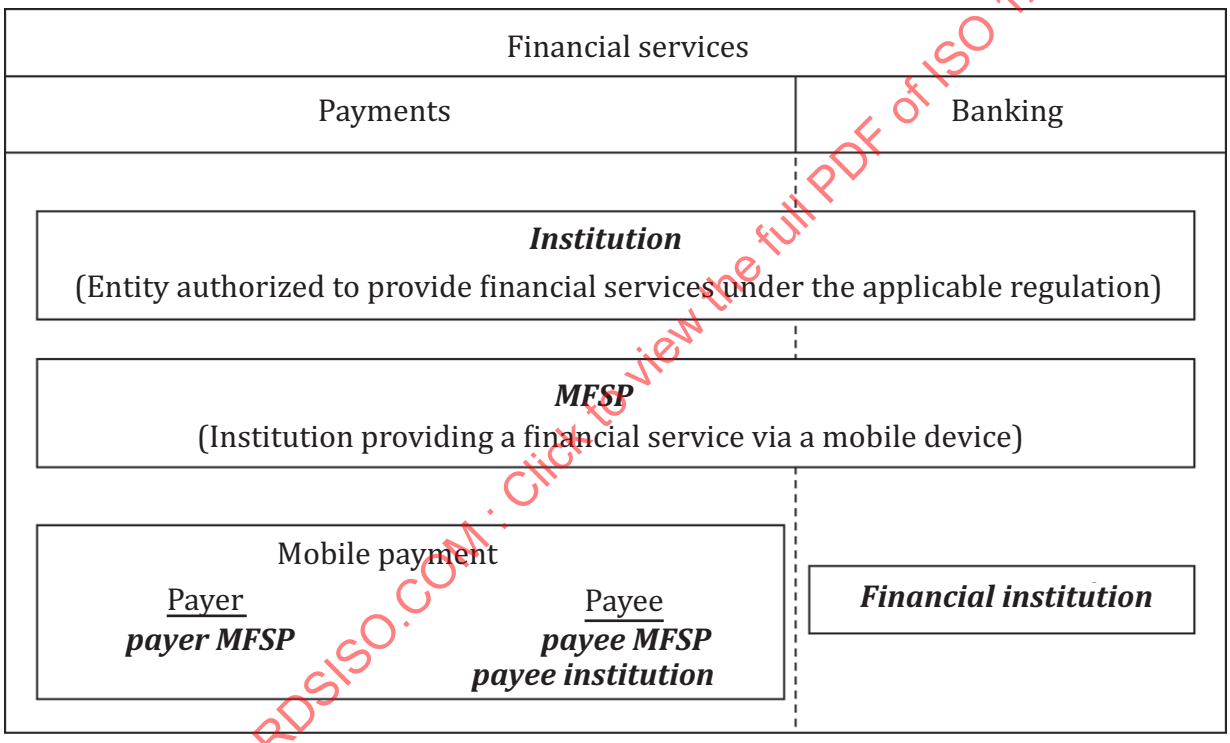

Figure 1 — Terminology related to institutions

6.2 Legal status of the customer

The customer may be either a person (i.e. an individual) or a legal entity (i.e. a business, a merchant).

6.3 Role played by the customer

In case of a mobile payment between two customers from one or two institution(s), the customer that confirms the payment is called the payer and the customer that is the recipient of the funds is called the payee.

6.4 Contractual relationship between the customer and the institution

Institutions mainly distinguish between two types of contracts with their customers for the use of mobile financial services:

a) a contract for persons who are (1) paying for goods and services and/or (2) sending and/or receiving funds and/or (3) using banking services;

b) a contract for legal entities which are (1) receiving funds for providing goods and services and/or (2) paying for purchasing goods and services from another business and/or (3) using banking services.

NOTE It is up to the institution to decide to have a new contract with their customers for mobile financial services.

6.5 Choice of wording for ISO 12812 (all parts)

Depending upon the context, the following wording is used in this document:

a) payer/payee;

b) person/legal entity or business;

c) consumer/merchant.

However, in the context of mobile payment, the term business is preferred over the term merchant or legal entity and the term person is preferred over the term consumer. ISO/TS 12812-4 is named "Mobile payments to persons" and ISO/TS 12812-5 is named "Mobile payments to businesses".

ISO/TS 12812-4 and ISO/TS 12812-5 differ by the nature of the payee (a person or a business, respectively). Depending on applicable legislations, ISO/TS 12812-4 includes payees as own-account workers (e.g. babysitting, gardener). ISO/TS 12812-5 includes situations where the payer is a consumer or a business.

The term customer is only used in the context of the relationship with an institution, while the term consumer is used in the context of a payment to business.

7 Rationale for ISO 12812 (all parts)

7.1 General

ISO 12812 (all parts) is intended to contribute to the development of MFSs by leveraging the mobile environment features described in 7.2 and by contributing to solve the challenges identified in 7.3.

7.2 Environment description

7.2.1 General

Several factors and changes in the area of mobile devices explain how these devices represent significant opportunities for the development of MFSs. First, the number of persons using mobile devices is growing in all parts of the world with a high penetration among the total population. Second, users of mobile devices almost always carry them, providing the users with a high degree of connectivity and access to MFSs. Finally, major evolutions beyond voice and short message service (i.e. text messaging) communications have enhanced the technological features of mobile devices. For example, the current MNO infrastructure supporting packet-oriented Internet access has led to the migration of mobile phones toward smartphones with more advanced computing ability and connectivity. Furthermore, an increasing number of mobile devices are being manufactured that are enabled with the NFC technology in parallel with other technologies such as the use of bar codes (see 10.3).

7.2.2 Increased dematerialization of financial services

Mobile devices present growing opportunities for MFSPs such as delivering new value-added services or conducting customer relationships in more dematerialized ways (e.g. by replacing less efficient means of payment such as cash and cheques).

7.2.3 Increased use of financial services

MFSs may be accessed by a customer anytime and anywhere and the use of these services is increasing. This is the case for traditional customers of MFSPs but also for individuals having few or no banking relationships. It is increasingly the case that these so-called "under-banked" or "unbanked" persons have access to mobile devices, creating an opportunity for broader financial inclusion through access to MFSs.

Mobile device penetration is providing significant opportunities for customers to use their mobile devices in a variety of payment scenarios.

7.2.4 Increased cross-border payments

Dematerialization of payments made by mobile payment services is facilitating increased cross-border use such as remittances where expatriates and guest workers in one country send part of their wages home to support family members in another country.

7.2.5 Remote management of applications

Thanks to their communication features, mobile devices enable the remote management of applications hosted within the device. The MFSP may carry out this management each time the mobile device is connected, i.e. mostly on a permanent basis. Examples of application management include:

a) the first application installation in the mobile device, its personalization and activation;

b) subsequent application upgrades;

c) application blocking when the mobile device is declared lost or stolen or compromised by some other means;

d) application reactivation when conditions are met;

e) application removal at the end of service.

The remote management of applications in case of mobile payments is a more efficient process compared to traditional means of payments such as plastic cards which need to be replaced by a new card, for example, when lost or stolen.

NOTE In case the application cannot be managed remotely, alternative solutions (e.g. the need for a direct physical connectivity) can be proposed by the MFSP for the application management. Such configurations are out of scope of ISO 12812 (all parts).

ISO/TS 12812-3 specifies the lifecycle management of applications.

7.2.6 Enhanced proximate functionalities

The introduction of the NFC technology (and other technologies) has become a source of new services because the mobile device may be used at the proximate point of interaction in a similar way as contactless cards. With respect to contactless cards, NFC mobile devices represent a new form factor enhancing the payment functionalities but using the same infrastructure as contactless readers which already accept contactless cards. The payment transaction speed is preserved with NFC mobile devices. An example of enhancement is the possibility to have higher transaction amounts (e.g. with respect to contactless cards used without PIN) as the customer authentication may be efficiently performed on the mobile device (e.g. using the mobile code).

Other proximate technologies such as bar codes are a source of new services described in 8.2.3.

Mobile devices may communicate with a secured server at the time of the transaction enhancing the functionalities of the service.

7.2.7 Enhanced multi-application environment

Mobile devices offer the capacity to host multiple applications issued by different service providers including MFSPs. It is an opportunity for MFSPs to provide their mobile services to customers already equipped with mobile devices, and it is also an opportunity for customers to access mobile services from several MFSPs. 10.5 describes the concept of the mobile wallet which is a possible supporting technology to implement multi-application.

Mobile devices offer the opportunity to host additional applications that may be used for financial services, such as identification, authentication and digital signature.

7.3 Standardization challenges

7.3.1 General

The technological evolutions described in 7.2 offer new opportunities to customers. But these evolutions also represent challenges to MFSPs for maintaining the sustainability of such services.

The use of global standards is key to solving these challenges and for fostering the conditions for an efficient development of MFSs.

7.3.2 Adaptation of mobile financial services to a fast evolving technology

In order to offer MFSs to a wide range of customers, MFSPs have to support multiple implementations to host their services on a variety of mobile devices with multiple and frequent new releases. This fast-evolving technology may lead to customers' frequent replacement of mobile devices.

7.3.3 Complexity of ecosystems

The technological evolution of mobile devices has introduced new stakeholders into the ecosystems. As a consequence, the value chain is more complex.

In some situations, the existence of proprietary solutions may limit the access to other service providers.

7.3.4 Complexity of regulatory systems

MFSPs have to comply with multiple applicable regulations including data privacy, protection of personally-identifiable data, consumer protection, anti-money laundering and prevention of financial crime. Applicable regulations cover national and local law, legislation and regulation issued by regulatory authorities, as well as supra-national legislation and regulation.

Different jurisdictions may have different regulatory approaches. As a consequence, global MFSPs have to accommodate the different local regulations for providing cross border MFSs compliant with these regulations.

7.3.5 Consumer expectation for accessing all services using the same device

A strong expectation of consumers is that a mobile device supports a multi-service/application environment. They expect that the mobile device is capable of hosting services of any of the competing MFSPs with which they have contracted. Furthermore, the consumers expect that their mobile devices support services outside of a purely financial environment (e.g. transit/public transport, loyalty). The challenge is to accommodate all requirements of the different service providers sharing the same device, without impacting mobile financial services considered as sensitive ones. Another consumer requirement is to have a convenient user interface for accessing the different mobile services.

7.3.6 Risk management in the mobile environment

It is a challenge for MFSPs to maintain the sustainability of their investments in MFSs. Security is key to building trust in MFSs for their adoption by consumers and merchants. MFSPs have little control over mobile devices and with the increased access to the Internet, mobile devices are subject to new vulnerabilities in this environment, e.g. malware. An assessment needs to be conducted to identify risks and to define proper counter measures relevant to any MFS. Specific security mechanisms (e.g. secure environment) should then be implemented to prevent the identified risks and to minimize fraud. Such mechanisms have to be cost efficient, yet robust enough to counter possible attacks, with minimal impact on the transaction time. ISO/TS 12812-2 describes and specifies a framework for the management of the security of MFS.

7.3.7 Certification programs

To ensure that functional and security requirements are correctly implemented, it would be beneficial to have certification programs in place even if it is very challenging due to the increasing sophistication of this environment. Indeed, these programs should cover:

a) mobile devices and their related components when part of the MFS (e.g. secure environments);

b) components and functionalities providers;

c) each part of the infrastructure.

The scale of the certification programs may vary according to business decisions between stakeholders involved in the MFS.

7.3.8 Role of the mobile device

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 may be seen as a channel to use a payment instrument or access a banking service or a tool for customer identification and/or authentication.

8 Mobile payments

8.1 General payment functions

8.1.1 General

A mobile payment is defined as a payment enabled by a mobile device using a payment instrument (e.g. card payment, credit transfer) and infrastructures (e.g. card networks, automated clearing houses). The general functions forming the different steps of the existing payment service apply also to mobile payments and are described hereafter (other specific functions may exist). The following functions assume that the customer (payer and payee) has accepted to use the service. The steps and their order described hereafter may differ according to implementations. Some functions may not be present for a mobile payment transaction.

8.1.2 Payment service issuance

During this first step, the MFSP checks the eligibility of the mobile device to host the service and then contracts with the customer. Then, the MFSP makes the application available to the customer and establishes any associated authentication credentials (e.g. PIN or password).

8.1.3 Payment service activation

This is the action by the customer to activate the service. It may require the use of an authentication credential.

8.1.4 Payment service selection by the payer

This is the action of the payer to select one payment service among several hosted on the mobile device.

NOTE This step can be optimized by e.g. a pre-selection of one payment service by the payer.

8.1.5 Application selection by the POI or the payment gateway

This is the process handled by the POI or the payment gateway to select one application, taking into account the preferences of the payer.

8.1.6 Application data retrieval

This step consists of providing the necessary data for the payment transaction. It may be performed either manually by entering payment credentials or by the application itself.

8.1.7 Customer identification

Customers are traditionally identified using an account number, but in a mobile environment, other identifiers (e.g. mobile phone number) may be used as alias, especially for payments to persons.

8.1.8 Payer authentication

This is the step MFSPs use for verifying the payer identity through authentication. It is performed using UVMs which are based on something the payer has (e.g. mobile device), something the payer knows (e.g. PIN, passwords) or something the payer is (e.g. biometrics). In the mobile environment, the knowledge factor may be entered either on the POI or on the mobile device. In the framework of this document, the term PIN is used when the knowledge factor is entered on the POI and the term mobile code is used when the knowledge factor is entered on the mobile device.

8.1.9 Application authentication

This is the process by which the POI (for offline authentication) or the MFSP (for online authentication) verifies the legitimacy of the application using cryptographic mechanisms.

8.1.10 Payer authorization/confirmation

This is the consent of the payment transaction by the payer.

NOTE This consent can be materialized, for example, by entering a PIN, by pressing a key or by approaching the mobile device on the contactless target of the POI (Tap).

8.1.11 Transaction data authentication

This is the process by which the MFSP checks that the transaction data (e.g. transaction amount, UVM results, transaction context) are genuine by using cryptographic mechanisms.

NOTE Transaction data authentication can also be performed by the POI in combination with application authentication.

8.1.12 MFSP authorization

During this step, the MFSP authorizes the payment based on its own risk management policy, the results of previous steps (e.g. authentication) and the context of the transaction. The authorization response is given either online by the MFSP or offline by the payment application when hosted within the mobile device.

NOTE When the payment instrument is a credit transfer, the MFSP authorization response can be given in the form of a confirmation message to the beneficiary. This response only indicates the payment has been initiated.

8.1.13 Completion of the transaction

At the end of the transaction, both payer and payee are notified about the completion of the transaction (e.g. by delivering a paper or dematerialized receipt).

8.1.14 Clearing and settlement

Clearing is the process performed by a clearing system whereby institutions (e.g. acquirers for card payments or payer institution for credit transfer) present and exchange payment data to other institutions (e.g. issuers for card payments or payee institution for credit transfers), in order to facilitate the settlement of their obligations in the settlement system.

8.1.15 End of service

The end of service is initiated either by the customer or by the MFSP. The application is then removed or disabled so that the service cannot be used anymore. When applicable, the MFSP should inform the customer about relevant regulations that govern handling of any remaining assets, for example, after the death of a customer.

8.2 Mobile proximate payment

8.2.1 General

Mobile proximate payments may be initiated by the mobile device using different interfaces such as the contactless one (e.g. NFC), the optical one (e.g. bar code) and others (see 10.3).

8.2.2 Mobile contactless payment

8.2.2.1 General

A mobile contactless payment occurs when the payer and the payee (and/or their equipment) are in the same location and communicate directly through their equipment using a contactless interface (e.g. NFC).

8.2.2.2 Payments to businesses

Two scenarios are considered (see ISO/TS 12812-5).

a) Scenario 1: card emulation mode.

The mobile contactless payment to business transactions are based on the card instrument; the mobile device is the emulation of a contactless card from the POI reader perception. This scenario uses the POI communication network to connect to the card infrastructure.

These transactions may be performed in different ways such as the following non-exhaustive examples.

1) Mobile contactless payments with tap and go: the customer uses his/her contactless-enabled mobile device to conduct a payment at a contactless POI terminal with no CVM during the transaction (typically for low-value payment).

2) Mobile contactless payments with double tap: the customer uses his/her contactless-enabled mobile device to conduct a payment at a contactless POI terminal with a CVM (such as a mobile code) during the transaction. This use case induces a second tap in order to inform the POI terminal that the CVM has been successfully checked and the user confirms the transaction.

NOTE The mobile code could be entered on the mobile device just prior to the payment (resulting in a single tap) or a PIN could be entered on the POI (also resulting in a single tap).

b) Scenario 2: in-store remote payment.

Mobile contactless payment to business transactions may be initiated in a contactless mode and then further processed remotely using the mobile communication network. The payment instrument may be card or others. This use case is a hybrid solution compliant to both definitions of proximate and remote payments.

8.2.2.3 Payments to persons

The so called peer-to-peer mode of the NFC technology allows the establishment of a contactless channel between two mobile devices. This mode enables contactless payments to persons (see ISO/TS 12812-4).

8.2.3 Mobile proximate payment based on bar code

8.2.3.1 General

A mobile bar code payment occurs when the payer and the payee (and/or their equipment) are in the same location and communicate directly through their equipment using an optical interface.

8.2.3.2 Payments to businesses with bar code displayed by the mobile device

In this use case, the bar code is displayed by the mobile device of the payer at the time of the payment and presented to the merchant equipment in order to be optically read. The bar code includes the payment credential of the payer.

8.2.3.3 Payments to persons with bar code displayed by the mobile device

In this use case, the bar code is displayed by the mobile device of the payee at the time of the payment and presented to the payer mobile device in order to be optically read. The bar code includes the payment credential of the payee.

8.2.3.4 Payments to businesses with bar code displayed by the merchant

For this use case, the payer is located in the merchant location and at the time of the payment, the bar code is displayed on the merchant equipment or printed on a receipt. The bar code contains the transaction data and an Internet link. Once the mobile device has read the bar code, the payment is completed in a remote way.

This use case is a hybrid solution between a proximate and a remote payment as the transaction is initiated optically and then further processed remotely using the mobile communication network. It is another use case of in-store remote payment.

8.3 Mobile remote payment

8.3.1 General

Mobile remote payments are conducted independently from the payee's location. The payer uses the mobile device without interacting with a physical POI but by conducting the transaction over a mobile communication network. They cover both payments to businesses and payments to persons and the payment instruments used include card and credit transfer.

A mobile device includes features such as various user interfaces or geolocation enabling new payment use cases.

8.3.2 Payment to businesses

The typical mobile remote payment to a business occurs when a customer makes a purchase from a remote merchant (see ISO/TS 12812-5). It also includes a payment to a creditor (e.g. a utility) as long as

the customer is not connected to his/her MFSP to initiate the transaction. If the customer is connected to his/her MFSP to initiate the transaction, then the transaction is considered as a mobile banking service. Several use cases may be identified, such as the following.

a) Mobile remote card payments (single device): The customer uses his/her mobile device to conduct a payment to a mobile Internet merchant.

b) Mobile remote card payments (multiple devices): The customer uses his/her mobile device to conduct a payment to an Internet merchant after having purchased good or services through another device.

c) Customer-request mobile remote credit transfer: The customer uses his/her mobile device to initiate and conduct a payment to a mobile Internet merchant.

d) Merchant-request mobile remote credit transfer: The customer uses his/her mobile device to conduct a payment to a merchant upon receiving a payment request message from the merchant.

e) Remote payment based on geolocation: Businesses located in the neighbourhood of the mobile device may send advertisements with special offers on the condition that the payment is processed through the mobile device within a limited timeframe and before the customer physically reaches the merchant. An example of such a service is the advertisement by a restaurant of booking at a special rate and proceeding mobile remote payment at the time of receipt of the advertisement. Such advertising may fall within applicable regulations (e.g. should only be conducted with the customer's prior consent).

f) Interaction with an advertising medium: In this use case, the merchant generates a bar code on an advertising medium for public use. The bar code is generally the representation of an Internet link giving access to the merchant website. The customer uses an application on his/her mobile device to read and process the bar code. The payment is then completed remotely. When the advertising medium is, for example, a poster or street furniture, a contactless tag (that can be read by an NFC mobile device) may be used instead of a bar code.

g) Payment of invoice: The bar code is printed on the invoice. It contains the data related to the invoice and a link to the payment server. The customer uses an application on his/her mobile device to read and process the bar code.

8.3.3 Payment to persons

Remote mobile payments to persons include payments to other persons (e.g. family members, friends, colleagues) and remittances (see ISO/TS 12812-4). Several use cases may be identified such as the following.

a) Mobile remote credit transfer payment: The customer uses his/her mobile device to initiate a credit transfer to another person's account.

b) Mobile remote card payment: The customer uses his/her mobile device to conduct a card payment to another person's account.

A remote payment to a person may also consist of two transactions; for example, a first payment transaction with the card instrument between the payer and an intermediary institution, and secondly, credit transfer between this intermediary and the institution of the payee.

9 Mobile banking

9.1 General

Banking services encompass all financial services other than mobile payments. Mobile banking services are performed by the customer with its financial institution through the mobile device and may include services such as:

a) opening accounts;

b) accessing account balance information;

c) reviewing transaction history;

d) locating ATMs and/or branches to facilitate face-to-face banking;

e) storing of value and related transactions such as reloading;

f) bill presentment;

g) bill payment;

h) transferring funds between accounts;

i) remote deposit capture (check);

j) financial institution loyalty program such as cash rebate.

NOTE Payments performed from a mobile banking channel (see 9.3) are considered as mobile banking operations.

Mobile banking services are mainly performed remotely with the exception of services based on data recorded in the mobile device (e.g. reviewing of transaction log).

As mobile banking involves only one financial institution, the need for interoperability differs from mobile payment services. The issue of customer experience should be addressed to avoid important divergences between financial institutions concerning, for example, the access to mobile banking services. Nevertheless, the financial institution should consider the ease and effectiveness of the customer experience, although these issues, including the consistency of a customer's experience, may be viewed as a matter of competition between financial institutions over how their individual services are evaluated by their customers.

9.2 General mobile banking functions

9.2.1 General

The general functions forming the different steps of mobile banking services are described hereafter (other specific functions may exist). The order of the steps may differ according to implementations. Some functions may not be present for a mobile banking service.

9.2.2 Enrolment

In this function, the customer of the financial institution subscribes to the mobile banking service through a contract.

NOTE The customer can be an existing customer of the financial institution or a new customer, where the financial institution can require a higher level of risk management (e.g. KYC).

9.2.3 Customer profile management

In this function, the customer sets up his/her initial profile and updates it when necessary. A customer profile may contain preferences and other data such as a mobile phone number.

9.2.4 Banking service issuance

This function may include the delivery of an identification credential (mobile banking identifier) and an authentication credential to the customer for accessing the service. It may also include the downloading of an application and its personalization.

9.2.5 Customer identification

Customer identification is performed using the mobile banking identifier. Other identifiers (e.g. mobile phone number) may be used as an alias.

9.2.6 Customer authentication

Customer authentication is performed using the authentication credential associated with the mobile banking identifier. Different authentication credentials and/or mechanisms may be used depending on the service.

9.2.7 Customer authorization/confirmation

This is the consent of the mobile banking operation by the customer.

9.2.8 Transaction data authentication

This is the process by which the financial institution checks that the transaction data (e.g. amount of funds to be transferred) are genuine by using cryptographic mechanisms.

9.2.9 Financial institution authorization

During this step, the financial institution authorizes the banking operation by having taken its decision based on its own risk management policy, the results of previous steps (e.g. authentication) and the context of the operation.

9.2.10 Completion of the banking operation

At the end of the mobile banking operation, the customer is informed of the completion of the operation.

9.2.11 End of service

The end of service may be initiated by the customer or the financial institution. The application is then removed or disabled so that the service cannot be used anymore. When applicable, the financial institution should inform the customer about relevant regulations that govern handling of any remaining assets.

9.3 Channels for mobile banking

9.3.1 General

There are different ways/approaches to carrying out mobile banking operations such as using a mobile Internet browser, an application, the Short Messaging Service (SMS) and other real time services offered by MNOs (e.g. USSD). The use of one or another mobile banking channel depends on the actual financial institution, but in general, mobile Internet banking and applications are available in mature markets. Some other markets, on the other hand, are still relying on the SMS-based mobile banking approach.

9.3.2 Mobile Internet browser

In this scenario, a customer accesses the mobile banking service using the Internet browser on their mobile device. This can be seen as a similar experience to using Internet banking via a desktop or a laptop computer. In this scenario, the applications are installed within the internal infrastructure of the financial institution.

This scenario presents the same security and legal considerations as exists in Internet home banking.

9.3.3 Mobile application

In this scenario, a customer accesses the mobile banking service using the application which he/she would have downloaded either from their financial institution official website or from an application store.

The financial institution providing the application installed onto the mobile device is responsible for ensuring appropriate security measures are in place. Similarly, the financial institution would also have to ensure that the provided application works properly (as required) on the customer's mobile device.

9.3.4 Short Messaging Service (SMS)

In this scenario, the customer sends an SMS to the financial institution requesting a mobile banking service (e.g. to check the account balance or recent transactions or to transfer money to a pre-assigned bank account). This scenario does not need any use of an Internet browser or a downloaded application and does not request any mobile data communication services.

To enhance the customer experience and the ease of use, the customer's mobile phone number may be used as an identification method.

10 Mobile financial services supporting technologies

10.1 Mobile device

In addition to mobile communication capabilities (see 10.2), a mobile device may contain other components and functionalities such as:

a) an operating system;

b) user interface components, e.g. a display, a keyboard/touch screen, a microphone (see 10.7);

c) applications including functionalities for MFSs (see 10.4);

d) user interface applications (see 10.7);

e) a mobile wallet (see 10.5);

f) an NFC controller and antenna for contactless communication (see 10.3);

g) an optical camera in particular for reading bar codes (see 10.3);

h) a secure environment such as:

   1) one or several secure elements (see 10.6);

   2) a TEE (see 10.8);

   3) software with supplementary security controls (see ISO/TS 12812-2);

   4) a secured server (see 10.9).

10.2 Mobile communication

The mobile communication is based on different wireless technologies which provide at least the physical and transport layers which are not in principle under the direct control of the MFSP. Different wireless protocols can be used to connect the mobile device with a payment processing infrastructure (e.g. a payment gateway). This connection is performed through a mobile communication network provided by an MNO or a third entity.

The following wireless networks are examples of carriers for mobile financial services:

a) Wireless Wide Area Networks (WWAN), including 2G, 2,5G, 3G and 4G networks also known as GSM, EDGE,UMTS, LTE and CDMA;

b) Wireless Local Area Networks (WLANs): IEEE 802.11, a, b, g, n, ac (Wi-Fi);

c) Wireless Metropolitan Area Networks (WMANs): IEEE 802.16 (WiMAX).

10.3 Mobile device local interface

Mobile financial services may be initiated locally by the mobile device using different interfaces such as the contactless one (NFC) or the optical one (bar code) or other technologies (e.g. audio, Bluetooth Low Energy).

The contactless interface is different from the contact interface that was first used for smart cards. The contactless interface is based on a radio frequency communication whereas the contact interface is based on an electrical contact. The voluntary gesture of the user of a contactless device may induce a physical "contact" (or a "tap") of the mobile device with another equipment.

One of the advantages of contactless is to enable form factors other than the usual card format as the personal device.

Bar codes have been introduced in the mobile payment chain as the NFC technology was not widely deployed. Communication between the mobile device and the merchant equipment is however limited to one optical reading, with respect to NFC where communication exchanges are possible in both directions and where computations by the mobile device or the use of other resources may be mobilized in the course of the transaction. However, a one-off bar code may be generated before each optical reading.

10.4 Applications

An application is a set of program modules (application software) and/or data (application data) needed to perform a functionality. MFSs require one or several applications which may be located either on the mobile device or remotely, or both.

When an application has been downloaded by the customer from an application store or from a website of the MFSP, it is often called an App.

When the application is located on the mobile device, it may reside in the memory of the device under the control of its OS, or in the TEE or in a secure element. Additional information may be found in ISO/TS 12812-3 which specifies the financial application management.

Some general payment functions involving an application are described in 8.1.

10.5 Mobile wallet

Mobile devices are seen by businesses promoting their use as devices being able to replace physical wallets with digital ones. Mobile wallets contain applications able to deliver the same or enhanced services as items carried by physical wallets. These functionalities include, for example:

a) payment applications for the replacement of cash or payment cards contained in the physical wallet;

b) identification data or applications, for the replacement of magnetic stripes or smart cards including identity, access control or loyalty;

c) electronic value instead of physical representation (e.g. access tickets, vouchers or coupons);

d) transaction logs for the replacement of paper receipts.

The implementation of mobile wallets may occur either in the mobile device itself (hardware, software, data) or remotely on a server. Whichever implementation is used, the mobile wallet is always accessed by the user via the mobile device.

NOTE When the mobile wallet is on a server, it can also be accessed through another channel. In such a case, the wallet is considered in a more general way as a digital wallet.

Regarding financial services, the mobile wallet, more specifically, allows the user to securely store, access, manage and use payment instruments related information to initiate payments.

Although the mobile wallet provider (e.g. an MFSP, an institution, a merchant) provides the wallet functionalities, the usage of the mobile wallet is under the control of the user.

A mobile wallet should not be confused with electronic money which is a payment instrument used through an application (e.g. electronic purse) that could be contained in a mobile wallet.

10.6 Secure element

Due to the new vulnerabilities of mobile devices as a result of their increased access to the Internet, secure elements are seen as a solution to reinforce the security of mobile financial services. Secure elements offer features allowing the hosting of the applications in a secure manner using their own cryptographic capabilities. These features include:

— separation of applications;

— supervision of the application management by the sole MFSP;

— access rules to the application under the sole control of the MFSP.

The secure element is a means for the applications to provide the following basic trust services:

a) the strong authentication of the customer;

b) the integrity, end-to-end confidentiality and non-repudiation of the transactions;

c) the protection of customer privacy in the framework of a given regulation (i.e. an authorized access to and processing of personal identifiable information).

Secure elements have initially been introduced by institutions for the purpose of mobile contactless payment, but they can be used for increasing the security of other services such as mobile remote payment and mobile banking. Secure elements may host additional security functionalities (e.g. digital signature) that may be used by specific mobile financial services.

Secure elements may have several form factors such as UICC, SD card or embedded and may be issued by diverse categories of stakeholders, e.g. MNO for UICC, mobile device manufacturer for embedded. Whatever the configuration is, it is expected in the framework of ISO 12812 (all parts) that the secure element is able to host several applications issued by several institutions. The choice of the type of SE has an impact on the implementation of mobile financial services. The implication for the user has to be addressed and minimized.

10.7 User interface

The user interface of a mobile device is made of input and output components (e.g. display, keyboard/touch screen) allowing the customer to interact with the device. For mobile financial services, some user interface applications are needed to perform the following operations.

a) The management of the financial application, including its provisioning. This user interface application is part of the financial application itself.

b) The management of the multi-application environment. This user interface application is intended to help the customer

   1) select a financial application among several ones;

   2) order the available financial applications in a list;

   3) assign a level of priority of applications (e.g. for mobile contactless payments so a subsequent matching can be performed by comparison with the priorities of the POI).

   Mobile wallets provide such an interface and might be managed by the institution or be provided by a third party.

c) The mobile financial service transaction. This user interface application is used to interact with the customer for functions described in 8.1 and in 9.2 needing an action or for information of the progression of the transaction. This user interface is part of the financial application itself.

The user experience remains strongly challenged by the necessarily-small form factor of some mobile devices. For example, the amount of information that can be displayed at any given time and the ability of the user to enter complex text are limited. Therefore, it is important to provide easy-to-use mobile device interfaces with consistent user experience across all of the supported implementations.

The user interface may be subject to threats such as man-in-the-middle attacks between the user interface and the financial application. Some mechanisms have to be implemented to guarantee at the required level the integrity, the authenticity and the confidentiality of the information entered and/or confirmed by the customer using the user interface. One example of the mechanism is to establish a trusted path (see, for example, 10.8).

10.8 Trusted execution environment

A trusted execution environment is an execution environment inside the mobile device that runs alongside but is isolated from the environment provided by the 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 objective is to prevent the financial application from being executed by the generic OS of the mobile device as the OS may not be a secure enough environment for the application. The TEE offers an application program interface (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 may be implemented by the mobile device manufacturer.

A TEE may be used together with a secure element 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 secure element.

10.9 Secured server

A secured server is a secure environment located on a server and implementing a controlled storage and use of information for storing and processing personal and/or confidential data during the whole lifecycle management of the MFS.

In the context of ISO 12812 (all parts), a secured server is accessed by the mobile device.

NOTE Secured servers are also located in the MFS chain without a direct link with the mobile device (this is the case, for example, of a payer MFSP server connected to an acquirer in a mobile proximate payment using a card instrument).

A secured server is used for different purposes including:

a) application lifecycle management such as installation, personalization and activation of an application located on a mobile device (see 7.2.5 and ISO/TS 12812-3);

b) MFS transaction processing.

The use of secured servers for the processing of MFS transactions includes a large variety of configurations combining functionalities performed by both mobile devices and secured servers. An example of such a configuration for mobile proximate payment is where the application is held in the mobile device OS (e.g. host card emulation) and where additional MFS functionalities (e.g. tokenization) located in the secured server are used to complement the OS security.

A secured server may be used to access a mobile wallet containing applications for MFSs (see 10.5).

Applicable security requirements for secured server are described in ISO/TS 12812-2.

10.10 Service management

Service management related to the lifecycle management of applications is described in ISO/TS 12812-3.

In particular, mobile configurations using a secure environment shared by several service providers require a collaborative model between the provider of the secure environment and all service providers providing applications hosted within the secure environment. This collaborative model allows the management of the applications and their related data elements during their lifecycle. The main steps include the application provisioning and the data personalization, as well as subsequent maintenances. This model defines the different technical and security roles, as well as the responsibilities of the actors that are necessary for MFSP to implement their services on the mobile device of the customer. Of particular interest are the back-ends managing the lifecycle processes. ISO 12812 (all parts) offers flexibility to accommodate any business relationships between the different actors.

11 Stakeholders involved in the mobile payment ecosystems

Existing payment infrastructures involve other stakeholders in addition to institutions and their customers (payers and payees). For example, in the case of smart card payments, the stakeholders of this particular ecosystem include chip and card manufacturers, POI providers, card schemes and certification providers.

With mobile payments, new stakeholders have appeared in related ecosystems:

a) the mobile device manufacturers;

b) the mobile network operators, who are responsible for securely routing messages, operating the mobile network and issuing and recycling mobile phone numbers, which is important when the mobile numbers are used as alias.

Where secure environments are used and shared by several mobile service providers, the following stakeholders are added to this ecosystem:

— the manufacturers of any secure environment components (e.g. secure element manufacturers);

— the secure environment provider, e.g. for secure element, it may be an institution (typically when the SE is a removable secure SD card inserted in the mobile device), MNO (typically when the SE is an UICC) or mobile device manufacturers (typically when the SE is embedded in the mobile device);